

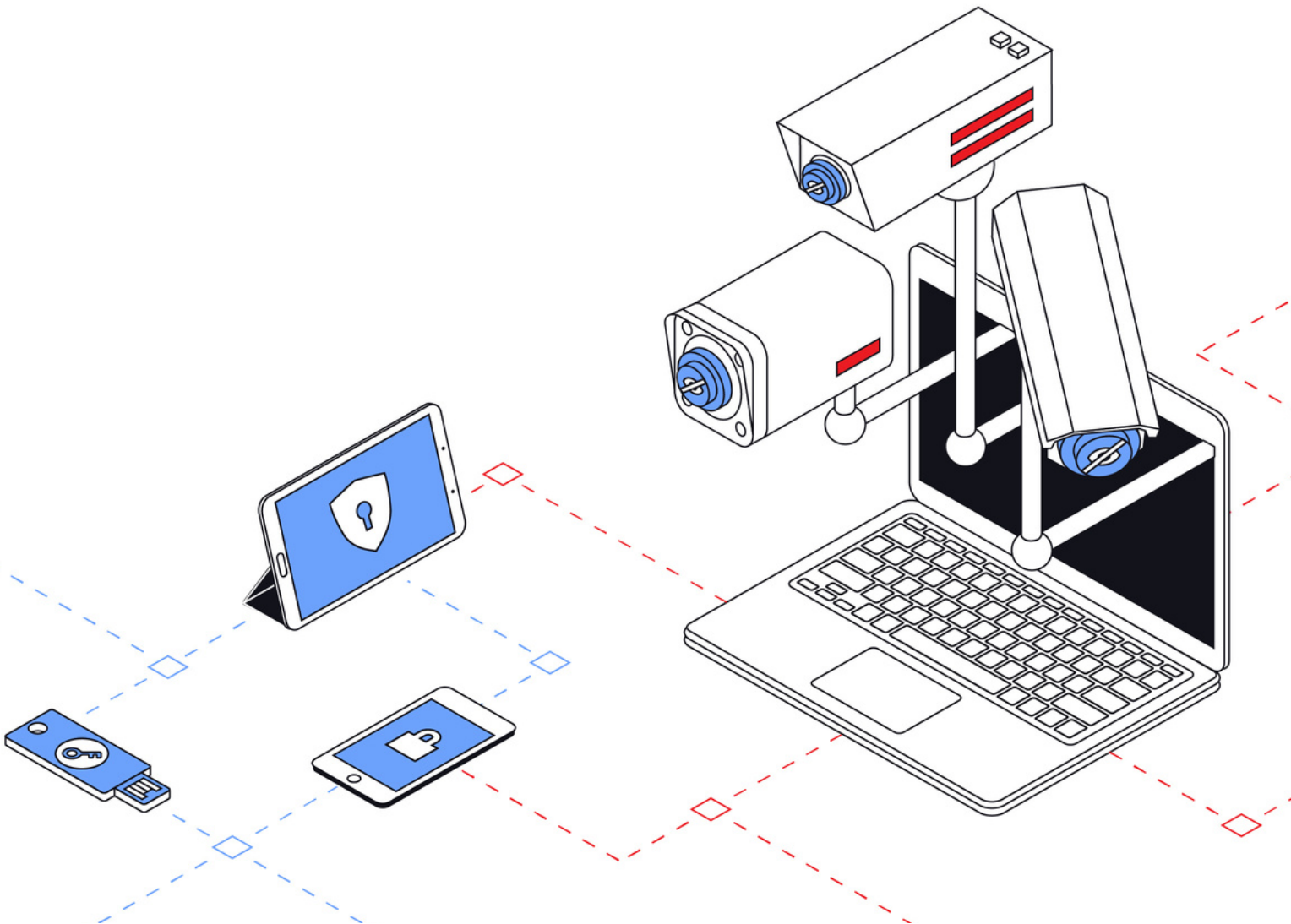


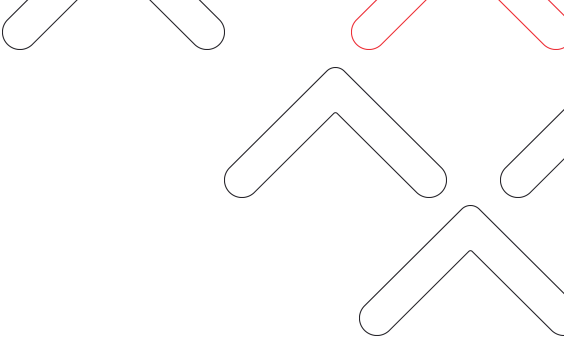
EngageMedia



ASIACENTRE

# Digital Security and Human Rights Defenders in the Asia-Pacific





**EngageMedia** is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at [engagemedia.org](https://engagemedia.org).

**Asia Centre** is a research institute that undertakes evidence-based advocacy by publishing policy reports, delivering capacity-building programmes, and engaging stakeholders to initiate change. In 2021, the Centre was accorded Special Consultative Status with the UN Economic and Social Council (UN ECOSOC), allowing it to advocate for human rights within the UN human rights framework.

Learn more at [asiacentre.org](https://asiacentre.org)



## Report Author

Asia Centre

## Research Team

### Lead

James Gomez, Asia Centre

Marc Piñol Rovira, Asia Centre

### Management

Egbert Wits, EngageMedia

### Indonesia

Research: Pradipa P. Rasidi, EngageMedia

Facilitator: James Gomez, Asia Centre

Logistics: Debby Kristin, EngageMedia

FGD Report: Vita Yudhani (Jakarta), Afina Faizah (Yogyakarta)

Partners: Muhammad Islah Satrio, KontraS (Jakarta); Ferdhi F. Putra, Combine Resource Institution (Yogyakarta)

### Bangladesh

Facilitator: Rezaur Rahman Lenin, Law Life Culture

FGD Report: Tasmiah Juthi, Digitally Right

Support: Rezwan Islam, EngageMedia; Md. Ashraful Haque, EngageMedia

## Thailand

Facilitator: Ekmongkhon Puridej, Asia Centre

FGD Report: Korbkusol Neelapaich, Asia Centre

## Advisory Team

Md. Ashraful Haque, EngageMedia

Khairil Zhafri, EngageMedia

Pradipa P. Rasidi, EngageMedia

## Editorial

Katerina Francisco, EngageMedia

Egbert Wits, EngageMedia

Published September 2023



Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License



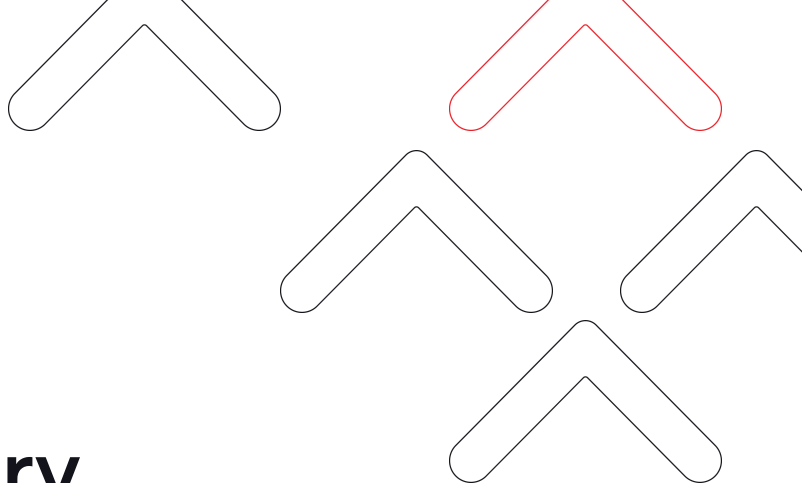
# TABLE OF CONTENTS

<b>List of Abbreviations</b>	<b>6</b>
<b>Executive Summary</b>	<b>7</b>
<b>Introduction</b>	<b>9</b>
Methodology	10
The Rise of Internet Usage by Human Rights Defenders	11
The Rise of State Surveillance	14
<b>The Adoption of Counter-surveillance Technology</b>	<b>16</b>
Online Security Threats Faced by Changemakers	16
Existing Security Measures Adopted by Changemakers	21
<b>Factors Shaping the Adoption of Security Measures</b>	<b>27</b>
Lackadaisical Attitudes Towards Security Tools	27
Segmentation Between Popular and Security Tools	29
Cultural and Language Barriers	31
Limited Resources	32
Financial Resources	32
Human Resources	33
Digital Infrastructure	34
<b>Recommendations</b>	<b>35</b>
<b>Conclusion</b>	<b>37</b>
<b>Bibliography</b>	<b>39</b>



# LIST OF ABBREVIATIONS

<b>COVID-19</b>	Coronavirus Disease 2019
<b>CSO</b>	Civil Society Organisation
<b>DDoS</b>	Distributed Denial of Service
<b>FGD</b>	Focus Group Discussion
<b>HRDs</b>	Human Rights Defenders
<b>IFJ</b>	International Federation of Journalists
<b>INGO</b>	International Non-governmental Organisation
<b>IP</b>	Internet Protocol
<b>IT</b>	Information Technology
<b>IPI</b>	Internet Penetration Index
<b>ISOC</b>	Internal Security Operations Command
<b>KIIs</b>	Key Informant Interviews
<b>LAN</b>	Local Area Network
<b>MFA</b>	Multi-factor Authentication
<b>OST</b>	Open and Secure Technology
<b>NGO</b>	Non-governmental Organisation
<b>PAHRA</b>	Philippines Alliance of Human Rights Advocates
<b>PGP</b>	Pretty Good Privacy
<b>POFMA</b>	Protection from Online Falsehoods and Manipulation Act
<b>TOC</b>	The Online Citizen
<b>VOD</b>	Voice of Democracy
<b>VoIP</b>	Voice over Internet Protocol
<b>VPN</b>	Virtual Private Networks



# Executive Summary

“Digital Security and Human Rights Defenders in the Asia-Pacific“ highlights the importance of adopting a multi-stakeholder approach to enhance digital security and address the online threats that changemakers currently face in the Asia-Pacific amid increasing state surveillance. Addressing online security threats is necessary since state surveillance threatens both the online and physical security of those advocating for human rights in the region.

