DigitalReach

DIGITAL RIGHTS
IN SOUTHEAST ASIA 2021/2022

DigitalReach

About DigitalReach

DigitalReach was founded in 2019 with the objective of assessing the impact of technology on human rights in Southeast Asia. The organization's mission is to safeguard digital rights and internet freedom in the region. Our work revolves around three core strategies, which are research and monitoring, advocacy, and community building and empowerment.

Published in 2022 by DigitalReach

Report Design : Control A All Design

Contact :
E-mail : controladesign@gmail.com
Facebook : https://m.facebook.com/ControlAalldesign

Table of Contents

List of Infographics

Methodology

This report is based on the organization's monitoring of situations across Southeast Asia in which technology is impacting human rights. Covering January-December 2021, the analysis was primarily conducted using secondary resources such as news articles, press releases and reports. Reference materials were selected based on their creditability. The analysis for this report was conducted based on international human rights standards.

Digital Rights in Southeast Asia 2021

Key Takeaways

- Southeast Asia is witnessing increasingly sophisticated tactics in terms of digital authoritarianism.
- The situation in Myanmar has dominated 2021 due to the severity of human rights violations, in which many tactics represent direct threats against digital rights. This situation is not only a national issue but also a regional issue that reveals how ASEAN perceives human rights.
- Freedom of expression in digital rights is at great risk as it faces more sophisticated threats. This includes the actions of governments across the region in attempting to control how social media platforms operate, the potential of information disorders expanding to emerging platforms, new forms of harassment against independent media, and the normalization of internet restrictions in Southeast Asia.
- Digital surveillance is on the rise in 2021 following the discovery of spy ware, believed to be Pegasus, one of the most sophisticated and powerful in the world, employed against Thai activists.
- Digital contact tracing, introduced by governments in 2020, is a failed approach according to health experts in many countries in the region, as it did not help to control the pandemic. However, many governments are still pushing for its use, while the transparency of the overall system remains a concern.
- Dissidents in Southeast Asia are likely to face more digital threats in the near future, but there is still uncertainty as to how prepared they are for these threats. Further research is needed to document and understand the extent of these threats in the local context. Capacity building activities based on the local context that can access the inner circle of targeted dissidents are also needed. Digital security protection should also be undertaken as a key process.
- State-sponsored information operations targeting political dissidents have tended towards greater sophistication in the region, yet independent fact-checking organizations that work on this issue are few, and face more threats from the state, as well as limited funding and resources. There is also a need to build more independent fact-checking initiatives.

Overview

One month into 2021, the situation in Myanmar fell under the world's spotlight with the Myanmar military, or the Tatmadaw in the local language, staging a coup d'état. The situation, including extreme levels of human rights violations, became the focus of attention of 2021, a situation in which digital authoritarianism played a significant role in the tactics used by the Tatmadaw to seize control of the country. This has included internet restrictions, the blocking of social media platforms, the dissemination of misinformation and disinformation, the coercion of telecom operators to comply with state surveillance, the proposing and amending of laws related to digital rights, the undisclosed use of surveillance tools, and the harassing of independent online media and the seizing of their equipment.

The situation in Myanmar does not only reflect digital authoritarianism at the country level but also at the regional level, with the Association of Southeast Asian Nations (ASEAN) taking little to no action in order to address the situation. ASEAN miscalculated by hosting a meeting in April 2021 to which they invited the head of the Myanmar military, Min Aung Hlaing, widely considered a criminal for heading the operation that had already killed over a thousand civilians. The meeting resulted in the announcement of a five-point consensus to solve the crisis, but little progress followed throughout 2021. The appointment, which sprung from the consensus, of the ASEAN Special Envoy, Erywan Yusof, in August 2021, to address the Myanmar crisis, also led to little of note. Furthermore, ASEAN leaders lobbied the United Nations to drop a call to suspend arms sales to the Myanmar military in May 2021. Even though Myanmar was barred from the ASEAN leaders' summit in October, the decision is considered to have been politically motivated rather than a serious commitment by the bloc to finally take serious action concerning the human rights situation in Myanmar.

Overall, human rights situations across Southeast Asia have long been a concern, and threats against human rights have increasingly crept into the digital space in recent years due to the prominence of the internet. Apart from what happened in Myanmar, 2021 showed that the region is facing more sophisticated tactics that threaten human rights, including the normalization of internet restrictions, regimes striving to control social media platforms, the expansion of information operations, the plan to establish national internet gateways, and escalations of digital threats. The incident of Thai activists being attacked by spyware believed to be Pegasus marks the first time that the use of such spyware has been publicly confirmed in Southeast Asia. In the Philippines, distributed denial-of-service (DDoS) attacks took a new turn in 2021 when the tactics used against media and fact-checking organizations, namely ABS-CBN, Rappler, and VERA Files, were discovered to be different from tactics previously used. The discovery of attacks from surveillance-for-hire firms on the platforms of Meta, known as Facebook until October 2021, also shows the extent to which dissidents are facing new forms of digital threats.

Based on the work by Digital Reach, the digital rights situation in Southeast Asia can be divided into three main themes; freedom of expression, the right to privacy, and digital security, with a particular focus on the situation

