DIGITAL SECURITY & HUMAN RIGHTS DEFENDERS LANDSCAPE

RECOMMENDATIONS FOR NHRIs IN THE ASIA-PACIFIC

ASIACENTRE

Funded by
the European Union

APF

DIGITAL SECURITY & HUMAN RIGHTS DEFENDERS LANDSCAPE

Recommendations for NHRIs in the Asia-Pacific

2023

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

Page

Abbreviations V

Executive Summary VI

1. Introduction 1

1a. Methodology 1

1b. Definition of Key Terms 1

1c. Background: Encroachment on HRDs' Rights 2

1d. International Legal Framework 4

International Human Rights Frameworks 4

The Marrakesh Declaration (2018) & Regional Action Plan of HRDs (2021-2025) 5

2. Digital Security Threats Faced by HRDs 6

2a. Restrictive Legal and Regulatory Frameworks 6

2b. Disruption of Communications 8

2c. State Surveillance 10

2d. Information Operations 11

3. NHRIs: Their Efforts & Limitations 13

3a. Monitoring & Reporting 13

3b. Advocacy & Awareness Raising 14

3c. Capacity & Network Building 17

4. Recommendations 20

5. Conclusion 22

ABBREVIATIONS

APF	Asia-Pacific Forum of National Human Rights Institutions
CSO	Civil Society Organisation
GANHRI	Global Alliance of National Human Rights Institutions
HRD	Human Rights Defender
ICCPR	International Covenant on Civil and Political Rights
ISP	Internet Service Providers
NHRI	National Human Rights Institution
OHCHR	Office of the United Nations High Commissioner for Human Rights
RAP	Regional Action Plan on Human Rights Defenders (2021–2025)
UN	United Nations
UPR	Universal Periodic Review

National Human Rights Institutions

AIHRC	Afghanistan Independent Human Rights Commission
AHRC	Australian Human Rights Commission
NIHR	National Institution for Human Rights in the Kingdom of Bahrain
NHRCB	National Human Rights Commission of Bangladesh
FHRADC	Fiji Human Rights and Anti-Discrimination Commission
NHRCI	National Human Rights Commission of India
KOMNAS HAM	Indonesian National Commission on Human Rights
NHCR	High Commission for Human Rights of Jordan
NCHRK	National Centre for Human Rights of Kazakhstan
NHRCK	National Human Rights Commission of Korea
Akyikatchy	Ombudsman of the Kyrgyz Republic
SUHAKAM	Human Rights Commission of Malaysia
HRCM	Human Rights Commission of the Maldives
NHRCM	National Human Rights Commission of Mongolia
NHRCN	National Human Rights Commission of Nepal
NZHRC	New Zealand Human Rights Commission
OHRC	Oman Human Rights Commission
ICHR	Palestine Independent Commission for Human Rights
CHRP	Commission on Human Rights of the Philippines
NHRC	National Human Rights Committee of Qatar
HRCSL	Human Rights Commission of Sri Lanka
NHRCT	National Human Rights Commission of Thailand
PDHJ	Provedor for Human Rights and Justice of Timor-Leste

EXECUTIVE SUMMARY

In the digital age, the rights of many human rights defenders (HRDs) in the Asia-Pacific region are in jeopardy. With the rapidly evolving technological landscape, opportunities and challenges for HRD' advocacy have emerged. In this context, the increased institutional capacity of national human rights institutions (NHRIs) to cope with HRD's challenges in the digital domain is critical.

Since the 2000s, there has been a significant shift towards online activism due to the region's increasing internet usage. This has made it necessary for HRDs to adapt to the digital environment and adapt to the latest digital developments, since the online sphere has expanded the horizons of human rights advocacy, enabling HRDs to overcome media restrictions and coordinate protests more effectively.

Nevertheless, the proliferation of digital tools has raised concerns about HRDs' safety and security. Governments in the Asia-Pacific region have responded to HRD's new online advocacy strategies, affecting their online advocacy through the use of legal and non-legal measures to harass them and impede their work. Against this backdrop, NHRIs have a mandate to protect human rights, including those of HRDs. The Marrakech Declaration of 2018, outlined a framework for NHRIs to support HRDs, emphasising both offline and online civic space. However, there is a need for NHRIs to adapt these plans to address digital security threats to HRDs.

This report contributes to this goal by outlining four specific ways through which HDRs are threatened online. First, it shows that, in the Asia-Pacific region, HRDs often face legal threats through laws related to defamation, insult, and "fake news", as well as broader online regulations granting government authorities extensive powers to limit online freedoms.

Second, governments have disrupted online communications by limiting or suspending internet connectivity. Some countries control internet gateways to regulate information flow, and during political instability, internet service providers (ISPs) and mobile carriers are ordered to restrict internet speed or access.

Third, governments in the region use technology for legal and covert mass data collection and surveillance. They create national internet gateways for centralized control, consolidating information and data storage.

Lastly, HRDs encounter digital threats from "cybertroops", combining human operatives and bots on social media to influence public opinion in favour of the government. Governments are complicit by showing minimal commitment to addressing the problem.

Identifying these threats is the basis for this report to recognise the efforts and limitations of NHRIs in ensuring HRDs' rights online in three areas - monitoring and reporting; advocacy and awareness-rising; and capacity and network building - and provide a set of recommendations aimed at increasing NHRI's institutional capacity.

In terms of the monitoring and reporting system, the report recommends that NHRIs should systematically strengthen it and increase their capacity to identify complaints as coming from HRDS; to encompass all aspects of digital security threats to establish a robust foundation for effective complaints handling. Once equipped with this information, NHRIs should step up their engagement both with the government and at the parliamentary level. They should also focus on raising public awareness about digital security threats through a well-structured Communications Plan and forge partnerships with tech companies and ISPs to ensure online rights and privacy for HRDs. Furthermore, they should actively participate in civil society events, host gatherings for HRDs, provide capacity-building opportunities for staff in digital rights and HRD-related programs, and foster collaboration with regional NHRI associations and initiatives like the NHRI Tech Alliance.

Only with multi-faceted efforts, NHRIs will be able to increase their institutional capacity, being better equipped to ensure that HRDs' online advocacy is carried out safely.

1. Introduction

The adoption of the internet and digital tools among human rights defenders (HRDs) in the Asia-Pacific has resulted in a range of new opportunities for their advocacy, particularly with improved communications and capacity to mobilise people. However, the rights of many are threatened through the use of digital measures by government actors and the limited institutional capacity of many National Human Rights Institutions (NHRIs) to ensure their safety in the online sphere. This report evaluates NHRIs' effectiveness in safeguarding the rights of HRDs against digital security threats. It underscores the need for these bodies to increase their institutional capacity to better monitor and report the rights violations that many HRDs are currently facing in the digital domain. With this analysis, the report also offers a set of recommendations for NHRIs to enhance their performance in supporting HRDs in their human rights advocacy.

1a. Methodology

This report was prepared by conducting desk research to gather information from the 26 countries that house NHRIs affiliated with the Asia-Pacific Forum (APF) between August and September 2023. Primary and secondary documents consulted included NHRIs' annual reports, strategic plans, news and other activities as presented on their websites and submissions to the Universal Periodic Review (UPR) process and the International Covenant on Civil and Political Rights (ICCPR) reporting mechanism. It also consulted international human rights covenants and news reports. The scope of this research encompasses the period from 2017 onwards, with a focus on the goals and objectives outlined in the RAP. Before its final submission, the report underwent internal review by both the research team and APF.

1b. Definition of Key Terms

Human Rights Defenders (HRDs)

Individuals or groups of people who engage in peaceful actions to advance or safeguard human rights (OHCHR, nd.). In the Asia-Pacific, they are vital actors due to their role in addressing complex human rights challenges, holding governments accountable, protecting vulnerable communities, advocating for environmental and media freedoms, supporting civil society, and contributing to conflict resolution and peacebuilding, all while promoting justice and equality.

National Human Rights Institutions (NHRIs)

NHRIs are independent state institutions, established by a state's constitution or national legislation, with a broad mandate to protect and promote human rights.They serve as intermediaries between international and domestic human rights standards, working to raise awareness, mediate conflicts, ensure government accountability, and foster regional cooperation. In this diverse and dynamic region, NHRIs play a pivotal role in advancing human rights.

Digital Security Threats

These can be categorised into three main areas. Firstly, government pressure through internet- and digital-related laws and regulations allows government agencies to take control of internet infrastructure as well as censor and take down content online. Secondly, digital surveillance and interception of digital communications. Thirdly, government-sanctioned or tacit endorsement of information and communication operations to influence opinions, and spread propaganda against HRDs.

1c. Background: Encroachment on HRDs' Rights

In the digital age, the rights of many HRDs in the Asia-Pacific region have been encroached upon. This has become a problem since HRDs play a pivotal role in advocating and safeguarding human rights, thus cultivating a more equitable society within the region. Their endeavours encompass a spectrum of activities aimed at advancing and preserving these rights, including the documentation of human rights transgressions, the provision of legal aid to affected parties, the propagation of awareness through nonviolent demonstrations, media-driven campaigns, and grassroots mobilisation. The nature of their task is highly subject to the latest social developments, including the technological ones, which have brought new opportunities for advocacy but have also challenged HRDs' rights to undertake their tasks.

Since the 2000s, the operations of HRDs have gradually shifted to the online domain due to the exponential growth in internet usage in the region. In 2001, the average internet penetration of Asia-Pacific countries stood at 17%. In 2021, it had risen to 71%.[1] Additionally, Asia-Pacific users contribute towards more than half of the total social media users in the world[2] and rank among the world's most time spent online.[3] This underscores the role of digital applications among the people and, most importantly, the need for HRD to adapt to this trend.