The internet has become an essential tool for advocacy by changemakers. The online world has brought a range of positive developments, such as making instant communication to large audiences and access to a broader range of information sources possible. Yet, in this context, governments have also improved their digital skills and technical capacities to monitor the actions of changemakers. This is known as state surveillance and threatens changemakers as it infringes on privacy, restricts freedom of expression, and undermines civil liberties when conducted without proper legal oversight.

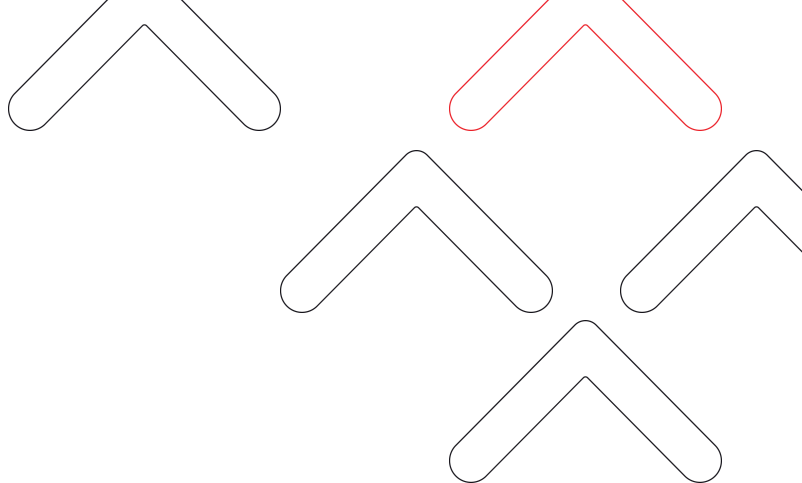
This report identifies three key digital threats jeopardising changemakers. First, increased government pressure on the changemakers’ actions, particularly on those trying to hold government officials and policies accountable. Various Asian-Pacific governments use legal frameworks and strict regulations to limit the (online) freedom of human rights defenders. Second, the interception of digital communications by state authorities using sophisticated spyware to monitor the activities of changemakers. This surveillance can lead to harassment, intimidation, and offline threats against changemakers, fostering a climate of self-censorship and fear.

Third, information operations and warfare like patriotic trolling undermine the work of activists and human rights groups, particularly members of gender and sexual minorities.

Changemakers have responded to these threats in three ways: by conducting assessments to evaluate the security system of their online infrastructure, by increasing ownership of their digital infrastructure, and by adopting more secure software. Nonetheless, responses to these threats are not uniform among changemakers. The report identifies several barriers to the effective and widespread adoption of security tools to increase online security. First, the scepticism shown by some changemakers towards safe tools is driven by factors like financial constraints and the age gap between changemakers. Second, the general public, and even some changemakers, make use of less secure software and free online platforms to reach mass audiences. Third, cultural and language barriers usually affect those with limited English proficiency. Finally, limited human, technical, and financial resources hinder the creation of a safer digital infrastructure.

The report concludes with a set of recommendations for changemakers, INGOs, donors, and technology companies to address key challenges that limit the effective implementation of digital security tools and protocols. This report advocates that a multi-stakeholder approach is the most effective way to address digital threats faced by changemakers, thus reducing the online risks faced in the Asia-Pacific when advocating for human rights.





# I.

## Introduction

In the Asia-Pacific, civil society actors like human rights defenders (HRDs) and civil society organisations (CSOs) in the field of human rights - also referred to as changemakers in this report - face significant challenges in their advocacy work to promote people's rights. This has become particularly evident in the digital age, where governments' skills and technical capacity to monitor their actions have increased drastically in the last decade, jeopardising human rights and democratic systems across the region.

Changemakers are key actors in addressing a wide range of civil liberties and political rights violations to bring about positive social change. They operate individually or collectively and are usually driven by their commitment to social justice. Changemakers work on a wide range of issues, including gender-based rights violations, the rights of indigenous peoples, and human trafficking, to name a few examples. In doing so, they employ diverse techniques like monitoring and documenting human rights violations to call out for action against such violations, supporting victims, holding public officials accountable, supporting better governance, contributing to the implementation of international human rights treaties, and promoting human rights education and training (Special Rapporteur on human rights defenders, n.d.).

In the digital age, the internet enabled changemakers to increase the impact of their advocacy tasks through a range of new communication mechanisms and strategies. However, the popularisation of digital tools also exposed changemakers to the scrutiny of government officials, compromising their online presence and physical integrity and, overall, making their tasks more challenging.

Furthermore, changemakers do not always possess the necessary skills to fully benefit from digital security tools and practices. This has further threatened their integrity and safety, online and offline.

Against the backdrop of state surveillance, this report highlights how changemakers have responded to security threats and attempted to increase their safety in the digital sphere. First, the report frames state surveillance as a threat to changemakers in the internet age, where digital media and tools are vital for effective and efficient advocacy. Then, it identifies the most common security threats changemakers face and what measures they have taken to increase their safety online. Furthermore, the report also outlines a series of challenges that changemakers face when adopting digital security measures. Finally, the report includes a set of recommendations for changemakers, INGOs, donors, and technology companies to increase online security and ensure that changemakers can maximise the potential of digital tools for advocacy purposes.

## 1.1. Methodology

The research for this report was carried out in two stages, following a qualitative approach to delve into underexplored reasons that challenge online security for changemakers and the measures they are taking. The first stage involved desk research to conceptualise the study, narrow down the topic, and identify knowledge gaps regarding changemakers and digital technologies in the Asia-Pacific. The research team analysed secondary sources including reports from international organisations, tech companies, tech and human rights activists, and news reports to identify areas where knowledge was lacking.

The second stage involved generating, collecting, and analysing primary data to address the knowledge gaps identified during desk research. The research team conducted seven key informant interviews (KIIs) with relevant stakeholders from the countries included in the study: Cambodia (1 online interview conducted in English), Indonesia (2 interviews conducted onsite in Bahasa), Myanmar (1 online interview in English), Philippines

(1 online interview in English), Singapore (1 online interview in English), and Thailand (1 online interview in English).

Additionally, five focus group discussions (FGDs) were conducted: two in Indonesia, one in Bangladesh, one in Thailand, and a regional one as part of EngageMedia's Asia-Pacific Digital Rights Forum, which took place from 12 to 14 January 2023. Informants for the KIs and FGDs were identified through the networks of Asia Centre and EngageMedia and selected because of their expertise and experience in the intersection between human rights advocacy, digital media, and the usage of digital security tools. KIs were conducted because of their ability to provide deep insights regarding digital security, tapping into the personal experience of individuals, thus complementing the data from desk research with rich contextual information. The FGDs allowed for the inclusion of a diversity of participants in the research, encouraging idea generation, and complementing the outcomes from desk research.

## **1.2. The Rise of Internet Usage by Human Rights Defenders**

The internet has been widely popular across South and Southeast Asian countries since the onset of the 2000s. The internet penetration index (IPI) measures the level of internet adoption in a specific geographic area. This metric is helpful to make comparisons between regions and see the evolution of the spread of the internet. Below, Table 1 shows the internet penetration index in the relevant countries for this report in the years 2015 and 2023.

Table 1: Internet Penetration Index (IPI) in 2015 and 2023

Country	Internet Penetration Index	
	2015	2023
Bangladesh	26%	38.9%
Cambodia	25%	67.5%
Indonesia	28%	66.5%
Myanmar	5%	44%
Philippines	44%	73.1%
Singapore	81%	96.9%
Thailand	54%	85.3%

(We Are Social, 2015; We Are Social, 2023a,b,c,d)

Two trends can be observed: first, the IPI has increased in all countries included in this report. Second, the table shows that there are remarkable differences between countries in 2023.

The increase in internet usage across the Asia-Pacific has shaped the political landscape (Anduiza et al., 2009) with a plethora of benefits for citizens and changemakers. Many citizens gained affordable access to a wide range of information sources (Lewis, 2021), which empowered them with knowledge extending beyond government-controlled sources or mainstream media outlets (Paladino, 2018). Consequently, many individuals have been able to promptly express their views and concerns regarding issues that impact their rights, particularly in authoritarian countries (Ghonim, 2012). A noteworthy illustration of this is the 2013 general election in Cambodia. Social networking sites such as Facebook played a prominent role in reshaping social and political dynamics, facilitating public discussions on political matters and encouraging greater direct participation of the public in political processes (Kimseng, 2014).

The popularisation of the internet also altered the work of changemakers, reshaping advocacy and outreach strategies. As stated by the Internet Society (2015), "although the original architects of the Internet did not intentionally conceive it as a tool to advance human rights, the principles embedded in its design embody a vision of borderless, end-to-end communication." The internet facilitates collaboration between changemakers nationally and internationally (European Parliament, 2010), making resource-sharing and connections at a global level easier (Urbinati & Kim, 2017).