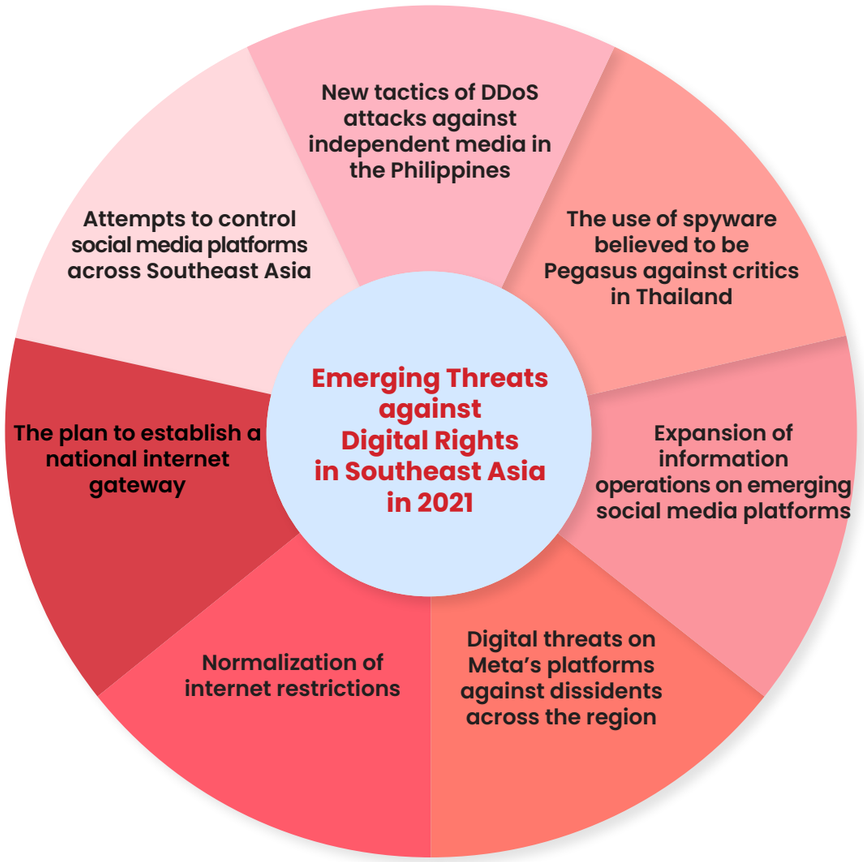
in Myanmar in 2021. Freedom of expression from the perspective of digital rights provides details on how governments across the region are trying to control social media platforms, how state-sponsored information disorders are becoming more sophisticated, how alternative media sources are being harassed, and how Southeast Asia is moving towards making internet restrictions the norm. The tightened control of social media platforms is seen to be a result of the social media activism of pro-democracy movements that have become more intense in recent years. State-sponsored information disorders are seen to become more sophisticated due to these tactics. It is also highly possible that this will expand to emerging platforms such as TikTok and Telegram. Independent alternative media continues to be suppressed by certain regimes in 2021. This harassment took a new turn in Malaysia, Singapore, and the Philippines, with the case against Malaysiakini, the Singaporean government's seeming obsession with foreign interference, and new tactics adopted vis-a-vis cyberattacks in the Philippines. Freedom of expression is also threatened by the normalization of internet restrictions that are influenced by political agendas in Myanmar and Indonesia.

2021 is also a year which saw a significant rise in digital surveillance. This has ranged from the discovery of the use of spyware in Thailand and the emergence of a surveillance state in Myanmar to the adoption of a law to establish the national internet gateway in Cambodia and Meta's discovery of dissidents being targeted by surveillance-for-hire firms. Despite the fact that countries in Southeast Asia are seen to be alert to efforts to protect personal data, the majority of those that have personal data protection laws are unlikely to protect individuals from digital surveillance as they do not include state agencies as part of the laws. Moreover, the inclusion of state agencies would collide with other existing laws that allow lawful interception by the state. 2021 also shows that the digital contact tracing that was initially rolled out in 2020 at a fast pace by governments across the region to tackle the pandemic has been a failed approach. Despite the continuation of many such tracing strategies, health experts across Southeast Asia have concluded that the approach has not played a significant role in bringing the pandemic under control. Digital contact tracing also leads to discrimination amongst the population as there will always be individuals who cannot afford smartphones and therefore remain unable to participate in these schemes.

In terms of digital security, threats against the security of dissidents are explored through three main areas; digital-related threats, threats from information disorders, and threats from repressive policies. Based on key situations in 2021, digital-related threats have intensified, given the rise of digital surveillance in the region. Dissidents are in need of support to understand these threats due to their technical aspects. Threats from state-sponsored information operations occur in the Philippines, Vietnam, Myanmar, and Thailand. There is a need to build more fact-checking initiatives and to empower existing ones as they are often subjected to harassment as well as lacking in resources and efficient tools. Threats from repressive policies against people's digital-related activities will also persist as these repressive laws related to digital space continue to be rolled out by governments in order to consolidate and maintain their power.

Despite Southeast Asia experiencing these emerging threats, there are also

concerns over whether civil society in Southeast Asia is adequately prepared for these threats. Areas of work including research, advocacy approaches, and capacity building of those that work on digital rights-related issues have to be adjusted to prepare for these specific threats. Further research is needed to gain a deeper understanding of these issues within the Southeast Asian context in order to respond to the situation efficiently. In addition to policy advocacy, pragmatic advocacy approaches are needed when an ongoing situation requires alignment with human rights principles. Capacity building related to digital rights protections needs to be conducted as a process that combines both preventive and reactive approaches and which is able to reach the inner circles of targeted dissidents. The activities should be designed based on the local context of Southeast Asia and maintain the flexibility to adapt and evolve as situations unfold.



I
Myanmar's Coup and Digital Authoritarianism

The coup in Myanmar constitutes the main focus of 2021 due to the extreme degree of human rights violations that have been perpetrated in the country. The Myanmar military used a range of tactics to establish their power and to suppress opposition following the coup. Unlike the coup d'état of 1962, when the internet was still unknown to the world, many of the tactics used by the Tatmadaw are related to digital space and the use of technology, reflecting the military's understanding of their importance and the key role that they can play in political situations.

These tactics have resulted in intermittent internet connections, limited access to social media platforms, pro-military propaganda that spreads like wildfire, justification of state surveillance, and dissidents being threatened or harassed for their pro-democracy activities. Human rights in Myanmar is at its lowest ebb since the opening up of the country in 2011, followed by the landmark election in 2015, when democracy's return to the country was widely hailed. The National League for Democracy (NLD) led by Aung San Suu Kyi, considered an icon of democracy at the time, won the landslide election and a bright and optimistic future seemed to lie ahead for the nation after remaining under military rule for 49 years from 1962 - 2011.

These events in Myanmar have implications for human rights both at the national and regional level. The reaction of the Association of Southeast Asian Nations (ASEAN) towards the human rights situation in Myanmar betrays the bloc's lack of concern. Given the extremity of the violations, it has set a precedent for how ASEAN can be expected to respond to other human rights violations in the future. ASEAN's failure to take efforts to restore democracy in Myanmar shows that human rights protection is not the bloc's priority, given the culture of authoritarianism in its member countries.