The development of the digital sphere has transformed human rights advocacy with a range of new opportunities for augmenting the role and effectiveness of NHRIs and HRDs in their efforts to advance and safeguard human rights. The increased use of the internet saw the rise in online independent media, which HRDs used to circumvent the lack of media freedom in certain environments that prevented them from reporting human rights issues freely.[4] The internet also facilitated protests. For example, in Myanmar, the internet and social media played a key role in facilitating the coordination of protests following the 2021 military takeover of the government and allowed the international community to quickly learn about the situation in the country.[5]

However, better digital tools and media have raised concerns about HRD's safety and security. With the development of the digital civic space and the creation of many new opportunities for advocacy, governments in the Asia-Pacific region have sought to create new measures to limit the impact that new advocacy strategies have had both online and offline. Firstly, many governments have continued using national security laws and other order-driven laws – which do not directly apply to the online sphere – to criminalise free speech in digital settings.[6] Nonetheless, they have also tightened their control over the online sphere by enacting internet laws and regulations to control the information flow online. Second, governments have deployed internet infrastructure technologies and hacking tools to monitor HRDs online. For example, the spyware Pegasus is reported being operated by various state

[1] World Bank (2023) 'Individuals using the Internet (% of population)', World Bank, at: https://data.worldbank.org/indicator/IT.NET.USER.ZS.
[2] Pixium Digital (2014) 'Social media usage in Asia Pacific', Pixium Digital, at: https://pixiumdigital.com/social-media-usage-asia-pacific.
[3] Kameke, Leander von (2023) 'Social media in the Asia-Pacific region – Statistics & facts', Statista, at: https://www.statista.com/topics/6606/social-media-in-asia-pacific.
[4] Notley, Tanya and Stephanie Hankey (2014) 'Human Rights Defenders and the Right to Digital Privacy and Security', in John Lannon and Edward F. Halpin (eds.), *Human Rights and Information Communication Technologies: Trends and Consequences of Use*, Hershey, PA: IGI Global, DOI:10.4018/978-1-4666-6433-3.ch108.
[5] Tangen, Ole Jr. (2021) 'The battle for Myanmar plays out on social media', DW, at: https://www.dw.com/en/the-battle-for-myanmar-plays-out-on-twitter-tiktok-and-telegram/a-57267075.
[6] Asia Centre (2021a) *Defending Freedom of Expression: Fake News Laws in East and Southeast Asia*, Bangkok: Asia Centre; Asia Centre (2022a) *Media Freedom in Southeast Asia: Repeal Restrictive Laws, Strengthen Quality Journalism*, Bangkok: Asia Centre; Asia Centre (2022b) *Foreign Interference Laws in Southeast Asia: Deepening the Shrinkage of Civic Space*, Bangkok: Asia Centre.

agencies across the region.[7] Third, they have covertly deployed or condoned information operations that sought to spread pro-government narratives and harass HRDs online. Together, these legal and non-legal measures have threatened HRDs' online advocacy, resulting in limited opportunities to promote and protect human rights – the next chapter will analyse these specific impacts in greater detail.

As a result of the restrictions of many governments imposed on the activities of HDRs, civic spaces across the region are generally in jeopardy, as several global indicators show.

Table 1: Civic Space Indexes in Asia-Pacific

Country	Freedom on the Net (Freedom House, 2022) (0= lowest, 100= highest)	Internet Censorship (Bischoff, 2023) (0= lowest, 10= highest)	State of Civic Space (CIVICUS, 2023)
Afghanistan	**N/A**	6	Closed
Australia	76	3	Narrowed
Bahrain	28	7	Closed
Bangladesh	41	7	Repressed
Fiji	N/A	3	Obstructed
India	50	7	Repressed
Indonesia	47	6	Obstructed
Iraq	11	9	Closed
Jordan	47	6	Repressed
Kazakhstan	34	7	Repressed
Kyrgyzstan	52	3	Obstructed
Malaysia	61	7	Obstructed
Maldives	**N/A**	3	Obstructed
Mongolia	**N/A**	1	Narrowed
Myanmar	10	2	Closed
Nepal	**N/A**	5	Obstructed
New Zealand	**N/A**	1	Open
Oman	**N/A**	8	Repressed
Palestine	**N/A**	5	Repressed
Philippines	61	5	Repressed
Qatar	**N/A**	8	Repressed
Samoa	**N/A**	2	Open
South Korea	67	5	Narrowed
Sri Lanka	52	6	Obstructed
Thailand	39	8	Repressed
Timor-Leste	**N/A**	1	Obstructed

[7] Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert (2018) 'Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries', The Citizen Lab, at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries.

As Table 2 data reveals, the Asia-Pacific region exhibits stark contrasts when it comes to internet freedoms and civic spaces. On one hand, countries like New Zealand boast highly open civic spaces and relatively minimal threats to their digital spheres. On the other hand, nations such as Myanmar have tightly closed civic spaces. According to Freedom House data, the average score for internet freedoms in the region is 45.07 out of 100, with 100 representing absolute freedom. Regarding internet censorship, Comparitech's data indicates an average score of 5.03 out of 10, where 10 signifies the highest level of censorship. Finally, CIVICUS indexes show that open civic spaces are a rarity, with 2 classified as open, 8 as obstructed, 3 as narrowed, and 9 as repressed.

In a context where civic spaces and internet freedoms are diminishing, it is essential to examine international legal frameworks to specify how HRDs' rights are being violated and start devising the necessary measures to reverse this trend. The next section reviews important international human rights principles, the Marrakesh Declaration, and the Regional Action Plan for HRDs.

1d. International Legal Framework

The Section outlines three normative frameworks to analyse the threats that many HRDs in the Asia-Pacific region are facing: United Nations (UN) mechanisms – including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR) – the Marrakesh Declaration, and the APF's Regional Action Plan of HRDs.

International Human Rights Frameworks

Several UN mechanisms and bodies have laid out states' duty to facilitate the work of HRDs. The right for individuals to associate and work together is recognised by the Universal Declaration of Human Rights (Article 20) (1948).[8] The Declaration on Human Rights Defenders (1998)[9] affirms their rights to collaborate both at the national and international levels to promote and protect human rights. Further, the Special Rapporteur on Peaceful Assembly and Association notes that States "have [an] obligation to abstain from unduly interfering with the rights of peaceful assembly and of association … [and an] obligation to facilitate and protect these rights".[10] The ICCPR (1966),[11] to which seven countries in the region are party, outlines that restrictions on association shall be imposed only if such association threatens democratic rules (Article 22).

The duties above extend online. The UN Human Rights Committee notes in General Comment No. 37 (2020)[12] "the Covenant protects peaceful assemblies wherever they take place: outdoors, indoors and online". It also emphasises that state interference with technological equipment can impede upon the right to assembly. They must therefore not hinder internet connectivity or issue geo-targeted or technology-specific interference against peaceful assembly.[13]

[8] "Universal Declaration of Human Rights" (1948), UN, at: https://www.un.org/en/about-us/universal-declaration-of-human-rights.
[9] "Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms" (1998), OHCHR, at: https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-right-and-responsibility-individuals-groups-and.
[10] Voule, Clément Nyaletsossi (2019) 'A/HRC/41/41 Rights to freedom of peaceful assembly and of association: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', UNHRC, at: https://undocs.org/A/HRC/41/41.
[11] "International Covenant on Civil and Political Rights" (1966), OHCHR, at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
[12] "CCPR/C/GC/37 General comment No. 37 (2020) on the right of peaceful assembly (article 21)" (2020), ICCHPR Human Rights Committee, at: https://www.undocs.org/CCPR/C/GC/37.
[13] Ibid.

The Marrakesh Declaration (2018) & Regional Action Plan of HRDs (2021–2025)

Existing as state-sanction – but independent – organisations, NHRIs carry a task to promote and protect human rights in their respective countries. Part of their coverage is to protect the rights of and facilitate the work of HRDs to ensure the effective functioning of civic space.[14] Building upon this principle, in 2018, the Global Alliance of National Human Rights Institutions (GANHRI) organised a conference among NHRIs. An output of the conference, the Marrakesh Declaration (2018) [15] established a framework of action for NHRIs to protect the rights of HRDs and support their work. Of note, civic space was specifically mentioned to incorporate both offline and online.

In line with the Declaration, APF adopted the "Regional Action Plan on Human Rights Defenders 2021-2025" (2021) which set out actions for NHRIs at both the national and international levels.

When grouped thematically, their objectives can be framed as follows:

- **Monitoring & Reporting:** This includes developing early warning systems, monitoring and reporting on violations against HRDs and creating a regional data set on violations against HRDs.
- **Advocacy & Awareness Raising:** advocating for national legal protections, and raising awareness of the rights of HRDs, promoting gender equality and mainstreaming the recognition of women, engaging with international human rights systems and engaging in regional policy-making on HRDs.
- **Capacity & Network Building:** Strengthening national networks of HRDs and engaging regional civil society, NHRI collaboration, and supporting the establishment of new NHRIs.