In this context, the internet made the documentation and collection of evidence of human rights violations easier. Changemakers' ability to quickly collect and disseminate evidence emerged as a strategy to hold rights violators accountable for their actions (GeSI, 2018; Kinpeng, 2020). Furthermore, the online sphere has facilitated the creation of campaigns, petitions, and the arrangement of protests, thus providing a platform to amplify changemakers' voices and advocate for change (Ng Wei Kai, 2022; Youngs, 2018).

The COVID-19 pandemic further entrenched technology in the work of changemakers, as physical interactions have largely migrated to cyberspace (Robinson, n.d). As a result, human rights defenders rely more than ever on digital technology in various aspects of their work, including the recruitment of staff and volunteers (NonprofitHR, 2022).

Although the development of the digital sphere has created numerous opportunities for changemakers, several challenges and threats have also emerged. The next section examines state surveillance as a major obstacle to advocacy work that tries to advance human rights.

### 1.3. The Rise of State Surveillance

The growing incidence of cyberattacks and state surveillance aimed at changemakers has become a challenge in the Asia-Pacific. These cyberattacks can disrupt their work and steal their data, which can put their physical safety at risk. Furthermore, state surveillance can also be used as an intimidatory strategy to deter changemakers from doing their work and undermine their credibility.

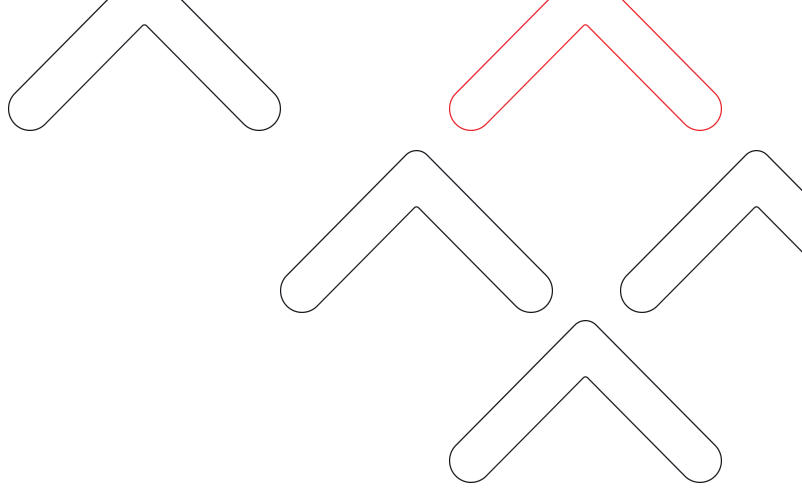
In 2021, state surveillance ranked as the fourth most common human rights violation in the Asia-Pacific ([Frontline Defenders, 2022](#)). Notably, Pegasus, a spyware software developed by the Israel-based NSO Group, has been used covertly to infiltrate the smartphones of HRDs, enabling monitoring of their activities ([Shankland, 2022](#)). In Thailand, the government admitted to using Pegasus in July 2022 to spy on journalists, activists, and dissidents ([Scott-Railton et al., 2022](#)). The government claimed that the use of Pegasus was necessary for national security, but critics counter that it was used to silence dissent ([Reuters, 2022a](#); [Reuters, 2022b](#)).

Pegasus has also been used against changemakers in Malaysia to target at least ten people in September 2021, including politicians, journalists, and human rights activists. The Malaysian government denied any involvement, but concerns were raised about the government's commitment to human rights and freedom of expression (Feldstein & Kot, 2023). According to a report by IndonesiaLeaks, Indonesian state agencies have been accused of using Pegasus to conduct phone surveillance on politicians and activists. The spyware reportedly entered the country in 2018, when Minister Sakti Wahyu Trenggono, who was part of Indonesia's current President Jokowi's campaign team in 2019, allegedly used it for political purposes. While the police denied the accusations, government officials refrained from commenting. Like the previous examples, investigations have also shown that Bangladesh acquired Israeli surveillance equipment in 2018 to track the phones of HRDs ([Al Jazeera Investigative Unit, 2018](#); [Ljubas, 2022](#)).

State surveillance has further implications for the work of changemakers. One of the primary worries regarding a cyberattack includes potential harm or disruption to essential infrastructure, reduced productivity, expenses incurred from hiring external consultants and specialists, or the possibility of facing regulatory penalties or legal actions ([Ongsakul, 2023](#)). Furthermore, some activists may be discouraged from continuing their work due to the risks associated with surveillance, while others reduce direct interaction with the public ([Frontline Defenders, 2021](#)).

Spyware not only poses a threat to digital security but also leads to physical harassment. In Southeast Asia, online monitoring is often followed by physical assaults ([Root, 2022](#)). For example, in Indonesia, authorities hacked the devices of HRDs and posted provocative content to justify their detention ([Forum-Asia & Kontras, 2021](#)). On the changemaker's dimension, those under surveillance are often isolated from their acquaintances due to fears of harm or monitoring ([Fataffa & Front Line Defenders, 2022](#)).

In summary, the internet has afforded changemakers with opportunities to advocate for and improve human rights, but it has also brought significant challenges, particularly the rise of state surveillance. This has subjected many changemakers to scrutiny by government officials, resulting in online and physical harassment aimed at impeding their advocacy efforts. Consequently, digital security tools have become increasingly important in mitigating the impact of state surveillance. The following chapter outlines the main security threats identified by informants and the measures they have taken to safeguard themselves.



# II.

## The Adoption of Counter-surveillance Technology

State surveillance contributes to creating a challenging environment for changemakers to advocate for civil and political rights. This chapter identifies several security threats faced by changemakers and analyses the security measures they adopt.

### 2.1. Online Security Threats Faced by Changemakers

Changemakers in the Asia-Pacific often face security threats due to the nature of their work, which involves keeping state officials and policies - often in semi-authoritarian and authoritarian regimes - accountable or confronting the interests of influential individuals and entities. In this section, changemakers highlight key threats impeding their advocacy work: the government's use of repressive legal frameworks, interception of digital communications, and state-sanctioned information operations and warfare. These concerns underpin the analysis of how HRDs utilise digital technologies to mitigate these threats in 2.2.

#### 2.1. 1. Government Pressure on Changemakers

Informants explained that government officials in many countries in the region often exert their influence and compel changemakers to cease their activities. In Cambodia, where the Cambodian People's Party and Prime Minister Hun Sen are politically hegemonic, changemakers who question the legitimacy of government officials and policies, or attempt to keep them accountable, risk putting themselves in jeopardy.



Voice of Democracy (VOD), one of the last independent media outlets in the country, received several warnings due to the nature of some of its content. In February 2023, Hun Sen issued an order to revoke its licence to operate, alleging that one of their publications had harmed the government's reputation. Consequently, VOD was compelled to cease broadcasting (Ng, 2023). Following this incident, the Cambodia Center for Independent Media, the organisation behind VOD, reported that their website and Facebook page were inaccessible (Interview 04).

A similar example can be found in the Philippines. In 2020, the government ordered the country's largest broadcast network, ABS-CBN, to stop broadcasting after its licence expired. Although Congress grants broadcasting rights and licences, lawmakers allied with then-President Rodrigo Duterte. They refused to act on bills seeking ABS-CBN's licence renewal due to its critical coverage of the government's political issues, including the war on drugs. In 2023, under the presidency of Ferdinand Marcos Jr., ABS-CBN's licence to broadcast on free public channels in the Philippines remains revoked. Meanwhile, many of its regular broadcasting frequencies have been handed to other media outlets. Like VOD in Cambodia, this case raised concerns over systematic attacks on freedom of speech with the government's pressure over media outlets (Lo, 2020).

In Singapore, the intersection between physical and digital security threats is evident, as seen in how the country's legal provisions allow state authorities to investigate suspected individuals, including changemakers, and seize their devices (Interview 2). In its latest report, Asia Centre (2023) flags that the country's legal provisions have been systematically used to target and silence changemakers attempting to keep government officials and policies accountable, thus limiting the space for free discussions on political issues. This includes strict regulations set out for changemakers who work online, such as the Broadcasting Act, which provides state agencies authority over which content can be shared over the internet and the power to revoke the licence to operate online platforms. Similarly, the fake news law (Protection from Online Falsehoods and Manipulation Act; POFMA), allows the government to control the sharing of content online, justifying the action based on the content being false or misleading.

On the other hand, state authorities have been remiss in acting on accounts harassing such individuals for their work through acts like hate speech and death threats. Together, these create a culture of self-censorship among changemakers in Singapore.

### **2.1.2. Interception of Digital Communications**

One informant noted that government authorities have upgraded their technical skills and capacity to gather data about changemakers' operations from their digital communications (Interview 3). This is happening even though the United Nations recognises the need to ensure that HRDs are protected against surveillance as it can lead to harassment, intimidation, and violence ([UN General Assembly, 2016](#)).

Changemakers in Thailand have consistently raised their concerns regarding online state surveillance translating into offline threats like intimidation of their relatives or forced disappearances ([TLHR, 2022](#)). Although it is a recent phenomenon in the country (FGD 02), it has intensified since the 2014 coup, driven by the government's use of increasingly sophisticated software to monitor changemakers. From October 2020 to November 2021, during the peak of pro-democracy protests, approximately thirty activists, academics, lawyers, and NGO workers were targeted by Pegasus spyware ([AFP, 2022](#)). In 2020, Wanchalearm Satsaksit, a Thai pro-democracy activist living in exile in Cambodia, was abducted by armed men while on a call with his sister and has not been seen since. His disappearance was linked to a pattern of exiled activists disappearing since Thailand's 2014 coup that targets those who criticise the Thai government and military, particularly in the online sphere ([Wright & Praithongyaem, 2020](#)).