The Development of Key Digital Rights-related Events in Myanmar in 2021

Feb 1 — The military stages a coup. Internet is cut off from the early hours until late morning. The SAC is formed.

Feb 2 — A statement is released warning some media and citizens not to spread rumors on social media or incite unrest

Feb 2 — A national civil disobedience movement starts. A Facebook campaign group dubbed the "Civil Disobedience Movement" is launched.

Feb 3 — A boycott movement called "Stop Buying Junta Business" emerges, calling for the boycott of products and services linked to the Myanmar military.

Feb 4 — Facebook, Instagram, and WhatsApp are banned.

Feb 5 — Twitter is blocked.

Feb 6 — Internet blackout for 30 hours following nationwide protests. Foreign and local independent media are banned.

Feb 9 — The military proposes a cybersecurity law.

Feb 12 — Media reports that China is lending technical support to the Tatmadaw to develop a cyber firewall similar to the Great Firewall of China.

Feb 13 — Directives are issued to the media not to use the words "regime" and "junta."

Feb 13-15 — The military amends the Law Protecting the Privacy and Security of the Citizens, Law on Penal Code and the Electronic Transaction Law.

Feb 15 — The start of the third internet restrictions, occurring nationwide from 1 – 9 a.m.

Feb 19 — Wikipedia is blocked in all languages.

Feb 24 — Facebook announces the ban of the military from its affiliated platforms.

Feb 27 — The military dismisses Kyaw Moe Tun, Ambassador to the UN, from his position.

MAR 2 — Justice for Myanmar publishes details of surveillance tools used by the military.

MAR 8 — The media licenses of Mizzima, DVB, Khit Thit Media, Myanmar Now and 7 Day News are revoked.

MAR 18 — The military shuts down public Wi-Fi connections.

Apr 1 — The military orders telecommunications service providers to shut down wireless broadband internet services indefinitely. Daytime-fixed line service becomes the only way to access the internet.

Apr 14 — Facebook announces a specific policy for Myanmar to remove praise, support and advocacy of violence by Myanmar security forces and protestors from the platform.

Apr 16 — The Committee Representing Pyidaungsu Hluttaw (CRPH), representing 76 percent of the 498 democratically-elected members of Myanmar's parliament, announces the formation of the National Unity Government (NUG).

Apr 24 — Min Aung Hlaing joins the ASEAN Leaders' Meeting in Jakarta among calls for ASEAN not to invite him. The five-point consensus is adopted at the meeting.

Apr 28 — Fixed-line internet connectivity restrictions are eased in Myanmar.

May 8 — The military declares the NUG, CRPH, and resistance forces as "terrorist groups."

May 19 — Telecommunication and internet service providers are ordered to install intercept spyware.

May 25 — The military begin whitelisting some 1,200 approved internet services.

May 25 — NUG designates the military and its affiliated organizations as terrorist groups.

Jul 8 — Telenor announces an agreement to sell 100 percent of its mobile operations in Myanmar to the M1 Group.

Aug 1 — Min Aung Hlaing establishes himself as Prime Minister.

Aug 2 — The military amends the Counter Terrorism Law.

Aug 4 — ASEAN appoints Erywan Yusof as Special Envoy to Myanmar.

Oct 26-28 — The virtual ASEAN Leaders Summit takes place without the Myanmar military.

Nov 22 — The virtual ASEAN-China Summit takes place without the Myanmar military.

Dec 8 — Facebook announces a ban on military-affiliated businesses.

Dec 17 — The UN adopts a resolution to delay a decision on who will represent Myanmar, resulting in Kyaw Moe Tun remaining in his position.

Tactics of the Tatmadaw on Digital Rights Violations

The scale of digital authoritarianism in Myanmar is unprecedented in Southeast Asia. Different tactics were combined and used together over a one-year period, arousing widespread concern for the situation in Myanmar. These tactics betray the Myanmar military's efforts to control the internet and the way in which people use the internet. These tactics as a whole have ensured the Tatmadaw's control of power. The amendments to the digital rights laws allow the Tatmadaw to lawfully conduct surveillance, criminally charge those who form part of the pro-democracy movements whether the activities are online or offline and brand the opposition as terrorists. The amendments made lawful the use of surveillance tools, the raiding of the offices of independent media and confiscation of their electronic equipment, and the ordering of telecommunications service providers to comply with its surveillance efforts. Tactics, such as internet restrictions, a crackdown on independent media, whitelisting IP addresses, blocking social media platforms and Wikipedia, and state-sponsored information operations, are all considered strategies deliberately employed to control information in the online space. It is feared that all these tactics may enable the military to pursue the implementation of an internet firewall similar to the Great Firewall ofChina in the coming years.

1. Internet Restrictions

On February 1, 2021, Burmese citizens woke up to the news that their country was under the control of the Myanmar military following a military coup staged in the early hours. The coup was led by Senior General Min Aung Hlaing, an influential military figure who succeeded the country's long-time military junta, Than Shwe, in March 2011 as the Commander-in-Chief of the Armed Forces of Myanmar. Immediately following the coup, the internet became restricted at around 3 a.m. nationwide and resumed in the late morning. It was reported that armed military officers raided at gunpoint the data centers of internet providers at around midnight, resulting in a dramatic drop inconnectivity across the country[1] .

On February 6, as mass protests erupted nationwide in response to the coup, the military then imposed the second wave of internet restrictions that lasted for 30 hours. From February 15, the internet was blocked on a daily basis from1 a.m. – 9 a.m. local time. Internet restrictions were further enforced when mobile internet was blocked from March 15 onwards.

Internet service providers, without receiving any explanation, were ordered to shut down wireless broadband services until further notice on April 1, a move which affected all connections that use wireless routers[2] . This situation resulted in the unavailability of both the wireless broadband service and mobile internet,

1 Funakoshi, Minami, and Andrea Januta. "Myanmar's Internet Suppression." Reuters, 7 Apr. 2021, graphics.reuters.com/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo.

2 "Myanmar Orders Wireless Internet Shutdown until Further Notice: Telecoms Sources." Reuters, 1 Apr. 2021, www.reuters.com/article/us-myanmar-politics-internet/myanmar-orders-wireless-internet-shutdown-until-further-notice-telecoms-sources-idUSKBN2BO5H2?il=0.

leaving less than one percent of the country's inhabitants with access to the internet using fixed-line connections[3]. It is unclear when the fixed-line connections became restricted, but they resumed on April 28, as did access to mobile data and wireless broadband service[4].