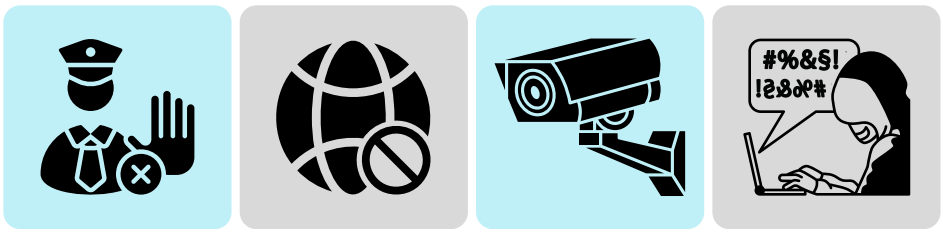
After review, there were no specific references to actions that NHRIs can take to protect and promote online civic space. Therefore, it is within the purview of each NHRI to adapt these plans and outline the necessary steps to safeguard HRDs against digital security threats.

To enhance NHRIs' institutional capacity and implement the required measures for HRD safety, the rest of the report analyses the key online threats faced by HRDs in the Asia-Pacific region and examines the actions taken by NHRIs to address these challenges. These findings will serve as the basis for the recommendations provided at the end of the report.

[14] GANHRI (nd.) 'Paris Principles', GANHRI, at: https://ganhri.org/paris-principles.
[15] GANHRI (2018) 'The Marrakech Declaration', GANHRI, at: https://ganhri.org/wp-content/uploads/2019/11/Marrakech-Declaration_ENG_-12102018-FINAL.pdf.

2. Digital Security Threats Faced by HRDs

This Chapter explores various legal and non-legal toolkits which threaten HRDs as they work online to advance human rights. It shows that, through these digital security threats, HRDs are restricted in their freedom of expression online and their online privacy. They also face inhibitions from working online and, in some cases, face coordinated online hatred against them.



2a. Restrictive Legal and Regulatory Frameworks

In the Asia-Pacific region, HRDs are often targeted by such laws, which include provisions in criminal codes and other pieces of legislation related to defamation, insult or blasphemy. However, apart from these, there also exist laws and regulations pertaining to the online sphere which are often drafted in a manner that grants government authorities broad powers to restrict freedoms online.

In **Malaysia**, the Communication and Multimedia Act (1998)[16] criminalises individuals who misuse network facilities to make obscene, indecent, or offensive comments. However, concerns have arisen due to the vague language within these provisions, which government authorities have used to target legitimate expressions by HRDs.[17]

In February 2023, **Mongolia** enacted the Law on Protecting Human Rights on Social Media (2023).[18] Among other provisions, the law disallowed the sharing of public and government information without approval by concerned government authorities. This potentially limits the role of journalists and HRDs who want to report on sensitive issues, which often involve cases of corruption and policy mismanagement.[19]

[16] "Communications and Multimedia Act" (1998), Malaysian Communications and Multimedia Commission, at: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Act588bi_3.pdf.
[17] Asia Centre (2022a) *Media Freedom in Southeast Asia*.
[18] "*[Law on Protecting Human Rights on Social Media]*" (2023), Parliament of Mongolia, at: https://web.archive.org/web/20230119040732/https://d.parliament.mn/tusul/d374b224-b0b2-4bff-9fcf-bf46717ee7bf.
[19] Smalley, Seth (2023) 'Mongolia moves to seize power to shut down internet, control social media', Poynter, at: https://www.poynter.org/fact-checking/2023/mongolia-law-protecting-human-rights-shut-down-internet.

Nepal's Electronic Transaction Act (2006)[20] was a piece of legislation originally enacted against online financial scams.[21] Yet, it has reportedly been used to restrict free speech online through its broad provisions which ban expressions online that "may be contrary to the public morality or decent behaviour" or disrupt "harmonious relations" among the people" – which are notably vague terms. Such unclear and unconcise terminology has been reported as decreasing the effectiveness of advocacy by HRDs, who struggle to determine the boundaries of the law.[22]

The **Iraqi** parliament is – as of September 2023 – legislating the Law on Freedom of Expression and Peaceful Assembly. Should it be enacted, the law would allow for the prosecution of comments that violate "public morals" or "public order". This law would be one in a series of laws, regulations and policies aimed at cracking down on HRDs' voices online.[23]

Laws are also enacted to cover the operation of Internet Service Providers (ISPs) as entities that have control over access to the internet. As an effect, they are forced to abide by these restrictive laws should they want to continue operating in the country or not be faced with heavy penalties. This allows the government to take down specific websites and servers run by HRDs – for example, independent online media.

Thailand's Computer Crime Act (2007)[24] assigns power to Thai authorities to issue orders to ISPs to block or remove "data from computer systems" within a specified timeframe. Non-compliance would result in a fine of up to USD 6,000.[25] The law has been used to take down content by online journalists and activists that government authorities deemed inappropriate and critical of the monarchy.[26]

Kyrgyzstan's Law On Protection from Inaccurate (False) Information (2021)[27] specifies a condition that ISPs in the country could potentially lose their licences should they not carry out government-mandated blocking orders as prescribed by the law. The law has been used to block and ultimately shut down a radio service which allegedly contained false information.[28]

In an amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule (2021) in 2023, the **Indian** government established a "fact check unit" which proscribed internet intermediaries to "make reasonable efforts" for its users not to publish "fake news" on their platforms. Failure to comply with the Rule would result in a potential liability to the providers – a liability once exempted.[29]

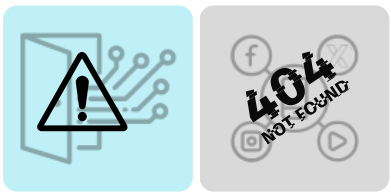
[20] "The Electronics Transactions Act" (2006), Trade and Export Promotion Centre, at: http://www.tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf.
[21] Kharel, Samik (2022) 'Towards digital authoritarianism in Nepal: Surveillance, data collection, and online repression', EngageMedia, at: https://engagemedia.org/2022/pandemic-control-nepal.
[22] Republica (2022) 'Authorities in Nepal using Electronic Transaction Act to stifle freedom of expression', myRepublica, at: https://myrepublica.nagariknetwork.com/news/authorities-in-nepal-using-electronic-transaction-act-to-stifle-freedom-of-expression.
[23] Iraqi Observatory for Human Rights (2023) 'Press release regarding the draft law on freedom of expression and peaceful demonstration', Iraqi Observatory for Human Rights, at: https://iohriq.org/118-.html.
[24] "Computer-related Crime Act" (2007), Ministry of Digital Economic and Society of Thailand, at: https://www.mdes.go.th/law/detail/3618-COMPUTER-RELATED-CRIME-ACT-B-E--2550--2007.
[25] Asia Centre (2022c) *Thailand Computer Crime Act: Restricting Digital Rights, Silencing Online Critics*, Bangkok: Asia Centre.
[26] Ibid.
[27] "*[Law on Protection from Inaccurate (False) Information]*" (2021), Ministry of Justice of the Kyrgyz Republic, at: http://cbd.minjust.gov.kg/act/view/ru-ru/112282?cl=ru-ru.
[28] RFE/RL Kyrgyz Service (2023) 'Bishkek court orders check of language in video that sparked blockage of RFE/RL's Kyrgyz Websites', RFE/RL, at: https://www.rferl.org/a/kyrgyzstan-radio-free-europe-azattyk-court-blockage/32333041.html.
[29] Panjiar, Tejasi and Prateek Waghre (2023) 'IT Amendment Rules, 2023 are a nightmare, dressed like a fact checking daydream', Internet Freedom Foundation, at: https://internetfreedom.in/public-brief-it-amendment-rules-2023.

Similarly, in 2019,[30] the **Australian** government amended the Criminal Code following the online streaming of the Christchurch massacre for it to be able to order ISPs – as well as social media platforms – to take down "abhorrent" videos. There are concerns about the harsh nature of the takedown order, which allows the government to issue a fine of 10% of annual revenue for such services. There are also criticisms regarding the unclear language of what content could be deemed illegal.[31]

Hence, an observable pattern emerges within the Asia-Pacific region as governments implement legislation and regulations that confer upon them the authority to restrict internet freedom. These legislative measures frequently focus on HRDs and employ ambiguous and broad terminology, thereby facilitating the suppression of authentic manifestations of advocacy by HRDs. This trend consistently manifests as the erosion of online liberties, thereby posing a threat to freedom of speech within the region.

2b. Disruption of Communications

In the Asia-Pacific region, governments have introduced measures aimed at interfering with online communications or issued directives to limit, decelerate, or entirely suspend internet connectivity. These interruptions occur amidst growing scrutiny of governmental actions.



At the structural level, certain nations have implemented measures to assume control over internet gateways within their borders, to regulate the flow of information. China provides a comprehensive outlook of how this is implemented. Its "great firewall" is used to block information coming out of and going inside the country. Similar ideas have been taken up by the Cambodian government, through its idea of a "National Internet Gateway".[32]

Such a centralised gateway has not been established among the 26 countries in the Asia-Pacific region targeted by this research.[33] Nonetheless, two countries, among others, have shown their intention to pursue such an internet model. If they are established, it could significantly impede the digital environment in both countries, as it would grant governments the authority to dictate the channels through which HRDs can engage in information-sharing activities.

The military-affiliated government of Thailand has proposed such a mechanism on two occasions. Initially, in 2015, this proposition was put forth by the then-junta regime, which sought to exert control over online narratives that criticised the military coup d'état in 2014. Subsequently, in 2022, the ruling party of Thailand's prior government – which included members of the military junta – announced its intention to pursue the concept of a "Single Gateway", citing concerns related to unlawful online

[30] "Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill" (2019), Parliament of Australia, at: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/bills/s1201_aspassed/0000%22.
[31] Crozier (2019) 'Australia's "world-first" social media laws could require action within an hour', itnews, at: https://www.itnews.com.au/news/australias-world-first-social-media-laws-could-require-action-within-an-hour-523389.
[32] Asia Centre (2021b) *Internet Freedoms in Cambodia: A Gateway to Control*, Bangkok: Asia Centre.
[33] The countries targeted in the region are selected based on the locations of APF's member NHRIs.

activities and criminal organisations.[34] This move is widely regarded as a response to the increased scrutiny and criticism directed at the government via social media platforms,[35] particularly in the aftermath of the youth-led protests that occurred between 2020 and 2021. The party is now part of the new government.