Before the military takeover in Myanmar in February 2021, ex-military officials at the civilian Ministry of Transport and Communications ordered telecom and internet service providers to install intercept spyware, according to one industry executive. This technology would allow the military to eavesdrop on citizens' calls, view text messages, track users' locations, and monitor web traffic without the assistance of the service providers.

The intercept spyware was part of the military's efforts to exert control over the internet, suppress protests, and keep tabs on political opponents. Industry executives revealed that the orders were presented as coming from the civilian government, but the military was expected to have control, leaving no room for refusal ([Potkin & McPherson, 2021](#)).

These examples of state surveillance pose a dual threat to changemakers. First, it enables state authorities to monitor the digital footprint of changemakers, making them vulnerable to harassment. Second, it creates a state of paranoia among HRDs, leading to a chilling effect that gradually erodes their spirit and ultimately results in self-censorship ([Pinol Rovira, 2021](#)).

### **2.1.3. Information Operations and Warfare**

The government's deliberate use of information and communication technologies to influence opinions, spread propaganda, and achieve strategic goals domestically and internationally was also pointed out as a significant threat to the security of changemakers (Interview 01, 05). In Thailand, state-backed online disinformation has threatened the legitimacy of changemakers. These operations involve smear campaigns orchestrated by either military actors or the Internal Security Operations Command (ISOC), targeting local CSOs and INGOs that advocate for human rights, particularly issues related to freedom of expression and assembly ([Asia Centre, 2023](#)).

In Indonesia, local CSOs acknowledge that their work exposes them to online and offline threats and attacks, including intimidation, stalking, ransomware, digital impersonation, social media hacking, doxing, office raids, criminalisation, and persecution (FGD 03, 04). Indonesian independent media outlet [Konde.co](#) faced a cyber-attack following the publication of an article on sexual harassment within the Indonesian Ministry of Cooperatives and Small Medium Enterprises. The attack, a Distributed Denial of Service (DDoS) incident, overloaded the website and made it inaccessible.

This is the second attack on Konde.co after publishing articles on sexual violence. Journalists and media outlets in Indonesia have faced similar digital attacks in recent years, which the International Federation of Journalists (IFJ) and Indonesian journalist unions have condemned ([IFJ, 2022](#)).

In the Philippines, state agencies have shifted from using physical threats, such as photographing activists and HRDs or surveilling them, to employing internet-based strategies to undermine their work. A notable example is the deployment of patriotic trolling to portray government critics and CSOs as "traitors" who are funded by the West, thereby undermining their legitimacy ([Sombatpoonsiri, 2018](#)). In the Duterte era, "keyboard armies" largely consisted of President Duterte's supporters who allegedly received payment to engage in similar tactics. This cyber trolling exacerbates social divides and contributes to the shrinking of civic space. Former President Duterte and his supporters created a narrative to portray his anti-drug campaign as a patriotic effort to "clean up" the nation. Online bullies mimicked Duterte's offensive language to target those critical of the government. Several human rights defenders, including journalists from critical news outlets like Rappler, received online threats while cyber-trolls, some allegedly using fake accounts, spread propaganda to attract genuine Duterte supporters and accused human rights groups of being anti-Filipino. This tactic was used to silence critics and discredit rights-based arguments (*Ibid.*).

It is worth noting that many of the attacks listed in this section specifically target members of gender and sexual minorities. The VOD closure in Cambodia also provides an example of gender-based harassment, which is amplified through social media. Shortly after VOD was shut down, the female reporter who wrote the article that triggered this case received abusive and misogynistic language from numerous internet users. ([ANFREL, 2023](#)). Cases from Indonesia also demonstrate that threats disproportionately burden women and LGBTQI+ individuals, particularly when their gender and sexual identity become known (FGD 03, 04). Informants also noted that awareness of gender-based attacks remains primarily at the individual level rather than the organisational level, indicating a limitation in awareness and safeguards.

The threats outlined above illustrate the challenges that changemakers and members of CSOs face in their daily lives. Nonetheless, these threats are contextual and not all changemakers experience all of them or in similar forms (Interview 01). Still, given the nature of their work and the developments in the digital sphere, various participants acknowledge that achieving a completely threat-free environment is realistically impossible. Hereby, these participants imply that changemakers will always be exposed to some threats, either in the digital sphere or the offline world, even if security measures are in place (Interview 02, FGD 02).

## **2.2. Existing Security Measures Adopted by Changemakers**

In this section, the report looks at some of the measures that changemakers have taken to adapt to the increasing threats in the online sphere and their associated challenges. Three specific security measures will be discussed:

1. security assessments;
2. increased ownership over online connections;
3. the use of secure software.

### **2.2.1. Security assessments**

Conducting regular security assessments is critical as this involves identifying gaps in protecting against online and physical threats and ensuring compliance with the best practices of digital safety. A security assessment may involve doing a risk analysis, conducting simulated attacks, and reviewing security measures and policies, as well as assessing employee awareness of digital threats and security.

Primary data from interviews revealed that technical capacity and resources, mostly financial, are the key factors that determine whether or not changemakers conduct security assessments. The examples provided show that the difference between changemakers who can conduct security assessments and those who do not is significant in relation to the prevention of online threats.

One informant (Interview 2) explained that he is aware of INGOs operating in the Asia-Pacific that have the means to conduct risk assessments and security check-ups regularly, as well as providing a 24/7 digital security helpline that operates globally. The helpline team has received security and technical requests from HRDs around the world and has also guided their team members (Interview 02).

One informant from Cambodia explained that some media outlets have dedicated technicians who assess cybersecurity risks for their organisations. They provide support to local CSOs facing risks and send security alerts to colleagues (Interview 04). Another representative from a Thailand CSO said that their organisation has an IT team responsible for ensuring that all staff members have the latest security tools installed on their devices. The IT team also provides training on how to use these tools. In the event of reported device hacking, the IT team conducts a basic check-up and takes precautionary measures such as password changes (FGD 02).

Nonetheless, not all organisations or changemakers conduct security assessments regularly. The main reason is not having a dedicated IT team to handle digital security issues. In such circumstances, when technical issues related to digital security arise, staff members have to navigate the problem themselves and find the most appropriate solution without the expert assistance of a technical support team (FGD 02). This perpetuates the limited knowledge that many CSOs have regarding cybersecurity. In the Philippines, Human Rights Online Philippines (HROnlinePH) and the Philippine Alliance of Human Rights Advocates (PAHRA), in partnership with other CSOs, have been conducting awareness-raising and training sessions on digital security and digital rights. The training covers topics such as physical security, well-being, and stress management. Data from another interview also revealed that some changemakers are often unaware that frontline defenders can conduct security audits (Interview 01).

### 2.2.2. Increased Ownership Over Online Connections

Gaining greater control over the data shared via online means was a security measure mentioned by informants. Data from interviews and FGDs identify two strategies changemakers have adopted to increase security and privacy: owning their servers, whether it be an in-house physical server or a dedicated server rented from a hosting provider, and using local area networks (LAN).

Changemakers have increased their online protection by relying on their own servers to store, process, and deliver information or data requested by clients. Several respondents reported that they have moved away from free cloud-based services (FGD 03). The rationale behind this is to exert greater control over their data and online communications by storing it within their organisations, allowing changemakers to have better control over data backups and, overall, increase their protection against attacks or interference within their digital systems.

A human rights organisation in the Philippines (Interview 01) explained that its members have considered adopting Matrix, a decentralised communication protocol for secure, real-time messaging and Voice over Internet Protocol (VoIP) communication. Matrix uses a federated model with multiple home servers communicating to share messages and user data. Users are identified by unique Matrix IDs, and communication happens in rooms, either public or private. End-to-end encryption ensures message privacy, and Matrix bridges allow integration with other communication platforms. Various clients are available to access the Matrix network, providing a unified and user-centric messaging experience. Initially, the Philippines-based organisation planned to implement it within their office and gradually extend it to other offices, aiming for a secure, end-to-end encrypted server that can be easily abandoned if needed.



The second security strategy identified by a respondent from Cambodia is the use of LAN networks instead of Wi-Fi connections (Interview 04). Wi-Fi and LAN connections are safe options but require maintenance. They must be configured and maintained properly. Regarding physical security, LANs are considered safer options since potential intruders need physical access to the network to obtain data. Wireless connections, on the other hand, can be accessed without authorisation remotely. There are also remarkable differences between the two types of connections in terms of data encryption. LAN networks manage authentication and access control at the device or user level, while wireless networks rely on access points and may have potential vulnerabilities if not properly configured (Froehlich, 2022).

Informants from Indonesia (FGD 03) also mentioned that “traditional” security measures such as the use of security cameras are still in place to protect their online data. Cameras are strategically placed around their offices to deter and monitor any attempt to access online data and technical equipment. Other Indonesian FGD participants mentioned that they don’t store certain data online at all, instead keeping sensitive data stored within USB flash drives only.

The aforementioned examples flag changemakers’ perceptions of security as an important element to be considered. Some changemakers have opted to use their own servers as opposed to relying on cloud services. Furthermore, some have been increasingly relying on LAN connections instead of wireless connections. Nonetheless, cloud servers and Wi-Fi connections are also safe options - each of these options comes with advantages and disadvantages. Yet, data from our FGDs suggests that being in more direct control of the security measures - such as by having one’s own servers and wired connections - positively influences changemakers’ perception of security.