The tactics of the Tatmadaw reveal their understanding of the importance and power of the internet. The longest internet blackout in Myanmar is deemed to have taken place in Rakhine and Chin States, lasting for 18 months, starting in June 2019, before being lifted shortly after the coup was staged in February 2021, as part of the NLD government's response sparked by the conflict between the Tatmadaw and the Arakan Army (AA). Together with the civilian government at the time, they claimed that the blackout was necessary to "maintain stability and law and order"[5]. During this period, the inhabitants of these states were greatly affected, with many remaining unaware of the existence of the COVID-19 pandemic. The objective of this restriction, implemented on February 1, 2021, the day of the coup, was to isolate people in the country to prevent them from reporting on the situation. Restrictions that were later enforced following the coup are viewed as an intention to suppress the pro-democracy movements. These actions have led to concerns that internet restrictions are likely to become a common and recurring tactic for the Tatmadaw to exercise their political agenda of maintaining control of the situation and preserving their power.

2. Blocking of Social Media Platforms, Wikipedia, and VPNs

In response to the coup, several resistance movements emerged, and online platforms became a crucial space for organizing initiatives, action and campaigns, and for reporting on the situation. The Civil Disobedience Movement was launched on February 2, 2021, and its Facebook group attracted approximately 100,000 members within a matter of hours after it was launched[6,7]. As half of Myanmar's inhabitants are Facebook users, Facebook became the most popular space from which to launch and organize campaigns and protest movements against the coup. On February 3, 2021, the military decided to block Facebook and its affiliated platforms, Instagram and WhatsApp. This deterrent, in turn, saw many people flock to Twitter, which was also subsequently blocked on February 5, 2021.

In addition to the blocking of social media platforms, Wikipedia was also blocked in all languages with no official reason provided by the authorities. The military banned the use of certain words related to the coup and to pro-democracy movements. Journalists and media, for instance, were prohibited from using words such as "junta" or "regime" as a result of the MOI's directives issued to the country's Press Council on February 13[8]. An "edit war" also broke out in a Wikipedia article's reference to Min Aung Hlaing's title and career[9].Virtual Private Networks (VPN), which enable users to circumvent content blocked in their areas, were

3 Robinson, Gwen, and Rory Wallace. "Myanmar Shutdown of Wireless Internet Fuels Fears of News Blackout." Nikkei Asia, 2 Apr. 2021, asia.nikkei.com/Spotlight/Myanmar-Crisis/Myanmar-shutdown-of-wireless-internet-fuels-fears-of-news-blackout.
4 "Myanmar's Junta Has Lifted the Overnight Internet Ban, and No One's Really Sure Why." Coconuts Yangon, 28 Jan. 2021, coconuts.co/yangon/news/myanmars-junta-has-lifted-the-overnight-internet-ban-and-no-ones-really-sure-why.
5 Preece, Cassandra, and Helen Beny. "Internet Blackouts in Myanmar Allow the Military to Retain Control." The Conversation, 17 Feb. 2021, theconversation.com/internet-blackouts-in-myanmar-allow-the-military-to-retain-control-154703.
6 Milko, Victoria. "EXPLAINER: How Are the Myanmar Protests Being Organized?" AP NEWS, 9 Feb. 2021, apnews.com/article/technology-aung-san-suu-kyi-myanmar-yangon-asia-pacific-026ad5eb9ad6920f0d0d5446e17e27c2.
7 "After Coup, Medical Workers Spearhead Civil Disobedience Campaign." Frontier Myanmar, 4 Feb. 2021, www.frontiermyanmar.net/en/after-coup-medical-workers-spearhead-civil-disobedience-campaign.
8 "Myanmar Military Bans Use of 'Regime', 'Junta' by Media." The Irrawaddy, 13 Feb. 2021, www.irrawaddy.com/news/burma/myanmar-military-bans-use-regime-junta-media.html.
9 "Internet Disrupted in Myanmar amid Apparent Military Uprising." NetBlocks, 28 Apr. 2021, netblocks.org/reports/internet-disrupted-in-myanmar-amid-apparent-military-uprising-JBZrmlB6.

also obstructed by the Tatmadaw[10], resulting in the inaccessibility of some free VPNs inside the country, while some paid VPNs continued to work at a slower speed, and with many individuals unable to afford the paid subscription[11].

3. Whitelisting the Internet Access

Whitelisting is a new tactic employed by the Myanmar military to limit access to websites considered to be critical towards the regime. After blocking social media platforms and Wikipedia, in May 2021 the Tatmadaw whitelisted over 1,200 online services and domain names considered to be acceptable for public viewing. Facebook and Twitter did not feature on the list but Instagram, YouTube, Netflix, Tinder, WhatsApp, LinkedIn, Viber and Zoom were whitelisted. Media sites such as The New York Times and CNN were also on the list. Issued by the Ministry of Transport and Communications this list was shared with local internet service providers and telecommunications companies. The reason given for whitelisting was to reconnect the education and small and mid-size enterprises (SMEs) sectors, and the internet service providers were requested to follow the order to ensure their accessibility as soon as possible[12]. It was revealed that the Tatmadaw ordered the telecommunications companies to blacklist hundreds of thousands of IP addresses[13].

4. Information Operations on Social Media Platforms

State-sponsored information operations on social media platforms have long been documented in Myanmar. The genocide against the Rohingya ethnic minority in 2017 was a result of disinformation and misinformation on Facebook. The false, fake, and misleading information on social media formed part of the Tatmadaw's operation on ethnic cleansing[14]. Facebook was heavily criticized following the incident. Many military-affiliated accounts were banned from the platform shortly after, including the account of Min Aung Hlaing[15].