In March 2023, the Mongolian parliament passed a social media law that aims to establish a framework akin to a national internet gateway. It is important to note that this legislation was subjected to a soft veto by the President; however, the bill remains under consideration within the parliament.[36] In addition to national gateways, during some periods characterised by political instability, ISPs and mobile carriers were ordered to restrict internet speed or access altogether. In 2021 and 2022, the following cases were reported:[37]

- Afghanistan: 1 occasion
- Bangladesh: 2 occasions
- India: 139 occasions
- Indonesia: 2 occasions
- Jordan: 2 occasions
- Myanmar: 23 occasions
- Oman: 1 occasion
- Pakistan: 7 occasions

In the aftermath of the coup that took place on 1 February 2021, the military junta in Myanmar promptly implemented internet shutdowns in key urban centres, including Naypyidaw. Subsequently, the junta issued directives instructing Internet Service Providers (ISPs) to enact prohibitions on access to various social media platforms, including Facebook, Messenger, WhatsApp, Twitter, and Instagram. Access to Wikipedia was also blocked. Although certain restrictions were partially lifted at later stages, there have been instances in which the junta has persisted in limiting the use of mobile data and public Wifi services.[38]

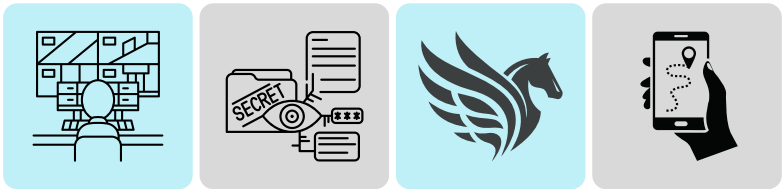
In India, for another example, an internet blackout occurred following a months-long farmer's protest in 2021.[39] Research on internet shutdowns in the country found that they regularly occur at a time when authorities are called out by HRDs and netizens for policy mismanagement.[40] (American Bar Association, 2022).

In Jordan, the cities of Maan and Karak, among others, during a protest over fuel prices in December 2022, saw restrictions on internet access as well as a ban on accessing TikTok.[41]

[34] O'Conner, Joseph (2022) 'Minister signals a move to resurrect a national internet gateway and stronger online controls', Thai Examiner, at: https://www.thaiexaminer.com/thai-news-foreigners/2022/02/22/minister-resurrects-internet-gateway-scheme.
[35] Ibid.
[36] Stucchi, Massimiliano (2023) 'Mongolia joins growing number of countries reducing openness and resilience of the internet', Internet Society Pulse, at: https://pulse.internetsociety.org/blog/mongolia-joins-growing-number-of-countries-reducing-openness-and-resilience-of-the-internet.
[37] AccessNow (2023a) 'Internet shutdowns in 2021: the return of digital authoritarianism', AccessNow, at: https://www.accessnow.org/internet-shutdowns-2021; AccessNow (2023b) 'Weapons of control, shields of impunity: Internet shutdowns in 2022', AccessNow, at: https://www.accessnow.org/internet-shutdowns-2022.
[38] Asia Centre (2021c) 'Myanamr Coup and Internet Shutdowns', Asia Centre, at: https://asiacentre.org/wp-content/uploads/Briefing-Note-Myanmar-Coup-and-Internet-Shutdowns.pdf.
[39] Rajvanshi, Astha (2023) 'How internet shutdowns wreak havoc in India', Time, at: https://time.com/6304719/india-internet-shutdowns-manipur.
[40] American Bar Association (2022) 'The Impact of Internet Shutdowns on Human Rights Defenders in India', Kasmir Law & Justice Project, at: https://www.kljp.org/articles/the-impact-of-internet-shutdowns-on-human-rights-defenders-in-india.
[41] Jordan Open Source Association (2022) 'Internet shutdowns and blocking of TikTok in Jordan: The right to access the internet should be preserved', Jordan Open Source Association, at: https://jordanopensource.org/blog/239.

2c. State Surveillance

Governments in the region have been observed employing technology to engage in both lawful and covert mass data collection, interception, and surveillance of their citizenry. To achieve this, one method commonly employed is the establishment of national internet gateways, which centralise control over the nation's internet infrastructure. This arrangement allows for the consolidation of information flow through government-sanctioned exchange points, facilitating the storage and retrieval of data.



Furthermore, in some instances, countries have undertaken digital wiretapping of data cables passing through their jurisdiction. The specific nature and extent of the data stored through such means remain largely undisclosed. Nonetheless, this practice poses a significant risk to HRDs operating within countries where the government possesses the capability to intercept their digital communications. It is worth noting Australia and New Zealand participate in digital wiretapping activities as part of the Five Eyes intelligence alliance.[42] Those in the alliance share sensitive and oftentimes personal and private information. For another example, in **Qatar**, the government can tap into telecommunications networks without the operator's knowledge or consent.[43] Another example concerns **Kazakhstan**, where the government intercepts encrypted communications that are facilitated by KazakhTelecom, the country's largest ISP.[44] There are also reports that over 50 countries part of the China-led Belt and Road Initiative are importing Chinese artificial intelligence surveillance technologies.[45] (Chandran, 2022). Among them, are 24 countries in the Asia-Pacific region whose NHRI are part of APF, except for Mongolia, South Korea and Timor-Leste.[46]

Concerns also exist that governments throughout the region use illegal spying software to monitor HRDs, constituting another form of state surveillance. For one example, the spyware "Pegasus" is reportedly used by various government agencies in the following countries to tap into HRD's mobile

[42] Gallagher & Hager (2015) 'New Zealand spies on neighbours in secret "Five Eyes" global surveillance', The Intercept, at: https://theintercept.com/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore.
[43] AccessNow (2018) 'Submission to the United Nations Human Rights Council, on the Universal Periodic Review for Qatar in 2019', AccessNow, at: https://www.accessnow.org/wp-content/uploads/2018/10/Qatar-UPR-Digital-rights.pdf.
[44] Sundara Raman, Ram, Leonid Evdokimov, Eric Wustrow, Alex Haldermana, and Roya Ensafi (2019) 'Kazakhstan's HTTPS interception', Censored Planet, at: https://censoredplanet.org/kazakhstan; Earp, Madeline (2019) 'Kazakhstan's move to control internet prompts censorship, surveillance concerns', Committee to Project Journalists, at: https://cpj.org/2019/07/kazakhstans-move-to-control-internet-prompts-censo.
[45] Chandran, Rina (2022) 'FEATURE-Activists fear rising surveillance from Asia's Digital Silk Road', Reuters, at: https://www.reuters.com/article/china-southeast-asia-surveillance-idUSL8N1WD0DP.
[46] Carnegie Endowment for International Peace (2019) 'AI Global Surveillance (AIGS) Index', Carnegie Endowment for International Peace, at: https://carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf.

phones: Bahrain,[47] India,[48] Jordan,[49] Kazakhstan,[50] Palestine,[51] and Thailand.[52] In Bahrain, for example, three HRDs who were hacked are members of a civil society organisation working on human rights.[53]

In addition to Pegasus, a civil society-led effort to inventorise the use of commercial spyware deployed by governments worldwide, found that, by March 2023, several nations have purportedly employed diverse spyware technologies within their territories. This deployment serves various objectives, prominently among them being the surveillance of HRDs. Notably, among the countries identified as engaging in such practices are India, Indonesia, Mongolia, Oman, and the Philippines, each maintaining at least one more spyware variant within their inventory (in addition to Pegasus). Bahrain, Bangladesh, and Malaysia each demonstrate the presence of two supplementary spyware systems. Additionally, Indonesia and Kazakhstan are reported to possess no less than four other distinct spyware tools in their arsenals.[54] One tool used across the region is Finfisher/FinSpy. The tool has been reportedly used by Bahrain against Arab Spring activists and in Jordan to monitor HRDs, among other countries. Another tool, by "Hacking Team" was deployed in Thailand during 2013–2014 against civil society organisations.[55]

To note, during the COVID-19 period, reports have also been made that COVID-19 tracking apps were used for surveillance purposes or collected personal data in a government-operated database. These tracking apps were instated without proper independent review due to the emergency nature of the pandemic. However, no actions have been taken to address possible rights violations from these apps.[56]

2d. Information Operations

Another variant of digital threats faced by HRDs entails the use of social media accounts, facilitated by entities known as "cybertroops", comprising both human operatives and automated bots. These orchestrated efforts aim to shape public opinion and disseminate pro-government sentiments. Despite the persistent online nature of these attacks, governments have demonstrated a minimal commitment to addressing this pressing concern. More disconcerting is the complicity of government agencies in facilitating and supporting these cyberattacks.