### 2.2.3. The Use of Secure Software

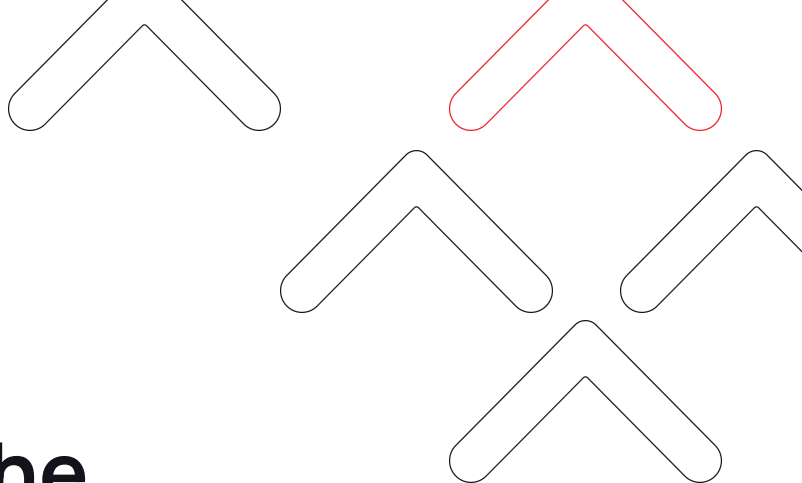
Another measure to mitigate digital risks is the adoption of secure communication software or applications that offer more sophisticated safety features. One such application mentioned by two respondents (Interviews 01, 03) is ProtonMail, a Swiss-based email service. Although ProtonMail is a popular option for changemakers in the region, they also noted that it can be less user-friendly compared to services like Gmail. Additionally, certain features, such as expanded email and file storage, require payment (Interview 01, 03). ProtonMail stands out because of the security measures it offers, prioritising user privacy and security. Unlike many email services that collect personal data, ProtonMail doesn't collect such information; it offers anonymous sign-ups and does not log IP addresses. Users can enjoy complete anonymity. Additionally, the paid plans allow anonymous or decentralised payment methods like Bitcoin. ProtonMail claims to provide robust security features, including end-to-end encryption, which prevents anyone, including ProtonMail itself, from reading users' emails. The service also offers address verification to ensure emails reach the intended recipients ([Proton, n.d.](#)).

Another widely used application among HRDs is Signal, a privacy-focused messaging app known for its end-to-end encryption, minimal collection of user data, and non-profit foundation structure. Compared to WhatsApp and Telegram, Signal stands out due to the privacy and security options it offers. It has gained popularity among the general public, making it a preferred platform for daily communication. In addition to sending messages, CSOs also express comfort in using Signal for sharing documents and disseminating sensitive information. However, some individuals mentioned it was difficult to use at first. It required time to become familiar with the application (Interview 03). It must be noted that as Signal is connected to a phone number, it is not completely anonymous.

Virtual private networks (VPN) are another type of software that changemakers use frequently to increase their security online (Interview 02). A VPN enhances online privacy by establishing a secure tunnel between a user's computer and the VPN server. This effectively hides their online activity and location while encrypting data to prevent unauthorised access ([Matthews-Ela et al, 2022](#)). The main barrier to using VPNs is cost, as these usually require a paid subscription. Although some respondents indicated that they share their login information with multiple users, one respondent remarked that VPNs are impractical and unsustainable (Interview 02). Informants from Myanmar also reported that VPNs are not always accessible due to bad internet connections, especially in remote areas (Interview 03).

Local CSOs also mentioned the use of LastPass, a password manager, to enhance the security of their passwords. LastPass generates highly complex and secure passwords for accounts, helping protect CSO staff's passwords in several ways. Firstly, it creates passwords that are difficult to decipher. Secondly, it discourages the practice of saving passwords in insecure locations such as local PCs or internet browsers (FGD 02).

Informants also mentioned Pretty Good Privacy (PGP) to increase their safety (FGD 03). PGP is a type of digital tool used for encryption and decryption of electronic communications. It provides a method for secure communication, ensuring that only authorised recipients can access the contents of the encrypted message. It is widely used for email encryption, file encryption, and secure data transmissions over the internet. It relies on public-key cryptography, where each user has a public key for encryption and a private key for decryption, making it a popular choice for securing sensitive information and maintaining privacy ([Kost, 2023](#)).



# III.

## Factors Shaping the Adoption of Security Measures

As shown in the previous section, numerous changemakers have adopted new hardware, software, and perspectives concerning digital tools and media to enhance their digital security. However, informants have identified several challenges linked to the use of these technologies. This chapter outlines four of these challenges and discusses how they hinder the implementation of security measures in digital environments.

### 3.1. Lackadaisical Attitudes Towards Security Tools

Overall, participants in interviews and focus group discussions expressed a certain indifference towards the adoption and use of security tools in their advocacy tasks (FGD 01). Three reasons explain why this is the case: effort and time to adopt and use them, the existence of an age gap, and conformity. Together they emerged as remarkable hurdles that hinder the full potential of security tools in protecting changemakers performing their advocacy duties.

Some changemakers expressed that embracing security tools is a daunting task that involves significant time investment (FGD 00). This perception can be linked to a key point made earlier: the lack of financial and technical resources to adopt security tools (FGD 03). Some changemakers, particularly those with limited resources, often lack a dedicated team of IT experts or colleagues who are capable of implementing security tools effectively and efficiently.

As a result, some changemakers might be hesitant to adopt these tools as they perceive them as complex and foresee a steep learning curve, which translates to a time-consuming process. Additionally, technological advancements occur at a rapid pace, making it increasingly challenging for changemakers with limited resources to invest the necessary amount of time to upgrade their protection system.

The generational gap was also pointed out as a factor impacting changemakers' scepticism towards the adoption of security tools. Younger generations are often referred to as digital natives - those who were born in the digital age. They are likely to feel more comfortable with technology, thus being more agile in incorporating security measures into their devices. On the other hand, older changemakers tend to have lower levels of digital literacy. Although this does not mean that they cannot use digital technology, their ability to do so tends to be more limited.

Some CSOs in Thailand believe that their security measures are sufficient and they do not require better security tools. They argue that their organisations have implemented necessary security measures, followed protocols, and utilised the available tools (FGD 02). Conformity is linked to the impracticality mentioned by some respondents in using security measures. One participant mentioned that implementing multi-factor authentication in the field is "impractical" (FGD 02) due to the time and effort it requires to log into accounts which results in some of them disabling these measures. CSOs in Indonesia have adopted alternative protocols such as regularly renewing passwords for online accounts and using licensed operating systems. Instead of using cracked versions, they choose to purchase the original Microsoft Office and invest in antivirus applications (FGD 00). In Cambodia, CSOs have changed their behaviour by turning off their phones and GPS while travelling to prevent tracking and ensure their security (Interview 04).

However, changing behaviour to adopt more secure protocols is not an easy task. Some CSOs find following security protocols tedious and burdensome. Nonetheless, having the right mindset to transition to increasingly digitally safe working practices is important for CSOs that intend to improve their online safety. As emphasised by a key informant:



No matter how sophisticated the technology is, if the behaviour has not changed, the vulnerability remains.

FGD 03

## 3.2. Segmentation Between Popular and Security Tools

The lack of integration between security tools and mainstream applications (those used by the general public) poses another challenge to the adoption of security measures by changemakers. Many changemakers do not use security tools to the extent that they would like to because the general public does not use them, complicating collaboration between the two. As a result, changemakers are compelled to resort to mainstream tools to facilitate cooperation. Unlike mainstream applications, which offer more integration possibilities with other software, applications designed with security as their key priority tend to have limited functionalities in this regard.

In some cases, changemakers face challenges in using encryption features because their contacts lack access to such tools (Interview 02). The fact that senders can consequently not read or access the information sent shows that security apps often do not cater to their partners and networks. Even if CSOs can afford secure versions of these tools, they may struggle to use them effectively as these applications require a large user base to be fully functional. When an application is new or has fewer users, it can be difficult to attract people to use it, creating a loop that challenges those using these more secure applications (Interview 02).

As a result, many changemakers are compelled to rely on less secure communication channels commonly used by their colleagues and partners to facilitate communication (FGD 02).

For example, respondents from the Philippines explained that some changemakers avoid using less secure messaging applications like Facebook Messenger, Telegram, or Viber. However, these applications are highly popular among the masses. Furthermore, some internet service providers offer data packages allowing users to use them for free. Therefore, many people tend to opt for these applications instead of more secure alternatives due to financial constraints and pragmatism (Interview 01). In these cases, changemakers adopt other strategies to increase their digital security, such as password protection (using complex and unique passwords, for example), multi-factor authentication (MFA), and verification processes (FGD 00; Interview 05).

This poses a challenge for changemakers who rely on multiple programmes to accomplish their advocacy goals. In their efforts to reach out to the masses, it is not uncommon for CSOs to encourage their staff to use less secure mainstream applications. Organisations see this trade-off as necessary to ensure smoother collaboration and data sharing between actors (FGD 00). Some participants in the Indonesia focus group (FGD 03) exemplified this with WhatsApp. The aforementioned fragmentation has played a key role in making some CSOs reluctant to stop using WhatsApp and switch to more secure messaging applications because other actors, like their partners and colleagues, continue to use WhatsApp.

Most social interactions are deeply ingrained in these free-to-use, commercial applications, making it challenging to transition to another platform. Therefore, as long as high-security programs remain fragmented from widely used mainstream alternatives, the full potential and benefits of comprehensive security measures may not be fully realised in various organisational contexts.

### 3.3. Cultural and Language Barriers

Language is seen as a significant hurdle by changemakers when it comes to adopting security tools. Most security tools and applications are in English, catering to a global user base. Although English language proficiency is improving in the region, changemakers' English fluency cannot be taken for granted. The educational divide that still prevails in many Asia-Pacific countries has implications for changemakers' work. For example, informants from the Philippines explained that in the country's largest island of Luzon, changemakers tend to have higher levels of education, including English language skills. On the one hand, this allows them to use security tools in English more easily. On the other hand, this puts them in a position of advantage compared to other changemakers in more remote areas, where English language proficiency tends to be lower (Interview 01).