Following the coup in February 2021, the company announced the ban of all Tatmadaw-associated content from Facebook and Instagram with immediate effect and later announced a ban on all pages, groups, and accounts associated with Tatmadaw in December[16]. The ban has resulted in the Tatmadaw and its supporters migrating to the emerging platforms, TikTok and Telegram. Pro-military propaganda, information disorder aiming to divide and confuse protestors, and death threats from military officials towards supporters of the pro-democracy movement, can be found on TikTok[17]. On Telegram, pro-military accounts banned from Facebook resurfaced on the platform. These accounts are found to target the Rohingya, the NLD party, and civilian

10 "Myanmar Junta Blocks Facebook, VPNs as The UN Security Council Voices 'Deep Concern.'" Radio Free Asia, 4 Feb. 2021, www.rfa.org/english/news/myanmar/facebook-blocked-02042021140109.html.
11 Beech, Hannah, and Paul Mozur. "How the Military Behind Myanmar's Coup Took the Country Offline." The New York Times, 23 Feb. 2021, www.nytimes.com/2021/02/23/world/asia/myanmar-coup-firewall-internet-china.html
12 "Myanmar Allows Tinder but Axes Dissent Havens Twitter, Facebook." Nikkei Asia, 25 May 2021, asia.nikkei.com/Spotlight/Myanmar-Crisis Myanmar-allows-Tinder-but-axes-dissent-havens-Twitter-Facebook.
13 "Whitelisted Internet Takes Myanmar Back to a 'Dark Age.'" Frontier Myanmar, 30 Jun. 2021, www.frontiermyanmar.net/en/whitelisted internet-takes-myanmar-back-to-a-dark-age.
14 Mozur, Paul. "A Genocide Incited on Facebook, With Posts From Myanmar's Military." The New York Times, 15 Oct. 2018, www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.a." The Irrawaddy, 13 Feb. 2021, www.irrawaddy.com/news/burma/myanmar-military-bans-use-regime-junta-media.html.
15 "Removing Myanmar Military Officials From Facebook." Facebook, 28 Aug. 2018, about.fb.com/news/2018/08/removing-myanmar-officials.
16 Frankel, Rafael. "An Update on the Situation in Myanmar." Facebook, 11 Feb. 2021, about.fb.com/news/2021/02/an-update-on-myanmar.
17 Guest, Peter, et al. "TikTok Is Repeating Facebook's Mistakes in Myanmar." Rest of World, 18 Mar. 2021, restofworld.org/2021/tiktok-is-repeating-facebooks-mistakes-in-myanmar.

arm resistance groups. Women who participated in the pro-democracy movement were also attacked through sexual harassment on Telegram[18].

The spread of information disorder that has shifted to emerging platforms is concerning as Telegram and TikTok's efforts to handle disinformation and misinformation on their platforms have been criticized as incompetent and as exacerbating such content. False, fake, and misleading information was also spread via text messages, with the aim of suppressing the pro-democracy protest. Among the messages commonly shared was the claim that the protestors were hired by the military to justify a more brutal crackdown on the general population[19].

5. Proposing and Amending the Laws Related to Digital Rights

After the coup, Min Aung Hlaing held absolute power with all legislative, executive, and judicial powers transferred to him. He established the State Administration Council (SAC), a government authority that replaced the NLD government during the state of emergency. The SAC proposed a cybersecurity law, and its draft was shared with telecommunications service providers and other related businesses in Myanmar on February 9, 2021. The draft bestowed the Tatmadaw with significant powers to censor, brand content critical of the military as disinformation or misinformation, gain access to personal data, and punish online service providers that failed to comply with the law. Despite the apparent urgency of this draft, no further development was seen from April and indeed throughout 2021.

The military then proceeded to amend a series of laws to preserve their power. Four digital-rights-related laws were amended in favor of the Tatmadaw: the Law Protecting the Privacy and Security of Citizens, Penal Code, Electronic Transactions Law, and Counter Terrorism Law. Some of the provisions in the draft cybersecurity laws were then inserted into the amended versions of these laws. The Law Protecting the Privacy and Security of Citizens was amended on February 13, and the amendment grants the authorities the power to intercept private messages and request personal communications data from telecommunications service providers as provisions that prohibited such actions were suspended[20]. On February 14, the Penal Code was also amended. The Tatmadaw adjusted it to ensure that they would not be held accountable for staging the coup and also targeted those who took any action against them, both offline and online[21]. Moreover, on February 15, the SAC adopted an amendment to the 2004 Electronic Transaction Act. This amendment led to the inclusion of provisions related to personal data, which allows the military to collect, retain, and use personal data in accordance with the law or any existing laws[22]. Following the self-appointment of Min Aung Hlaing as Prime Minister on August 1, 2021, the military amended the Counter Terrorism Law that targeted the National Unity Government (NUG) and its affiliated organizations[23]. The amendment provides harsher penalties for supporting anti-regime activities.

19 Nachemson, Andrew. "Why Is Myanmar's Military Blocking the Internet?" Al Jazeera, 4 Mar. 2021, www.aljazeera.com/news/2021/3/4/myanmar-internet-blackouts.
20 "Myanmar Military Junta Suspends Laws Protecting Citizens' Privacy to Crack Down on Opposition." The Irrawaddy, 14 Feb. 2021, www.irrawaddy.com/news/burma/myanmar-military-junta-suspends-laws-protecting-citizens-privacy-crack-opposition.html.
21 "Myanmar Ruling Council Amends Treason, Sedition Laws to Protect Coup Makers." The Irrawaddy, 16 Feb. 2021, www.irrawaddy.com/news/burma/myanmar-ruling-council-amends-treason-sedition-laws-protect-coup-makers.html.
22 "Amended Law Throws Myanmar Back into Media Dark Age." Myanmar Now, 19 Feb. 2021, www.myanmar-now.org/en/news/amended-law-throws-myanmar-back-into-media-dark-age.
23 "Myanmar Coup Chief Amends Counterterrorism Law." The Irrawaddy, 3 Aug. 2021, www.irrawaddy.com/news/burma/myanmar-coup-chief-amends-counterterrorism-law.html.

Laws Related to Digital Rights Amended Following the Coup

Names	Amendment
Law Protecting the Privacy and Security of Citizens ("Privacy Law")	Amended to empower the authorities to conduct arrests, searches and seizures, intercept telecommunications, and request disclosure of information from telecommunications operators without a warrant.
Penal Code	The 1861 Penal Code was amended to target protestors and those who participate in pro-democracy movements whether online or offline.
Electronic Transactions Law	Amended to allow the authorities to confiscate personal data and prohibit sharing various types of information online.
Counter Terrorism Law	Amended to introduce harsher penalties for supporting anti-Tatmadaw activities. The amendment targets the NUG and its affiliates.