[47] Marczak, Bill, Ali Abdulemam, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, John Scott-Railton, and Ron Deibert (2021) 'From Pearl to Pegasus: Bahraini Government hacks activists with NSO group Zero-click iPhone exploits', The Citizen Lab, at: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits.
[48] Shantha, Sukanya (2019) 'Indian activists, lawyers were "Targeted" using Israeli spyware Pegasus', The Wire, at: https://thewire.in/tech/pegasus-spyware-bhima-koregaon-activists-warning-whatsapp; Robinson, Kali (2022) 'How Israel's Pegasus spyware stoked the Surveillance debate', Council of Foreign Relations, at: https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate.
[49] Kirchgaessner, Stephanie (2022) 'Victim's iPhone hacked by Pegasus spyware weeks after Apple sued NSO', The Guardian, at: https://www.theguardian.com/world/2022/apr/05/apple-iphone-pegasus-spyware-nso-group-israel-jordan.
[50] Robinson (2022) 'How Israel's Pegasus spyware stoked the Surveillance debate'.
[51] Kirchgaessner (2022) 'Victim's iPhone hacked by Pegasus spyware weeks after Apple sued NSO'
[52] iLaw (2022) 'Parasite that Smiles: Pegasus Spyware Targeting Dissidents in Thailand', Ilaw Freedom, at: https://freedom.ilaw.or.th/en/report-parasite-that-smiles.
[53] Marczak, et al. (2021) 'From Pearl to Pegasus'.
[54] Fieldstein, Steven and Brian Kot (2023) 'Global Inventory of Commercial Spyware & Digital Forensics' *Mendeley Data* V10, DOI:10.17632/csvhpkt8tm.10.
[55] Ibid.
[56] Asia Centre (2023b) *Moving Beyond COVID-19 Restrictions in Southeast Asia: Pushing Back Against Authoritarian Pandemic Governance*, Bangkok: Asia Centre; Asia Centre (2023c) 'Moving Beyond COVID-19 Restrictions in South Asia: Pushing Back Against Authoritarian Pandemic Governance', Asia Centre, at: https://asiacentre.org/wp-content/uploads/Moving-Beyond-COVID-19-Restrictions-in-South-Asia.pdf.

A comprehensive global survey conducted in 2020[57] sheds light on this issue. The survey identified evidence of social media manipulation in 13 out of the 26 APF member countries.[58] Within this subset of 13 countries, all except Indonesia exhibited clear indications of government agencies deploying "cybertroops" – whether human or bots – to launch attacks against HRDs. The **South Korean** intelligence agency (the National Intelligence Service) has been reported to use information operations domestically to attack activists, and opposition politicians as sympathisers of North Korea.[59] This muddles the works of legitimate HRDs, who made comments regarding key rights violations and policy mistakes of the government, with North Korea-planted activists. This tactic was also reportedly used during the electoral period in 2012 to boost the positive sentiments for former president Park Geun-Hye, who was then one of the candidates.

There is evidence showing that, in **Kyrgyzstan,** "troll farms" have been used systematically by pro-government parties since 2018.[60] One report found that the national agency for TV and radio is, at least in part, operating the network. The agency works closely with the presidential administration to manage information online.[61] Comments proliferate online during election seasons[62] to promote pro-government politicians. But they are also used to harass HRDs. For example, during a corruption scandal involving a politician, fake accounts were deployed en masse to deflect criticism and disrupt online narratives that were critical to the individual.[63]

In the case of **Indonesia,** while without clear evidence of government-sponsored disinformation online, there is a high level of pro-government cybertroop activity in the country. Controversial laws which saw criticism by HRDs and mass protests such as the Omnibus Law of 2020[64] are supported by the proliferation of such cybertroop activities that come to the defence of the government.[65] Little to no action has been taken against such activities online.

Therefore, as it has been shown, the digital security landscape facing HRDs in the Asia-Pacific region is characterised by a complex interplay of legal restrictions, communication disruptions, state surveillance, and information operations. These multifaceted challenges pose a grave threat to freedom of speech and expression, warranting sustained attention and concerted efforts to safeguard the rights and safety of HRDs in the digital age. In this context, the next chapter outlines the actions taken by NHRI to address these series of issues undermining the activism of HRDs in the Asia-Pacific region.

[57] Bradshaw et al. (2021) *Industrialised Disinformation*.
[58] Australia, Bahrain, India, Indonesia, Iraq, Kazakhstan, Kyrgyzstan, Malaysia, Oman, Qatar, South Korea, Sri Lanka, Thailand.
[59] Ibid.
[60] CABAR (2022) 'Kyrgyzstan's troll farms', Institute for War & Peace Reporting, at: https://iwpr.net/global-voices/kyrgyzstans-troll-farms.
[61] RFE/RL Kyrgyz Service (2023) 'Kyrgyz President's Office denies claims it runs a "troll factory"', RFE/RL, at: https://www.rferl.org/a/kyrgyzstan-troll-factory-ntrc-japarov/32478310.html.
[62] CABAR (2022) 'Kyrgyzstan's troll farms'.
[63] Bradshaw et al. (2021) *Industrialised Disinformation*.
[64] Lane, Max (2020) 'Protests Against the Omnibus Law and the Evolution of Indonesia's Social Opposition', *Perspective* No. 128, ISEAS Yusof Ishak Institute, at: https://www.iseas.edu.sg/wp-content/uploads/2020/11/ISEAS_Perspective_2020_128.pdf.
[65] Sastramidjaja, Yatun and Wijayanto (2022) 'Cyber Troops, Online Manipulation of Public Opinion and Co-optation of Indonesia's Cybersphere', *Trends in Southeast Asia,* Issue 7, ISEAS Yusof Ishak Institute, at: https://www.iseas.edu.sg/wp-content/uploads/2022/03/TRS7_22.pdf.

3. NHRIs: Their Efforts & Limitations

This chapter employs the conceptual framework in the Regional Action Plan (RAP) to evaluate the operational effectiveness of NHRIs in safeguarding and facilitating essential assistance for HRDs confronting digital security threats. The structure of this chapter is organised into three sections, aligning with the objectives of the RAP: first, the monitoring and documentation of infringements against HRDs; second, active advocacy and awareness-raising; and third, the building of institutional capacities and expansion of collaborative networks.

3a. Monitoring & Reporting

A series of Action Plans delineates a directive for NHRIs to establish a mechanism dedicated to the monitoring and reporting of violations against HRDs, which lays a foundation for an effective complaints-handling system that identifies HRDs. This includes the systemisation of an early warning mechanism, documenting instances of HRDs facing violations and facilitating a regional database of HRD violations. This then feeds into a targeted HRD relocation and respite programme.

NHRIs within the region currently lack robust mechanisms essential for the effective execution of these prescribed tasks. Critical components of such a mechanism, including HRD focal point personnel, rapid response teams, dedicated hotlines, and emergency communication channels – which collectively constitute the early warning system – as well as the broader complaint-handling infrastructure within NHRIs, were absent in numerous commissions. For example, only 2 (out of 26 countries) were found to possess a focal point staff on HRD violations and 9 had a hotline for urgent human rights violations.

Even in instances where these mechanisms were present, they were not purposefully designed to comprehensively monitor and meticulously track the various manifestations of violations against HRDs, as mentioned in the previous chapter.

Another issue also stems from the lack of capacity to identify cases as being an undue targeting of HRDs. This is a result of a limited understanding of who constitutes HRDs as well as a lack of overview of how such violations of rights cause further effects in the diminishing of HRD's works and calls for public accountability.

As a result, a review of reports on human rights situations and annual achievements from NHRIs revealed that, in the study's scope covering 26 countries, these institutions predominantly assessed the impact of digital security threats on HRDs by using case examples, rather than presenting a statistical analysis of violations. This approach was notable in 11 countries: Bangladesh, Indonesia, Jordan, Malaysia, Nepal, Palestine, Philippines, Qatar, South Korea, Sri Lanka, and Thailand.

Multiple NHRIs displayed a trend of reporting the practical application of laws that had the potential for misuse. For instance, the National Commission for Human Rights (NCHR) recorded instances related

to the enforcement of Article 11 in the Cybercrime Law No. 27 (2015),[66] although it did not explicitly mention its utilisation against HRDs.[67]

Among NHRIs, only KOMNAS HAM[68] consistently maintained records and reported on the repression of Human Rights Defenders (HRDs) through digital means. In 2021, they reported tracking freedom of expression violations and noted that a significant share occurred in digital spaces. Additionally, they compiled cases from a local civil society organisation (CSO) regarding the use of the Law on Electronic Information and Transactions, which is often employed against HRDs in the country.

As demonstrated in these examples, limitations in NHRIs' monitoring system have hindered their ability to comprehensively and systematically report violations against HRDs, particularly concerning digital rights violations. Additionally, a review of NHRI activities during the specified period reveals a lack of regional-level interactions and information-sharing efforts related to digital security, which is crucial for creating a regional dataset of violation cases. Such a regional collaboration, as outlined in the RAP, would facilitate cross-border coordination among NHRIs to monitor rights violations that transcend national borders and develop targeted relocation and support programs.

These limitations raise several concerns. Firstly, an underprepared system underreports digital violations against HRDs, leading to an incomplete understanding of the rights violation landscape and the inability to identify emerging trends, both domestically and internationally. Secondly, the lack of accountability may perpetuate a culture of impunity among perpetrators of violence.

Furthermore, these limitations diminish NHRIs' capacity to advocate for and raise awareness about such tactics, which is a crucial element of the RAP. This issue will be further developed in the next Section.

3b. Advocacy & Awareness Raising

As noted above, fewer than 50% of NHRIs monitored and reported digital security threats and violations on HRDs in their respective jurisdictions. Therefore, only this subset of NHRIs conducted advocacy & awareness-raising. However, without a toolkit that would have guided a capable monitoring and reporting process and provided evidence of cases and statistics, the advocacy efforts of NHRIs lacked solid support. Nevertheless, despite this limitation, efforts were made to shed light on the situation.