Respondents from Bangladesh also expressed concerns about the fact that local changemakers often face difficulties in using security applications due to language barriers (FGD 01). Other informants added that the language barrier hinders digital security training. A representative from a CSO in Thailand (FGD 02) noted that most security training is conducted in English, which exacerbates the differences between those with a good command of this language and those whose abilities are limited or non-existent. It is worth noting that some localisation efforts already exist to improve the impact of digital security in Southeast Asia. Localisation efforts focus on the creation of resources in the local language of each country to better suit the needs of local changemakers ([EngageMedia, 2022](#)).

There are also cultural elements that play a significant role in determining whether changemakers in the Asia-Pacific adopt security measures. One of these factors is the organisational culture. Some respondents (FGD 00) pointed out that the prevailing organisational culture can discourage the use of security tools, hindering efforts to improve activists' security. For example, even if certain members of the organisations are knowledgeable about security tools, they may be reluctant to express their concerns or views about the organisation's security practices. This hesitancy is often rooted in the rigid hierarchical structure of many organisations. In such a context, employees fear that their input might be dismissed if their supervisors do not acknowledge security as a priority. This creates a situation where one individual might be aware of security flaws within the organisation - and might even be in a position to offer a solution - but remains silent to avoid a conflict.

## **3.4. Limited Resources**

### **3.4.1. Financial Resources**

Limited financial resources emerge as a major factor contributing to the low usage of digital security tools among CSOs and HRDs in the Asia-Pacific. Several respondents acknowledged that their organisations lack sufficient funds to provide these tools. The budgets for their projects do not cover expenses related to security tools (FGD 00; FGD 03). An interviewee further emphasised the limited allocation of budgets for security in their country office (Interview 05). Respondents from Dhaka noted that they request separate budgets from donors for project expenses, yet these exclude security purposes (FGD 01). Moreover, an interviewee pointed out that financial challenges extend beyond allocating a security budget within the organisation.



While their organisation receives funding from donors to offer VPNs to a limited number of individuals and budgets to purchase encrypted devices for HRDs, they lack the necessary financial resources to offer these services and tools to a larger network of individuals they work with (Interview 02). Additionally, while changemakers might afford basic precautionary measures, their means to detect if they are under state surveillance is also limited (FGD 02).

As the next section highlights, changemakers' limited financial resources is a problem that is closely tied to their human resources. Detecting state surveillance necessitates both human and financial resources (FGD 03). Due to limited budgets for creating a secure work environment, most organisations cannot hire IT specialists or staff (FGD 03).

### **3.4.2. Human Resources**

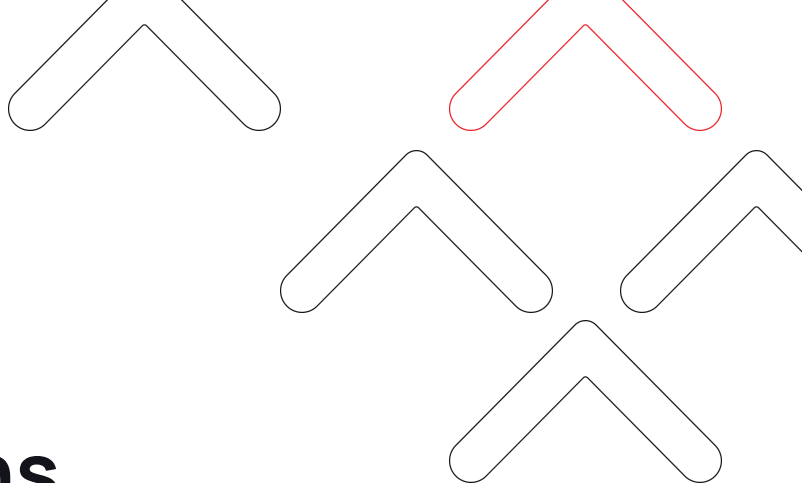
The limited adoption of security measures can also be attributed to a lack of IT specialists, experts, or staff. A representative from a CSO shared that their organisation only has one IT staff member who is responsible for various tasks, ranging from fixing printers to updating website content and practising security measures (FGD 03). In Thailand, there used to be a CSO that specialised in countering state surveillance and provided assistance to other local CSOs in preventing and detecting state measures. However, since the organisation became inactive, the Thai CSO community has been left without support (FGD 02). Human resources also play a significant role in the country office of an INGO located in Thailand. A representative explains that their organisation has experts based in London who work on security measures, but they can only provide general advice on behaviour and cybersecurity preparedness. The experts abroad cannot offer substantial assistance tailored to the local context (Interview 05). This point is further emphasised by a representative from another INGO, who highlights the need for a local help desk that truly understands the local context and can provide meaningful support. While INGOs can offer assistance, the bureaucratic nature of their operations often hinders their understanding of the specific local challenges (Interview 06).

IT experts or staff are expected to fulfil two primary roles for local CSOs and HRDs: providing security measures and offering capacity-building support. While CSOs may have access to security tools, they often lack the necessary IT staff to update security issues and maintain safety systems. This limitation hampers the effectiveness of the tools used by CSOs (FGD 00). In terms of capacity building, a representative from an independent media organisation in Cambodia acknowledges their limited knowledge of security measures and expresses the need for more support and training from technicians to enhance their proficiency in using digital security tools (Interview 04). The significance of security capacity building is also emphasised by CSOs in Bangladesh, who stress the necessity of acquiring security training to protect themselves from cyber threats and attacks (FGD 01).

### **3.4.3. Digital Infrastructure**

Issues concerning internet infrastructure have also contributed to the hindered adoption of security measures. First, limited access to the internet has profound implications for changemakers in remote regions. Although they are usually able to connect to the internet, connection speeds are low. This is illustrated in Myanmar, where informants explained that the speed of their connections poses a problem in using security tools effectively, even if these are available (Interview 03). Despite the availability and affordability of these tools, their performance is compromised, making it difficult for HRDs to implement robust security measures. Consequently, they may end up not using security tools, which might compromise the data that is shared online.

Second, inequality of access to the internet also poses a challenge. This is the case, for example, between Western and Eastern regions in Indonesia. In Eastern Indonesia, poor internet connectivity prevails due to the incomplete development of telecommunication infrastructure (FGD 03). This disparity in internet access between Western and Eastern Indonesia compounds the digital security challenges faced by activists and changemakers.



# IV.

## Recommendations

The report has highlighted how the rise of state surveillance has resulted in more digital threats affecting changemakers' efforts to protect and ensure human rights. Additionally, it has also shown that although most changemakers have adopted security measures against digital threats, many of them are not maximising what the available tools and mechanisms have to offer. Given these challenges, this report offers a set of recommendations for enhancing the digital security of changemakers.

### Changemakers should:

- Maximise their available resources to monitor and document all incidents related to their digital security, including offline implications. At a later stage, they should engage with INGOs and international organisations to report these security threats, as long as it is safe to do so.
- Create and engage in outreach opportunities - such as educational sessions, assemblies, and workshops - to increase awareness among other changemakers about the importance of adopting and, if necessary, increasing security measures, as well as creating new opportunities for the mitigation of security threats.
- Maximise the potential of the existing digital infrastructure by ensuring that it is properly configured against digital threats.
- Dedicate part of their existing financial, human, and technical resources to providing in-house security training, especially if their work takes place in more authoritarian regimes
- Cooperate with technology companies by providing their first-hand input about the challenges they face in adopting security tools, including their weaknesses, to contribute to the design of digital products with enhanced security measures.

### **INGOs should:**

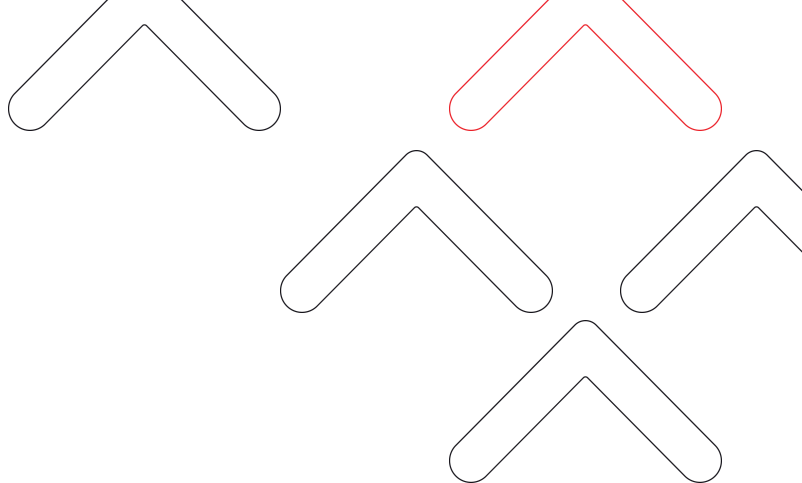
- Use their communication channels to report digital security violations and cases of state surveillance directly to international organisations and international human rights bodies.
- Contribute to the creation of regional networks that can become changemaker platforms for the exchange of experiences and protection measures related to digital security.
- Increase budget lines for digital security training, which should particularly focus on individual operators and organisations with the least amount of resources to implement the necessary digital infrastructure to protect themselves against digital threats.

### **Donors should:**

- Increment their digital security requirements when funding projects for CSOs and other changemakers as part of the risk assessment.
- Create dedicated programmes and budget lines for changemakers and CSOs to improve their digital security.
- Monitor the implementation of digital safety measures together with recipients to evaluate how to provide help more promptly.