6. Ordering Telecom Operators to Comply with Surveillance

The amendment of the Privacy Law and Electronic Transaction Law allows lawful interception by the state, in telecommunications. Internet service providers were later confidentially ordered by the Tatmadaw to install intercept technology that would allow the army to eavesdrop on the communications of citizens. The technology gives the military the power to listen in on calls, view text messages and web traffic, including emails, and track the locations of users without the assistance of the telecommunications and internet companies[24].

As a result, Telenor, a Norwegian telecommunications company that launched its business in Myanmar in 2013, announced that it would leave the country. This is due to the pressure to comply with the junta's order, an act which would have violated the 2018 European Union's arms embargo should the company have activated the intercept technology[25]. However, the announcement that the company would sell its business to the M1 Group, a company that has close ties with the Tatmadaw and has a history of aiding authoritarian regimes in many countries, has deepened the concerns of civil society.

24 Potkin, Fanny, and Poppy Mcpherson. "How Myanmar's Military Moved in on the Telecoms Sector to Spy on Citizens." Reuters, 19 May 2021, www.reuters.com/world/asia-pacific/how-myanmars-military-moved-telecoms-sector-spy-citizens-2021-05-18.
25 Potkin, Fanny. "Norway's Telenor Says Myanmar Unit Sale Plan Followed Junta's Pressure on Surveillance Tech." Reuters, 15 Sept. 2021, www.reuters.com/world/norways-telenor-says-myanmar-unit-sale-came-after-juntas-pressure-surveillance-2021-09-15.

On July 27, 2021, the Center for Research on Multinational Corporations (SOMO), on behalf of 474 Myanmar-based civil society groups, submitted a complaint to the OECD Norwegian National Contact Point (NCP)[26]. The document claimed that Telenor's decision to sell its business to the M1 Group failed to meet the standards of responsible disengagement set out in the OECD guidelines. The company later issued a statement in September, 2021, explaining that it was not possible for them to continue to operate in the country if they wished to commit to human rights, responsible business, and international best practices[27].

7. Undisclosed Use of Surveillance Tools

Documents obtained by Justice for Myanmar reveal that the military has purchased, and is in possession of, various surveillance tools from companies from the West and China[28]. Phone-cracking and computer-cracking make up a large portion of the budget allocations. Among those on the list are Cellebrite, BlackBag, and MSAB. Cellebrite is an Israeli company that sells Universal Forensic Extraction Devices (UFED), which can be used to access and collect mobile device data. In 2018, it was documented that the tool was used to infiltrate the phones of the two Reuter's journalists, Wa Lone and Kyaw Soe Oo[29]. Sweden-based MSAB also provides tools to access forensic data. BlackBag, which has been acquired by Cellebrite, provides MacQuisition forensic software that can extract and collect data from Apple computers. Apart from the device cracking tools, the list also includes Israeli's Elbit System that manufactures surveillance drone[30].

8. Revoking Licenses of Independent Media and Seizing Their Devices and Equipment

Harassment against independent media has been extensively documented in Myanmar. However, the crackdown on media has intensified since the coup. At least six independent media; Mizzima, DVB, Khit Thit Media, Myanmar Now, 7Day News, and Kamayut Media, had their licenses revoked in March 2021[31]. Their offices were also raided by the military and police. Some of the electronic equipment and data server components were also confiscated. Around a hundred journalists were also arrested and detained[32]. The confiscation of electronic equipment and raids were lawful following the amendment of the Privacy Law in February 2021. In November 2021, Danny Fenster, Managing Editor of Frontier Myanmar, was charged with terrorism under the Counter-Terrorism Act that was amended in August 2021[33]. The government accused him for his role as the editor of Myanmar Now at the time of his arrest, citing that Myanmar Now had had its license revoked. Both Myanmar Now and Frontier Myanmar officially stated that this claim was inaccurate. This chain of events marks an era in which press freedom in the country hit its lowest point since the opening up of the country in 2011.

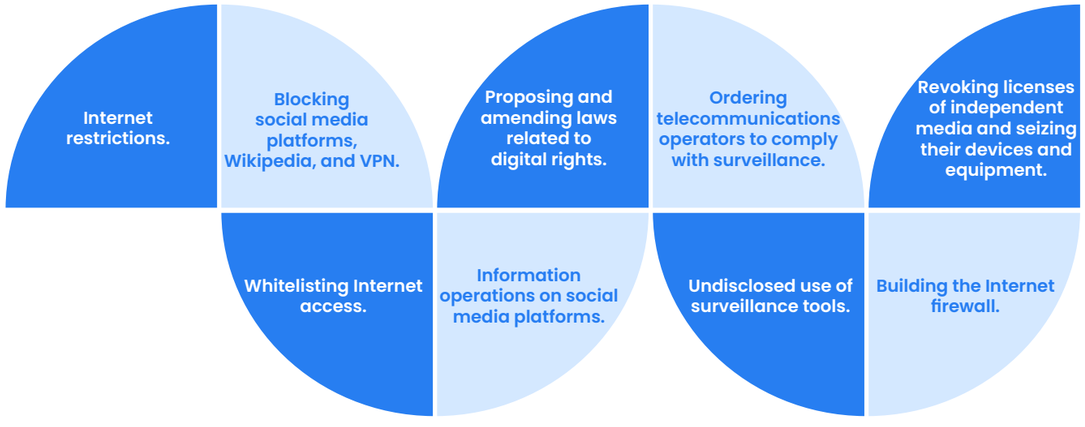
26 "Complaint against Telenor for Irresponsible Disengagement from Myanmar." Center for Research on Multinational Corporations (SOMO), 27 Jul. 2021, www.somo.nl/oecd-complaint-against-telenor-for-irresponsible-disengagement-from-myanmar.
27 "Update on the Ongoing OECD Complaint against Telenor on the Sale of Telenor Myanmar (27 September 2021)." Telenor Group, 27 Sept. 2021, www.telenor.com/media/announcement/update-on-the-ongoing-oecd-complaint-against-telenor-on-the-sale-of-telenor-myanmar-27-september-20
28 "Tools of Digital Surveillance and Repression." Justice for Myanmar, 2 Mar. 2021, www.justiceformyanmar.org/stories/tools-of-digital-repression.
29 Erickson, Evan. "Use of Digital Forensics Raises Questions in Reuters Case." Mizzima, 31 Jul. 2018, mizzima.com/news-domestic/use-digital-forensics-raises-questions-reuters-case.
30 Beech, Hannah. "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown." The New York Times, 1 Mar. 2021, www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html.
31 "Security Forces Raid Kamayut Media Office in Yangon." Myanmar Now, 9 Mar. 2021, www.myanmar-now.org/en/news/security-forces-raid-kamayut-media-office-in-yangon.
32 "Official Myanmar Records Mistaken about Detained US Reporter." Al Jazeera, 6 Nov. 2021, www.aljazeera.com/news/2021/11/6/activists-urge-u-n-intervention-over-myanmar-army-offensives.
33 "Myanmar Charges US Journalist with 'Terrorism' and Sedition." Al Jazeera, 10 Nov. 2021, www.aljazeera.com/news/2021/11/10/danny-fenster-myanmar-files-new-charges-against-us-journalist.