NHRIs concentrate on advocacy with duty-bearers by reporting on legal developments and assessing laws that affect freedom of expression in their country. These assessments were made without specific reference to HRDs. **NHRCK**[69] assessed a proposed amendment to a press law and highlighted the vague definitions of fake news and disinformation in the amendment, expressing concerns about

[66] "Information Systems and Cyber Crime Law No. 27" (2015), Cyrilla, at: https://cyrilla.org/en/entity/6ikhnir665ikg0zz8ow2ymn29.
[67] NCHR (2023) 'The 18th Annual Report on the Situation of Human Rights in the Hashemite Kingdom of Jordan', NCHR, at: https://www.nchr.org.jo/media/kvydbxap/the-18th-annual-report-on-the-situation-of-human-rights-in-the-hashemite-kingdom-of-jordan-for-the-year-1443-ah-2021-ad-january-1-december-31-2021-ad.pdf.
[68] Komnas HAM (2021) 'Annual Report: Synergy & Collaboration for Human Rights Promotion & Protection 2021', Komnas HAM, at: https://pusdahamnas.komnasham.go.id/home/data_detail/cfa0860e83a4c3a763a7259e62d825349f7.
[69] NHRCK (2021) 'Annual Report 2021', NHRCK, at: https://www.humanrights.go.kr/download/BASIC_ATTACH?storageNo=1068931.

potential misuse. This would have restricted the sharing of information in the country. The scrutiny from various stakeholders, with NHRCK as one leading figure, contributed to the amendment being postponed for further review.[70]

NHRC of Qatar made the same assessment for the Cybercrime Law[71] – as terms such as "violating public order" were loosely defined. **NHRCN**, on multiple occasions[72] raised a concern regarding the IT Bill and its potential limitations against media freedoms. It also flagged the fact that the law was passed without proper consultation with stakeholders. **FHRADC** [73] made a submission to the relevant parliamentary committees regarding the Cybercrime Bill (in 2020) and Online Safety Bill (in 2018).

AHRC issued a report "The Need for Human Rights-centred Artificial Intelligence" in 2023.[74] Despite not referencing HRDs, the report contemplated digital-related laws to take into account freedom of expression and the right to privacy. Previously, it also submitted a report on the impact of digital technology on human rights to the Prime Minister and Cabinet (PM&C) Digital Technology Taskforce.

A relatively small number of NHRIs moved beyond a strictly legalistic approach and made reference to a pattern of harassment and advocated for the misuse of powers to be halted. However, they continued avoiding mentioning the impact on HRDs. The **NHRCB** stated that the Digital Security Act (2018) has been improperly used against journalists.[75] **SUHAKAM** expressed concern over a court decision that held an online media outlet guilty of contempt of court over displaying readers' comments which was found to be disrespectful to the court.[76] **NHRCT** mentioned the impact the Computer Crimes Act has had on journalists.[77] The law was used to prosecute them for reporting on policy mismanagement by the government. **KOMNAS HAM** referred to the targeted internet shutdown in West Papua and noted that the action was not in line with international human rights standards.[78]

[70] Shin, Hyonhee (2021) 'S.Korea's ruling party retreats on "fake news" law after backlash', Reuters,"at: https://www.reuters.com/world/asia-pacific/skoreas-ruling-party-retreats-fake-news-law-after-backlash-2021-09-30.
[71] NHRC (2018) 'The Fourteenth Annual Report: Human Rights Situation in Qatar 2018', NHRC, at: https://www.nhrc-qa.org/storage/annualReports/file_643fe811bd3ab_1681909777.pdf.
[72] NHRCN (2020a) 'Annual Report 2020', NHRCN, at: https://www.nhrcnepal.org/uploads/publication/Annual_Report_FY_2019-20_compressed.pdf; NHRCN (2020b) 'NHRC opinion regarding the Information Technology Bill (IT Bill)', Press Release, NHRCN, at: https://www.nhrcnepal.org/uploads/press_release/NHRC_opinion_regarding_the_Information_Technology_Bill_(IT_Bill).pdf; NHRCN, National Women Commission, and National Dalit Commission (2020) 'The NHRI Nepal Joint Submission for The Third Cycle Universal Periodic Review of Nepal November 2020', OHCHR, at: https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=8081&file=EnglishTranslation.
[73] FHRADC (2018) 'Resources', FHRADC, at: https://www.fhradc.org.fj/resources.
[74] AHRC (2023) 'The Need for Human Rights-centred Artificial Intelligence', AHRC, at: https://humanrights.gov.au/sites/default/files/the_need_for_human_rights-centred_artificial_intelligence_0.pdf.
[75] NHRCB (2018) 'Annual Report 2018', NHRCB, at: http://nhrc.portal.gov.bd/sites/default/files/files/nhrc.portal.gov.bd/page/cb8edec9_5aee_4b04_bf2a_229d9cd226a0/Annual%20Report-2018%20English.pdf.
[76] SUHAKAM (2021) 'SUHAKAM Expresses its Concern of the Federal Court Decision on Malaysiakini', Press Statement, SUHAKAM, at: https://suhakam.org.my/2021/02/press-statement-no-10-2021_suhakam-expresses-its-concern-of-the-federal-court-decision-on-malaysiakini.
[77] NHRCT (2020) 'Human Rights Situation in Thailand: The National Human Rights Commission of Thailand submitted to the HRC under the Third Cycle of the UPR', OHCHR, at: https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=8823&file=EnglishTranslation.
[78] KOMNAS HAM (2020) 'Submission to Human Rights Committee: List of Issues Prior to Reporting (LOIPR) on Indonesia's anticipated 2nd periodic report under the International Covenant on Civil and Political Rights (ICCPR)', OHCHR.

Some provided their opinions regarding how the government should maintain a balance between digital toolkits and human rights and the rule of law.[79] **ICHR**, in May 2018,[80] cautioned against the misuse of the then newly issued law on cybercrimes to infringe upon freedom of expression and the right to privacy online. **NHRCB**[81] and **NIHR**[82] urged their respective governments not to misuse relevant laws in the country to impact digital rights.

Despite their efforts, the recognition and acknowledgement of surveillance and coordinated online harassment falls short.

NHRCK, for example, has undertaken advocacy projects on the issue of big data and AI-based surveillance.[83] Meanwhile, the "Human Rights & Technology" streams of work undertaken by AHRC have brought up the concern of the right to privacy online as they concern social media and AI.[84] However, state-operated surveillance projects remain unaddressed by these institutions.

Upon review, only three NHRIs had substantive advocacy on surveillance. In the submission to the UPR process of the Philippines in 2022, **PHRC** raised a concern that the provisions of the Anti-Terrorism Law permit surveillance of HRDs.[85] **ICHR** reported that hackers linked to the government target journalists and HRDs.[86] **HRCSL** emphasised governmental actors to deter from subjecting HRDs to surveillance, to enable them to work effectively.[87]

On disinformation, nearly all NHRIs that submitted reports mentioned the increased hate speech and disinformation online. However, no reference was made to the targeting of HRDs or evidence that linked such coordinated attacks to government authorities. Instead, disinformation and hate speech are mentioned in the context of sexual or ethno-religious violence perpetrated by individuals, without addressing attacks against HRDs and others who hold government officials accountable for their wrongdoings or voice grievances to the public. In this regard, only **PHRC** cautioned its government to

[79] NIHR (2021) 'Ninth Annual Report of the National Institution for Human Rights in the Kingdom of Bahrain', NIHR, at: https://www.nihr.org.bh/MediaHandler/GenericHandler/2022/NIHR_Annual%20Report%202021%20EN.pdf; NCHR (2023) 'The 18th Annual Report on the Situation of Human Rights in the Hashemite Kingdom of Jordan', NCHR, at: https://www.nchr.org.jo/media/kvydbxap/the-18th-annual-report-on-the-situation-of-human-rights-in-the-hashemite-kingdom-of-jordan-for-the-year-1443-ah-2021-ad-january-1-december-31-2021-ad.pdf; HRCSL (2023a) 'Recommended Guidelines to the State and Law Enforcement Officials on Dealing with Civilian Protests', HRCSL, at: https://www.hrcsl.lk/wp-content/uploads/2023/05/Recommended-Guidelines-to-the-State-and-Law-Enforcement-Officials-on-Dealing-with-Civilian-Protests-by-HRCSL_English.pdf

[80] ICHR (2018) 'ICHR welcomes the issuance of Law by Decree No. (10) 2018 on electronic crimes and introduces a series of observations and reservations', Statement, ICHR, at: https://www.ichr.ps/en/media-center/2595.html.

[81] NHRCB (2018) 'Stakeholder Report to UN Human Rights Council on Universal Periodic Review – 3rd Cycle', NHRCB, at: http://www.nhrc.org.bd/sites/default/files/files/nhrc.portal.gov.bd/notices/97b99286_2d85_4a88_a979_ae3daf1ca391/3rd%20cycle-%20final%20report%205th%20October.pdf.

[82] NIHR (2018) 'Parallel Report submitted by the National Institution for Human Rights on The Initial Report of the Kingdom of Bahrain regarding the progress made in the implementation of the provisions of the International Covenant on Civil and Political Rights', CCPR Centre, at: https://ccprcentre.org/files/documents/INT_CCPR_NHS_BHR_30835_E.pdf.