### **Technology Companies and Application Developers should:**

- Make both digital security and user-friendliness a priority in the design of digital applications and hardware.
- Increase cooperation with changemakers so they can provide input to improve the design of safer software and hardware.
- Increase and support localisation efforts which ensure that security tools and software are made available in local languages.
- Offer training and seminars on digital security for CSOs and changemakers to ensure that they work in safe digital environments.



# V.

## Conclusion

State surveillance is challenging the activities of changemakers in the Asia-Pacific. Online security threats are increasingly making operations more difficult. Although many changemakers have adopted security measures to protect themselves against state surveillance and online threats, several hurdles persist.

The rapid development of the cybersphere and the widespread use of digital tools in the early 2000s reshaped the social and political landscape in the Asia-Pacific. This led to new opportunities for advocacy. The internet provided changemakers with instant access to information and increased ways to engage with their audience. However, this progress also brought challenges, as online state surveillance, through spyware like Pegasus, escalated. This increase in surveillance has made changemakers vulnerable to government scrutiny, endangering their digital safety and physical well-being.

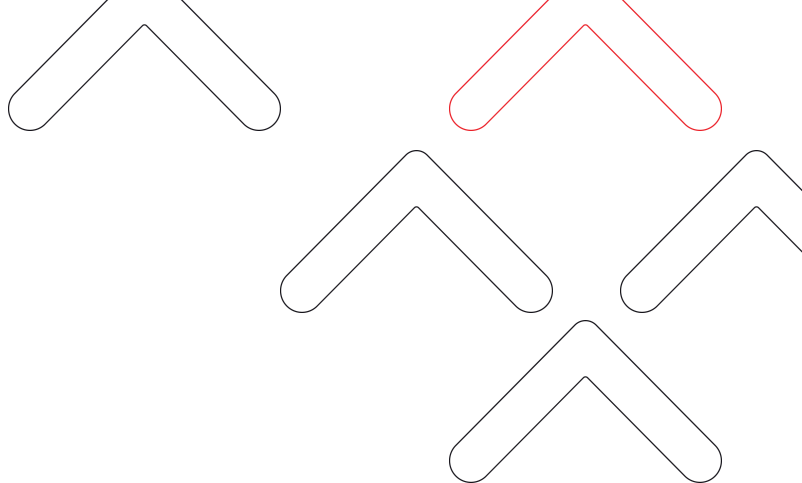
This report highlights three online threats faced by changemakers in the Asia-Pacific: increased government pressure through legal frameworks, interception of digital communications, and information operations and warfare. In response to these threats, changemakers have employed several strategies such as conducting security assessments, taking more ownership of their digital infrastructure (e.g., using wired connections), and adopting more secure software. However, barriers to the widespread adoption of security tools remain. There is scepticism among changemakers participating in this research due to financial constraints and the age gap between the so-called digital natives and the older generations.

The need to use less secure (and often free) platforms to reach a broader audience remains, while cultural and language barriers for those with limited English proficiency, and limited financial and human resources to create a safer digital infrastructure persist.

Moving forward, coordinated efforts with a multi-stakeholder approach are necessary to increase changemakers' capacity to implement effective responses against online threats. Efforts need to focus on two key challenges: limited resources to increase digital security and the relative lack of awareness around digital threats, both of which contribute to a non-optimal adoption of safety measures.

Changemakers play a key role in increasing awareness of existing digital security threats. Those with the skills and means should document and track cases of online security violations and report them to INGOs, if doing so is a safe option. This would allow INGOs to identify specific threats and trends which could be shared with other changemakers. INGOs should use their communication channels to gather cases of online threats directly from the local communities and condemn such actions using their own advocacy channels and through international human rights mechanisms. Additionally, INGOs should use their networks to convene changemakers from across the Asia-Pacific to create new solution-oriented learning opportunities to address existing digital threats. Given the financial constraints faced by several changemakers, donors hold the key to stimulating the allocation of resources towards increasing digital security. Financial resources could be allocated to improve digital infrastructures and for the hiring of qualified technical staff. Finally, more technology companies need to prioritise digital security. Through increased cooperation with changemakers, they could start designing software that better addresses their needs.

Through a multi-stakeholder effort, the digital security of changemakers in the Asia-Pacific can be increased. Without increased digital security, changemakers will continue to face obstacles in their advocacy duties and some might even stop their efforts or choose to self-censor. Creating increasingly digitally secure environments for changemakers is essential for the development of free and fair societies in the Asia-Pacific.



# Bibliography

Abdul Aziz, Mohd Nasiruddin et al. (2020) 'Preferred learning styles for digital native and digital immigrant visitors in the Malaysian Music Museum', Asia Journal of University Education, at: <https://files.eric.ed.gov/fulltext/EJ1274167.pdf>.

AFP (2022) 'Thai democracy activists targeted by Pegasus spyware: report', Bangkok Post, at: <https://www.bangkokpost.com/thailand/general/2348513/thai-democracy-activists-targeted-by-pegasus-spyware-report>

Anduiza, Eva, Marta Cantijoch & Aina Gallego (2009) 'Political participation and the internet', Information, Communication & Society, at: <https://www.dhi.ac.uk/san/waysofbeing/data/citizenship-robson-anduiza-2009.pdf>

ANFREL (2023) 'Joint statement: Media and civil society groups deeply disturbed by government's decision to revoke VOD's media license and the sexual harassment of a female reporter, at: <https://anfrel.org/joint-statement-media-and-civil-society-groups-deeply-disturbed-by-governments-decision-to-revoke-vods-media-license-and-the-sexual-harassment-of-a-female-reporter/>

Al Jazeera Investigative Unit (2021) 'Bangladesh bought mass spying equipment from Israeli company', Al Jazeera, at: <https://www.aljazeera.com/news/2021/2/2/bangladesh-bought-surveillance-equipment-from-israeli-company>.

Arai, Kenshi (2015) 'Cambodia Digital Communications', Slideshare, at:  
<https://www.slideshare.net/kenshiarai/cambodia-digital-communications-august-2015-51945532>.

Asante, Kwame (2020) 'Digital Security Best Practices for CSOs in Africa', WACSI, at:  
<https://wacsi.org/quick-tips-digital-security-best-practices-for-csos-in-africa/>.

Asia Centre (2023) 'State-sponsored online disinformation: Impact on electoral Integrity in Thailand' at: <https://asiacentre.org/wp-content/uploads/State-Sponsored-Online-Disinformation-Impact-on-Electoral-Integrity-in-Thailand.pdf>.

Duo, Matteo (2023) 'The top 14 secure email providers in 2023', Kinsta, at:  
<https://kinsta.com/blog/secure-email-providers/#:~:text=ProtonMail%20is%20the%20most%20well,ProtonMail%20is%20self%2Ddestructing%20emails>.

EngageMedia (2022) 'Localization: Digital security support for civil society', at:  
<https://engagemedia.org/projects/localization/>.

European Parliament (2010) 'Information and Communication Technologies and Human Rights', at:  
[https://www.europarl.europa.eu/RegData/etudes/etudes/join/2010/410207/EXPO-DROI\\_ET%282010%29410207\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2010/410207/EXPO-DROI_ET%282010%29410207_EN.pdf).

Fatafta, Marwa & Front Line Defenders (2022) 'Unsafe anywhere: women human rights defenders speak out about Pegasus attacks', Access Now, at:  
<https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/>.



Feldstein, Steven & Brian (Chun Hey) Kot (2023) 'Why does the global spyware industry continue to thrive? Trends, explanations, and responses', Carnegie Endowment for International Peace, at: <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229>.

Forum-Asia & Kontras (2021) 'Refusing silence: A joint analysis on the situation of Human Rights Defenders', Forum-Asia, at: <https://www.forum-asia.org/uploads/wp/2021/10/Regional-and-National-Analysis-FA-and-KontraS.pdf>

Froehlich, Andrew (2022) 'WLAN security: Best practices for wireless network security', TechTarget, at: <https://www.techtarget.com/searchsecurity/WLAN-security-Best-practices-for-wireless-network-security>.

Front Line Defenders (2021) 'Action needed to address targeted surveillance of human rights defenders', at: <https://www.frontlinedefenders.org/en/statement-report/action-needed-address-targeted-surveillance-human-rights-defenders>

Front Line Defenders (2022) 'Global analysis 2021', at: <https://www.frontlinedefenders.org/en/resource-publication/global-analysis-2021-0>

GeSI (2018) 'Enabling Rights', at: <https://gesi.org/research/download/37>.

Ghonim, Wael (2012) 'Revolution 2.0: The power of the people is greater than the people in power: A memoir', New York: Houghton Mifflin Harcourt Publishing Company

Idrus, Pizaro Gozali (2023) 'Whistle-blower: Indonesia may have used Israeli malware to spy on political opponents', Benar News, at: <https://www.benarnews.org/english/news/indonesian/israeli-spyware-used-by-state-agencies-06122023115033.html>.

IFJ (2022) 'Indonesia cyber attack targets independent media outlet', at: <https://www.ifj.org/media-centre/news/detail/category/press-releases/article/indonesia-cyber-attack-targets-independent-media-outlet>.

Jančis, Mindaugas (2023) 'Proton Mail review: have we found the most secure email provider in 2023?', Cybernews, at: <https://cybernews.com/secure-email-providers/protonmail-review>.

Kimseng, Men (2014) 'Shaping political change: The role of social media in Cambodia's 2013 elections', Asia Pacific Media Educator, at: <https://journals.sagepub.com/doi/abs/10.1177/1326365X14539201>

Kost, Edward (2023) 'What is PGP encryption? How it works and why it's still reliable?', UpGuard, at: <https://www.upguard.com/blog/what-is-pgp-encryption>.