9. Building the Internet Firewall

In February 2021, several media reported that that China had supported Myanmar in building an internet firewall similar to the Great Firewall of China[34]. China, however, denied the allegation despite five cargo planes arriving from Kunming to Yangon on February 9, 2021, believed to be carrying equipment to assist the project, with China stating that this was merely a part of normal import and export routes and procedures[35,36]. No further activity was reported after February.

The Great Firewall of China is considered the most extensive and most advanced in the world due to its complexity. The intention of the Great Firewall is to filter and censor politically sensitive information, dubbed as "wrong information," from outside China to curtail the influence of this information on Chinese society. It also spies on the internet activities of users. In terms of Myanmar, it would take years for the country to achieve the scale of internet censorship and surveillance of China's Great Firewall, given the differing contexts of both countries. However, the current situation has potentially paved an important path towards the future implementation of the initiative.

Tactics of the Tatmadaw on Digital Rights Violations



34 "Burmese Expert: China Helping Military Establish Cyber Firewall." VOA, 12 Feb. 2021, www.voanews.com/a/east-asia-pacific_burmese-expert-china-helping-military-establish-cyber-firewall/6201972.html.
35 "China Denies Helping Myanmar Military Regime Build Internet Firewall." The Irrawaddy, 11 Feb. 2021, www.irrawaddy.com/news/burma/china-denies-helping-myanmar-military-regime-build-internet-firewall.html.
36 Reed, John. "Myanmar Protesters Accuse China of Backing Coup Plotters." Financial Times, 17 Feb. 2021, www.ft.com/content/43e6ecfe-081a-4390-aa18-154ec87ff764.

Digital Authoritarianism in Myanmar
The Regional Challenge

The human rights situation in Myanmar extends well beyond country-level considerations. It represents a regional issue due to the extreme level of human rights violation that implicitly involves interference by third parties from outside the country. ASEAN is in an ideal position to be able to engage with the situation in Myanmar. As Myanmar is also a member of the bloc, the regional body has the capacity to exert pressure on the country. However, ASEAN's response towards events in Myanmar has been met with disappointment, despite ASEAN's customary non-involvement in human rights protection, and despite the fact that the majority of member nations themselves operate as authoritarian regimes.

Following the coup, ASEAN organized the ASEAN Leaders' Meeting on 24 April, 2021, to specifically respond to the situation. Amidst strong criticism and objection, Min Aung Hlaing was invited to the meeting. Through this action, ASEAN seemed to be giving legitimacy to the junta to rule Myanmar and to a leader who seized power by force to oust an elected government before leading an operation that killed hundreds of innocent people.

The meeting in question resulted in the following 5-point consensus:

(1) There shall be an immediate cessation of violence in Myanmar, and all parties shall exercise the utmost restraint.
(2) Constructive dialogue among all parties concerned shall commence, seeking a peaceful solution in the interests of the people.
(3) A special envoy of the ASEAN Chair shall facilitate mediation of the dialogue process with the assistance of the Secretary-General of ASEAN.
(4) ASEAN shall provide humanitarian assistance through the ASEAN Coordinating Center for Humanitarian Assistance (AHA).
(5) The special envoy and delegation shall visit Myanmar to meet with all parties concerned.

The consensus does not specifically reflect any human rights aspect and throughout 2021, not much progress was seen. Despite the first demand for an immediate cessation of violence, the number of civilians who died following the coup rose to over 1,000 in August[37]. In the same month, Erywan Yusof, Brunei's second minister for foreign affairs, was appointed as an ASEAN special envoy. He canceled his visit to Myanmar in October after being informed that he would not have the opportunity to meet with Aung San Suu Kyi and the other individuals he had requested to meet[38]. This made it impossible to achieve the second and fifth points in the consensus.

Myanmar was barred from the ASEAN Summit in October and later, the China-ASEAN summit in November. However, this does not point to the bloc finally taking a stance and recognizing Myanmar's violations of human rights. The fact that it chose not to invite a representative of the parallel National Unity

Government (NUG) and announced the invitation of a non-political representative to attend the summit instead, disappointed many observers. ASEAN's inability to invite a representative from the NUG, which was formed by a group of elected lawmakers and members of parliament who were ousted following the coup betrayed ASEAN's refusal to recognize those who were elected via a democratic process to represent the country.

In contrast to ASEAN's stance and action, the international body has sent a strong signal that it does not recognize the Myanmar military as a legitimate government as Kyaw Moe Tun, appointed by the previous elected government, still remains as Myanmar's permanent representative to the United Nations[39]. In fact, the military announced in February that Kyaw Moe Tun had been dismissed from his position after a speech he made on February 26, 2021, urging the international community to use "any means necessary to take action" against the military to help return democracy to Myanmar[40]. Again, in stark contrast to the stance of the UN, in May, nine nation members of the ASEAN bloc lobbied the UN to drop a call to suspend arms sales to the Myanmar military[41].