[83] NHRCK (2021) 'Annual Report 2021', NHRCK, at: https://www.humanrights.go.kr/download/BASIC_ATTACH?storageNo=1068931; NHRCK (2022) 'Annual Report 2022', NHRCK, at: https://www.humanrights.go.kr/download/BASIC_ATTACH?storageNo=10002967.

[84] AHRC (nd.) 'Technology and Human Rights', AHRC, at: https://humanrights.gov.au/our-work/technology-and-human-rights.

[85] PHRC (2022) 'Submission of the Commission on Human Rights of the Philippines on the Occasion of the Fourth Cycle Universal Periodic Review on the Philippines', OHCHR, at: https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=10275&file=EnglishTranslation.

[86] ICHR (2023) 'Shadow Report Submitted by the Independent Commission for Human Rights (ICHR) to the Human Rights Committee on the First Periodic Review of the State of Palestine', OHCHR, at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCCPR%2FIFL%2FPSE%2F48533&Lang=en.

[87] HRCSL (2023b) 'The HRCSL's Report relating to Civil and Political Rights within the Country for the review of Sri Lanka (6th Periodic Report) by the Human Rights Committee during its 137th Session', OHCHR, at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2FCCPR%2FIFL%2FPSE%2F48533&Lang=en.

take action against online gendered attacks which are directed against women HRDs. It specifically called out against "misogyny perpetrated by authorities".[88] (2022).

Furthermore, discussions of HRDs are generally avoided in public-facing platforms such as their social media profiles, resulting in diminished awareness-raising about the situation. In reference to "digital" and "online", the focus throughout the 26 countries is on awareness-raising on access to the internet or cyber threats against women and children. Other NHRIs, which have a stream of advocacy related to civil liberties, tended to promote awareness-raising on protecting the right to privacy online and the proliferation of hate speech on social media platforms. This is done with minimal mention of HRDs.

Overall, the advocacy and awareness-raising efforts are limited by a lack of a systematic monitoring and reporting mechanism. As a result, over half of NHRIs avoided mentioning digital threats faced by HRDs in their countries. Among those that did, there was a limited understanding of the different legal and non-legal means that, together, are used to impose harm onto HRDs and impede their activities.

3c. Capacity & Network Building

The last set of Action Plans relates to capacity-building and network-building activities at the national and international levels for HRDs and within the NHRIs. These plans aim to enhance the capabilities and collaborations of HRDs and NHRIs, facilitating their work in promoting and protecting human rights. In this regard, there appear to be various forms of activities conducted. However, there is a clear lack of strategy for these engagements.

During the review period, a range of engagement methods with HRDs by NHRIs were found. For one, they engaged with civil society organisations and took part in their events and conferences. This allows them to connect with other civil society actors and provides such events with legitimacy and recognition. For example, **NHRCT** actively reports on its engagements with civil society actors and speaks at seminars and conferences related to digital rights, where it speaks up on the need to support HRDs.[89] **SUHAKAM** participated in and supported the convening of a national seminar on digital rights. It also partook in a multi-stakeholder meeting that discussed the impact of the Communication and Multimedia Act and another on "Freedom of Expression, Hate Speech and Internet Regulation in Malaysia". The two meetings brought together CSOs, MPs and representatives from the Commission.

Some NHRIs also convened (or supported in convening) international conferences. For example, **NHRCN**, in 2018, convened a human rights conference where some panel discussions centred on HRDs, digital rights and mass surveillance.[90] **PHRC** in 2019 convened a conference on human rights

[88] PHRC (2022) 'Submission of the Commission on Human Rights of the Philippines on the Occasion of the Fourth Cycle Universal Periodic Review on the Philippines', OHCHR, at: https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=10275&file=EnglishTranslation.

[89] NHRCT (2021) *'[Human Rights Comissioner Wasan joins the online discussion "Freedom of expression and information in times of crisis"]'*, NHRCT, at: https://www.nhrc.or.th/News/Activity-News/กสม-วสันต์-ร่วมเวทีเสวนาออนไลน์-เสรีภาพในการแสดงออ.aspx; NHRCT (2022) *'[Human Rights Comissioner Wasan joins regional workshop on human rights law and digital media for expression in Southeast Asia and South Asia]'*, NHRCT, at: https://www.nhrc.or.th/News/Activity-News/21919.aspx; NHRCT (2023) *'[Human Rights Comissioner Wasan joins the online discussion on the topic "Human Rights in Digital Media"]'*, NHRCT, at: https://www.nhrc.or.th/News/Activity-News/22954.aspx.

[90] Ansari, Mohna, Gaurav Bhattarai, Niha Pandey and Abishek Jha (eds.) (2018) *Human Rights And Impunity in South Asia: States, Societies and Institutions*, NHRCN, at: https://www.nhrcnepal.org/uploads/publication/Intl_Conference_Book_June_2018.pdf.

and the internet.[91] In 2018, **AHRC** convened the "Human Rights & Technology Conference" where it launched its multi-year project on human rights & technology and presented an issue paper on this topic.[92]

Another stream of capacity-building events is those that are presented as training focused on media professionals. This is notable for NHRIs in countries such as Bahrain and Qatar. While not explicitly mentioned by these NHRIs during the events, journalists and social media activists are a group of civil society actors that constitute HRDs. **NIHR** of Bahrain organised the "Training Program in the Field of Human Rights for Journalists" which brought together journalists and CSOs in the field of media. In Qatar, in 2021, the NHRC convened a panel discussion on media and the right to information[93] and another for the occasion of World Press Freedom Day.[94] The 2020 conference "Social Media Pioneers" brought together social media activists to share experiences and build a network.[95]

Several activities seek to build cooperation among NHRIs regarding digital rights at the regional and international levels. For one, GANHRI is building up a portfolio of work regarding the intersection of the role of NHRIs and the digital rights of HRDs. The knowledge exchange session held on the side of the 2022 GANHRI Annual Meeting allows NHRI representatives to talk about the impact of digitalisation and reflect on what steps NHRIs should take to help ensure human rights and civic space are protected in the digital era.[96] The Global Action Plan for NHRIs that followed, took note of the key concern regarding the increased threats for HRDs from the development of digital technologies.[97]

Another ongoing project is the NHRI Digital Rights Alliance which started in November 2021. The Alliance is established as an informal network of NHRIs "aimed at strengthening the human rights compliance of digital technologies implications". The Alliance includes the participation of the NHRIs of Australia, Mongolia, New Zealand and Palestine (among NHRIs in other regions). Previously in December 2021, the Alliance convened a webinar that discussed the role of NHRIs as "digital rights watchdogs".[98] To build on its goals and aims, it is in the process of developing a toolkit to support the work of NHRIs.[99]

Overall, while engagements – both aimed at HRDs and NHRIs – are varied, they currently fall short of the stated aim of the RAP. One area is in building up NHRIs' capacity to monitor and report on violations of rights.

[91] PHRC (2020) 'Annual Report FY2019', PHRC, at: https://chr.gov.ph/wp-content/uploads/2021/02/CHR-2019-ANNUAL-ACCOMPLISHMENT-REPORT.pdf.
[92] AHRC (2019) 'Annual Report 2018-2019', AHRC, at: https://humanrights.gov.au/our-work/commission-general/publications/annual-report-2018-2019.
[93] NHRC (2021a) '*[The National Human Rights Committee organizes a panel discussion on media and the right to know]*', NHRC, at: https://www.nhrc-qa.org/news/the-national-human-rights-committee-organizes-a-panel-discussion-on-the-media-and-the-right-to-knownhrc5OMT/page.
[94] NHRC (2021b) '*[In cooperation with the National Human Rights Committee, Al Jazeera organizes a panel discussion on the occasion of World Press Day]*', NHRC, at: https://www.nhrc-qa.org/statement-page/in-cooperation-with-the-national-human-rights-committee-al-jazeera-organizes-a-panel-discussion-on-the-occasion-of-world-press-daynhrcoNim.
[95] NHRC (2020) '*[Under the patronage of His Excellency Khalid bin Khalifa bin Abdulaziz Al Thani, Prime Minister and Minister of Interior, the international conference on "Social Media Pioneers" was launched today]*', NHRC, at: https://www.nhrc-qa.org/statement-page/under-the-patronage-of-his-excellency-sheikh-khalid-bin-khalifa-bin-abdulaziz-al-thani-prime-minister-and-minister-of-interior-the-international-conference-on-social-media-pioneers-was-launched-todaynhrcGJfM.
[96] GANHRI (2022a) '2022 Knowledge Exchange', GANHRI, at: https://ganhri.org/2022-knowledge-exchange.
[97] GANHRI (2022b) 'GANHRI Global Action Plan to support the protection and promotion of human rights defenders and civic space', GANHRI, at: https://ganhri.org/wp-content/uploads/2022/04/Global-Action-Plan-on-HRDs-and-civic-space_EN.pdf.
[98] Ombudsman NHRI Samoa (2022) 'Annual Report FY2021-2022', Ombudsman NHRI Samoa, at: https://www.ombudsman.gov.ws/wp-content/uploads/2023/01/FINAL-Annual-report-2021-2022_-ENGLISH.pdf.
[99] Tech for Democracy (2023) 'National Human Rights Institutions as Digital Rights Watchdogs', Tech for Democracy, at: https://techfordemocracy.dk/action-coalitions/national-human-rights-institutions-as-digital-rights-watchdogs; The Danish Institute for Human Rights (nd.) 'NHRI Digital Rights Alliance', The Danish Institute for Human Rights, at: https://www.humanrights.dk/projects/nhri-digital-rights-alliance.