Kozlov, Alexey (2020) 'NGOs responses to coronavirus pandemic spell lasting changes for the sector', Article 20.org, at: <https://article20.org/news/ngos-responses-to-coronavirus-pandemic-spell-lasting-changes-for-the-sector/>

Kraus, Rachel (2021) 'What is Signal? The basics of the most secure messaging app', Mashable SE Asia, at: <https://sea.mashable.com/tech/14001/what-is-signal-the-basics-of-the-most-secure-messaging-app>.

Lewis, James Andrew (2021) 'A Short Discussion of the Internet's Effect on Politics', CSIS, at: <https://www.csis.org/analysis/short-discussion-internets-effect-politics>

Ljubas, Zdravko (2022) 'Pegasus Scandal Hits EU from Within', OCCRP, at: <https://www.occrp.org/en/daily/17032-pegasus-scandal-hits-eu-from-within>.

Lo, Barnaby (2020) 'Philippines' biggest TV network silenced after years feuding with Duterte', CBC News, at: <https://www.cbsnews.com/news/abs-cbn-philippines-cease-operations-rodriago-duterte/>.

Ng, Kelly (2023) 'Cambodia's Hun Sen shuts down independent media outlet Voice of Democracy', BBC, at: <https://www.bbc.com/news/world-asia-64621595>

Ng Wei Kai (2022) 'S'pore exploring petition platform where 10,000 signatures guarantee ministry response', The Straits Times, at: <https://www.straitstimes.com/singapore/politics/spore-exploring-petition-platform-where-10000-signatures-guarantee-ministry-response>.

NonprofitHR (2022) '2022 Nonprofit talent management priorities: Survey results', at: <https://www.nonprofithr.com/wp-content/uploads/2021/03/2022-TMPS-Infographic-for-Publishing2.pdf>

Ongsakul, Sirinnaree (2023) 'Organisations concerned despite improvement in risk index', Bangkok Post, at: <https://www.bangkokpost.com/business/general/2565546>.

Paladino, Brandon 'Democracy Disconnected: Social Media's Caustic Influence on Southeast Asia's Fragile Republics', Brookings, at: [https://www.brookings.edu/wp-content/uploads/2018/07/FP\\_20180725\\_se\\_asia\\_social\\_media.pdf](https://www.brookings.edu/wp-content/uploads/2018/07/FP_20180725_se_asia_social_media.pdf).

Pinol Rovira, Marc (2021) 'Political participation in post-authoritarian regimes in the digital age', Doctor of Philosophy, University of Bristol, at: [https://research-information.bris.ac.uk/files/347858178/Final\\_Copy\\_2022\\_05\\_12\\_Pinol\\_Rovira\\_M\\_PhD\\_Redacted.pdf](https://research-information.bris.ac.uk/files/347858178/Final_Copy_2022_05_12_Pinol_Rovira_M_PhD_Redacted.pdf)

Potkin, Fanny & Poppy McPherson (2021) 'INSIGHT-How Myanmar's military moved in on the telecoms sector to spy on citizens', Reuters, at: <https://www.reuters.com/article/myanmar-politics-surveillance-intercept-idCNL4N2MJ3KK>

Proton (2023) 'Proton Mail encryption explained', Proton, at: <https://proton.me/support/proton-mail-encryption-explained>.

Matthews-EI, Toni & Cassie Bottorff (2022) 'Is using a VPN safe? What you need to know about VPN security', Forbes, at: <https://www.forbes.com/advisor/business/software/are-vpns-safe/>.

Ravoof, Salman (2022) 'ProtonMail vs Gmail: The ultimate comparison guide', Kinsta, at: <https://kinsta.com/blog/protonmail-vs-gmail/>.

Reuters (2022a) 'Govt admits using phone spyware, cites 'national security'', Bangkok Post, at: <https://www.bangkokpost.com/thailand/general/2350068/govt-admits-using-phone-spyware-cites-national-security>.

Reuters (2022b) 'Thai minister backtracks on spyware admission as government denies Pegasus use', at: <https://www.reuters.com/world/asia-pacific/thai-minister-backtracks-spyware-admission-government-denies-pegasus-use-2022-07-22/>.

Robinson, Cassie (n.d.) 'Civil society in our extremely digital world', Commission on Civil Society, at: <https://civilsocietycommission.org/essay/civil-society-in-our-extremely-digital-world/>

Root, Rebecca (2022) 'Digital rights activists in Southeast Asia increasingly at risk', Devex, at: <https://www.devex.com/news/digital-rights-activists-in-southeast-asia-increasingly-at-risk-103946>

Sanhokwe, Hamfrey & Takawira, Simon (2022) 'Impact of COVID-19 induced teleworking arrangements on employees in NGOs: Implications for policy and practice for leadership', SAGE Open, at: [https://www.researchgate.net/publication/359872724\\_Impact\\_of\\_COVID-19\\_Induced\\_Teleworking\\_Arrangements\\_on\\_Employees\\_in\\_NGOs\\_Implications\\_for\\_Policy\\_and\\_Practice\\_for\\_Leadership](https://www.researchgate.net/publication/359872724_Impact_of_COVID-19_Induced_Teleworking_Arrangements_on_Employees_in_NGOs_Implications_for_Policy_and_Practice_for_Leadership)

Shalan, Sharif (2021) 'How cloud computing is breaking down barriers for global NGOs', Candid, at: <https://blog.candid.org/post/how-cloud-computing-is-breaking-down-barriers-for-global-ngos>

Shankland, Stephen (2022) 'Pegasus spyware and citizen surveillance: Here's what you should know', CNET, at: <https://www.cnet.com/tech/mobile/pegasus-spyware-and-citizen-surveillance-what-you-need-to-know/>

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

Sombatpoonsiri, Janjira (2018) 'Manipulating Civic Space: Cyber Trolling in Thailand and the Philippines', GIGA Focus Asia, at: <https://www.giga-hamburg.de/en/publications/giga-focus/manipulating-civic-space-cyber-trolling-in-thailand-and-the-philippines>

Special Rapporteur on human rights defenders (n.d.) 'About human rights defenders', OHCHR, at: <https://www.ohchr.org/en/special-procedures/sr-human-rights-defenders/about-human-rights-defenders>

TLHR (2022) 'Thailand the land of surveillance: From enforced disappearances to EM, Digital, and Biometric Surveillance', at: <https://tlhr2014.com/en/archives/45101>.

UN General Assembly (2016), 'Human rights defenders in the context of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms', United Nations Digital Library, at: <https://digitallibrary.un.org/record/821191?ln=en>.

Urbinati, Lorenzo & Sejin Kim (2017) 'Protecting human rights defenders in Asia: using networks to fill the gaps', Open Global Rights, at: <https://www.openglobalrights.org/protecting-human-rights-defenders-in-asia-using-networks-to-fill-the-gaps/>

Von Kameke, Leandor (2023) 'Internet penetration rate in Bangladesh from 2011 to 2020', Statista, at: <https://www.statista.com/statistics/764102/internet-penetration-rate-bangladesh/>

We are Social (2015) 'Digital 2015: Indonesia', Datareportal, at: <https://datareportal.com/reports/digital-2015-indonesia>

We are Social (2015) 'Digital 2015: The Philippines', Scribd, at: <https://www.slideshare.net/DataReportal/digital-2015-philippines-january-2015>

We are Social (2015) 'Digital 2015: Singapore', Datareportal, at: <https://datareportal.com/reports/digital-2015-singapore>

We are Social (2015) 'Digital 2015: Thailand', Datareportal, at: <https://datareportal.com/reports/digital-2015-thailand>

We are Social (2023) 'Digital 2023: Bangladesh', Datareportal, at: <https://datareportal.com/reports/digital-2023-bangladesh>.

We are Social (2023) 'Digital 2023: Cambodia', Datareportal, at:  
<https://datareportal.com/reports/digital-2023-cambodia>

We are Social (2023) 'Digital 2023: Indonesia', Datareportal, at:  
<https://datareportal.com/reports/digital-2023-indonesia>

We are Social (2023) 'Digital 2023: Myanmar ', Datareportal, at:  
<https://datareportal.com/reports/digital-2023-myanmar>

We are Social (2023) 'Digital 2023: The Philippines', Datareportal, at:  
<https://datareportal.com/reports/digital-2023-philippines>

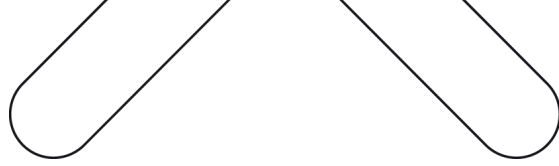
We are Social (2023) 'Digital 2023: Singapore', Datareportal, at:  
<https://datareportal.com/reports/digital-2023-singapore>

We are Social (2015) 'Digital 2023: Thailand', Datareportal, at:  
<https://datareportal.com/reports/digital-2023-thailand>

World Bank (2023) 'Individuals using the Internet (% of population) - Myanmar, World, at:  
<https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=MM>.

Wrights, George & Issariya Praithongyaem (2020) 'Wanchalearm Satsaksit: The Thai satirist abducted in broad daylight', BBC, at: <https://www.bbc.com/news/world-asia-53212932>.

Youngs, Richard (2019) 'Civic activism unleashed: New hope or false dawn for democracy?', Oxford Academic, DOI: 10.1093/oso/9780190931704.003.0006.



**EngageMedia.org/  
open-secure-technology-  
adoption-research**