For example, there are no current efforts to build a regional-level dataset or research on cases of digital rights violations that could potentially allow NHRIs to understand how HRDs under their support are threatened. In that regard, the NHRI Digital Rights Alliance could undertake such data collection efforts in addition to developing a toolkit for NHRIs.

Another area of concern relates to the assessment and evaluation of NHRIs' work. Their annual reports and strategic plans do not offer a thorough review of their activities, identifying gaps, or considering potential shifts in their areas of focus. There is also no mention of whether such an assessment is conducted regarding their programs aimed at safeguarding the digital rights of HRDs.

Similarly, while NHRIs have conducted various activities aiming to build capacity and network among HRDs, no assessment has been made of their effectiveness. These concerns lie in the lack of a clear strategy and goal for the engagements. As no NHRIs indicated the digital rights of HRDs as a key programmatic area in their annual reports nor their multi-year strategic/corporate/action plans, engagements and capacity-building – bar for some NHRIs – appear to be ad-hoc, without programmes that follow through these activities into further actions taken. A best practice can be observed from AHRC, which established the "Human Rights & Technology" programme, which includes research, advocacy and engagement with government officials, as well as capacity-building activities with stakeholders in the country.

In summary, NHRIs in the region lack a comprehensive work plan to support HRDs against digital security threats they encounter. They lack strong mechanisms for monitoring and reporting violations from the outset. Consequently, their advocacy, capacity-building, and networking initiatives are not well-targeted to the specific issue found in their jurisdiction. Given this assessment, the next chapter will present a series of recommendations for NHRIs.

4. Recommendations

This report has identified the key online threats faced by HRDs in the Asia-Pacific region. With this, it has been able to scrutinise how NHRIs address these challenges, thus identifying how its institutional performance can be improved. This chapter provides a set of recommendations for NHRIs to do so. To increase their institutional capacity and ensure that the rights of HRDs in the online sphere are respected, NHRIs should:

- Formulate and share a strategy for safeguarding the digital rights of HRDs, featuring specific objectives, action plans, and annual progress reports, with the flexibility to adapt it globally while catering to individual national needs. Concurrently, offer parliament recommendations to harmonise their roles with international human rights principles, bolstering their effectiveness in fulfilling their functions.
- Strengthen and expand the capabilities of the monitoring and reporting system to encompass digital security threats and detect HRD-specific violations that transcend legal boundaries. These digital security threats involve government policies within relevant ministries, internal security actions aimed at disrupting communications, online surveillance, and content manipulation. By gaining a comprehensive understanding of the multifaceted nature of digital security threat violations, we establish a solid foundation for more effective reporting and advocacy efforts.
- Establish a comprehensive monitoring and reporting system capable of addressing the complex interplay between digital rights violations and other fundamental rights and liberties. This entails:
    - Enhance ongoing monitoring of digital security concerns raised by HRDs and international organisations to safeguard their uninterrupted work and protect against unwarranted disruptions.
    - Comprehensively document and report on digital rights violations, including communication disruptions and surveillance in regions with significant ethno-religious minority populations, gender-specific online content manipulation impacting women HRDs, and racially biased online attacks targeting HRDs connected to or supporting ethno-religious minorities.
    - Elevating concerns regarding digital security threats against HRDs to public awareness. This can be done by developing an Advocacy Plan with the aim of sharing NHRIs' reports and recommendations through social media in bite-sized digital content.
- Promote public awareness of digital security threats against HRDs by developing an Advocacy Plan that shares NHRIs' reports and recommendations via bite-sized digital content on social media. Additionally, actively participate in civil society-led events and conferences, and consider organising national or international events to facilitate safe networking and information-sharing among HRDs, NHRIs staff, and government officials.
- Build on the current early warning system for it to be able to identify digital security risks against HRDs. This includes training focal point staff to understand issues related to digital threats as well as ensuring the complaints system is protected from external surveillance and monitoring.

- Aggregate third-party (civil society, tech companies and others) monitoring datasets and incorporate them into NHRI reports in areas where NHRIs currently lack the capacity and resources to conduct monitoring independently. NHRI representatives can also engage with CSOs where they can gather key information.

- Support the judicial process to ensure evidence gathering of HRDs and their activities are presented and considered before the law to avoid judicial bias in legal proceedings brought up against them.

- Increase their engagement at the parliamentary level, such as in annual report sessions or parliamentary committees. NHRIs should provide their expert opinions on the impact and/or potential misuse of key laws and regulations as well as gaps in the government policies that allow them to wield power to disrupt communications, surveil HRDs and conduct information operations.

- Enhance their interactions with tech companies and ISPs to offer expert guidance on ensuring the protection of online rights within their platforms and services. This includes ensuring freedom of expression is protected and HRDs are able to share critical information online. This also includes deterring attempts to surveil their activities online.

- Extend their more robust digital rights and HRD programming, whether within or beyond the Asia-Pacific region, by offering capacity-building to staff at other institutions. This can be achieved through the provision of comprehensive information on the scope of work, guidance on monitoring, reporting, and advocacy, and specialised training for their personnel.

- Encourage and provide the necessary support to regional and international level NHRI associations (eg. GANHRI and APF) to produce supporting documents such as research and toolkits to strengthen the role of NHRIs. NHRIs can also take part and engage with the NHRI Tech Alliance.

5. Conclusion

In a global context where the internet has become one of the backbones of our societies, the UN has noted that "human rights apply online just as they do offline".[100] This is a fundamental principle considering that digital technologies offer fresh avenues for the exercise of human rights, yet they frequently find themselves employed in the infringement of these very rights. Therefore, mitigating these new online threats has become essential in ensuring human rights for all, including human rights defenders (HRDs).

HRDs play a key role in defending people's rights. In this context, National Human Rights Institutions (NHRIs) play a crucial role in addressing complaints and supporting HRDs in their advocacy efforts. The Regional Action Plan (RAP) provides a framework for NHRIs in the Asia Pacific. With seven national and eight regional action points the RAP emphasises the importance of enhancing HRDs' capacity and networks to enable effective collaboration in promoting and protecting human rights across the region. The plan also highlights the NHRIs' essential role in engaging with stakeholders, including those responsible for upholding human rights and the public, to raise awareness of the challenges faced.

Implied in the RAP – though not made explicit – is the need to address security threats emanating from digital measures targeting HRDs. In such regard, this report sheds light on the advancement of human rights in the Asia Pacific by increasing the institutional capacity of NHRIs in two ways.

First, it identifies the key digital threats many HRDs face in the region when advocating for human rights. The report shows that governments in the Asia Pacific have used internet-related laws to criminalise free speech in digital spaces, enacted regulations to control online information flow, deployed internet surveillance technologies and hacking tools to monitor HRDs, and engaged in covert information operations. These multifaceted obstacles seriously jeopardise freedom of speech and expression, demanding ongoing focus and collaborative endeavours to protect the rights and safety of HRDs in the digital era.

Second, it contrasts these threats against the RAP principles, thus identifying areas for improvement for NHRIs to better support HRDs in the region and, more importantly, give them more tools to ensure their digital safety. NHRI's institutional capacity to support HRDs comprises three essential elements: rigorous monitoring and documentation of infringements against HRDs are vital, creating a comprehensive evidence base to address violations effectively; active advocacy and awareness-raising efforts are crucial, involving campaigns, lobbying, and public engagement to mobilise support and influence policymakers; building institutional capacities and fostering collaborative networks among HRD organisations enhance their ability to protect and promote human rights. Together, these pillars form a comprehensive strategy for bolstering the critical work of HRDs.

In the digital age, it is crucial for NHRIs to enhance their institutional capacity to effectively address digital threats. This not only protects the rights of HRDs but also aligns with the UN's goal of ensuring human rights in the digital sphere. To achieve this, NHRIs require a comprehensive action plan involving strategy development, alignment of mandates with international human rights principles, improved digital security monitoring, addressing intersections with other liberties, and documenting violations with a focus on minority and gender issues. Additionally, NHRIs should collaborate with law enforcement, participate in parliamentary discussions, digitally raise public awareness, engage HRDs in technology programs, work with tech companies, attend civil society events, offer capacity-building to other NHRIs, and support regional/international NHRI associations.

While digital threats will persist due to their evolving nature, these recommendations empower NHRIs to adapt the RAP to the digital age, developing specific, contextual strategies to help HRDs mitigate some of these threats.

[100] UN Office of the Secretary-General's Envoy on Technology (2023) 'Ensuring the protection of human rights in the digital era', UN, at: https://www.un.org/techenvoy/content/digital-human-rights.

Asia Centre, a civil society research institute, holds 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, focusing on four key themes: freedom of religion or belief, freedom of speech, freedom of association, and the right to political participation. Asia Centre collaborates with civil society stakeholders, international non-governmental organisations (INGOs), and parliamentarians to support their respective initiatives. Asia Centre operates from three offices in Bangkok (Thailand), Johor Bahru (Malaysia), and Phnom Penh (Cambodia).

The Asia Pacific Forum of National Human Rights Institutions (APF) is a network of 26 National Human Rights Institutions (NHRIs) working together to build an Asia Pacific where human rights are universally enjoyed and respected. A fundamental goal of the APF is to support the establishment of independent NHRIs and strengthen the capacity of its members through a range of services including tailored capacity development programs, advice on NHRI legislation and international accreditation, capacity assessments and leadership services. The APF fosters collaboration among its members and establishes partnerships with others to address some of the most serious and complex human rights challenges in the region. It works closely with governments, civil society organisations, regional human rights bodies, and the international community to build strong partnerships and enhance the impact of its members.