These actions reveal that the 10-member bloc has very little interest in human rights whether in their own country or in neighboring countries. Despite the tactics used by the Myanmar military reflecting a degree of digital authoritarianism that has never been seen in the region before, it is yet to be seen as a real concern by the regional body. These incidents of violation are deemed to be of limited importance and are therefore likely to be ignored by the bloc. Events in Myanmar have placed the spotlight firmly on ASEAN's tendency to turning a blind eye to issues of human rights while acting on priorities which are driven purely by political agendas.

37 "More than 1,000 Civilians Have Died in Myanmar Unrest, Say Activists." The Guardian, 19 Aug, 2021, www.theguardian.com/world/2021/aug/19/more-than-1000-civilians-have-died-in-myanmar-unrest-say-activists.
38 Peck, Grant. "Envoy Aborts Visit to Myanmar, Straining ASEAN Relations." AP NEWS, 15 Oct. 2021, apnews.com/article/business-asia-myanmar-global-trade-southeast-asia-55eba9d33db71a4dbf5f7ba66d4afe99.
39 Tin Htet Paing. "NUG Hails UN Decision on Myanmar Representation." Myanmar Now, 3 Dec. 2021, www.myanmar-now.org/en/news/nug-hails-un-decision-on-myanmar-representation.
40 "Myanmar Coup: UN Ambassador Fired after Anti-Army Speech." BBC News, 28 Feb. 2021, www.bbc.com/news/world-asia-56222987.
41 "ASEAN Lobbying to Remove Arms Embargo Call from UN Resolution on Myanmar." Radio Free Asia, 27 May 2021, www.rfa.org/english/news/myanmar/asean-embargo-05272021184301.html.

II
Freedom of Expression

Key Takeaways

- Repressive government regimes across the region are trying to control how social media platforms operate.
- State-sponsored information disorders are growing and have become more sophisticated on social media platforms across the region. How ever, the efforts of both mainstream and emerging social media plat forms to manage and mitigate this situation are proving to be inadequate.
- Independent media have faced new kinds of threats in 2021, developments which need to be closely monitored.
- Internet restrictions in Myanmar and Indonesia are likely to continue to be a common tool for governments to control political situations.

Overview

Threats against freedom of expression in the digital space are growing and became more sophisticated in 2021. Governments across the region are attempting to control the digital space in various ways, including tightening control over social media platforms, adopting more sophisticated tactics for state-sponsored information disorder, harassing alternative media, and restricting usage of the internet.

The tightening of control over social media platforms can be seen in Myanmar, Thailand, Indonesia, Vietnam, and Singapore, where governments have rolled out repressive laws and rules in order to control how social media platforms

operate in the country. Social media platforms are likely to be subjected to intense pressure in the near future when these laws are enacted, as they have to choose between following the requests of the repressive regimes or adhering to the principles of human rights.

Information disorder, a term encompassing misinformation, disinformation, and mal-information, has become more sophisticated across Southeast Asia in 2021. In Myanmar, state-sponsored information disorder has expanded to emerging platforms like Telegram and TikTok that have been criticized for their unclear policies and inconsistent efforts. In the Philippines, information disorder has been linked to the red-tagging campaign of the government where dissidents are falsely branded as terrorists with government-associated social media accounts at the center of the operations. The cyber-troop in Vietnam, Force 47, has expanded to the district level and is organized and well-equipped. More evidence of Thailand's information operation has been discovered this year with regards to their strategies, including the manner in which they have attacked dissidents.

2021 also witnessed the continued harassment of alternative media. Significant forms of harassment range from a court ruling that made Malaysiakini responsible for their readers' comments under their published online article and The Online Citizen being forced to go offline after an unfair allegation of "foreign interference", to the growing number of cyberattacks against alternative media outlets in the Philippines. These tactics signify a different approach from the attacks that were documented earlier. In terms of Malaysiakini, the ruling served as a warning for other alternative media to be more careful with what their readers say. As for The Online Citizen, the situation has alerted other alternative media to be careful with their sources of funding which could be interpreted as foreign interference, a situation which is likely to deteriorate with the enactment of the Foreign Interference (Countermeasures) Bill (FICA). For the Philippines, the new tactical approach of cyberattacks against alternative media has raised deep concerns as the form of harassment employed evolves.

In terms of internet restrictions, Myanmar and Indonesia are likely to establish this method as common practice for political reasons. This points to the strong possibility of it recurring in the future. However, with the exception of Myanmar and its nationwide internet restrictions following the coup in February 2021, complete restrictions are unlikely to happen in large cities across the region due to the potential economic damage which could ensue. Events witnessed in Indonesia constitute a threat to internet freedom and are seen as a short-sighted and unsustainable solution to prevent information disorder from spreading, while in Myanmar, controlling the information and pro-democracy movement with internet restrictions is considered as a severely counter-productive miscalculation with profound long-term implications.

Freedom of expression is fundamental to democracy. The rise of technology has seen a shift in the suppression of freedom of expression in Southeast Asia from offline to online channels in recent years. These draconian government measures have shown that, essentially, democracy, where freedom of expression is respected and valued, does not exist in the region, and it is very likely that the situation will only become worse given what we are witnessing.

1. Tightening Control of Social Media Platforms

2021 saw stepped-up efforts to control social media platforms by repressive regimes throughout Southeast Asia. Social media platforms have played an important role in recent years for activism. Apart from being a space where people can express their opinion online, the platforms have been used by activists in Southeast Asia to organize pro-democracy movements and report on situations by netizens or alternative media which mainstream media might not be able to cover, especially those that are controlled by the regimes.

Following the coup in Myanmar, social media platforms have been used for organizing movements and reporting on incidents. The Civil Disobedience Movement (CDM), a pro-democracy movement against the Myanmar military, started out as an online campaign by healthcare workers before it expanded into a wider movement. Its Facebook page had more than 230,000 followers within a few days of its launch. Myanmar also became part of the #MilkTeaAlliance, a hashtag born on Twitter in 2020 that represents a pro-democracy online regional solidarity movement, joining Thailand, Hong Kong, and Taiwan. As well as campaigning for democracy in solidarity, the Alliance also led protestors to exchange tactics, strategies and ideas in organizing movements with each other[42].

Successful cases of social media activism can be observed throughout the region. Mytel, a military-owned telecommunications service provider, reportedly lost $24.9 million and almost 2 million customers between February and April 2021 after a campaign against the Myanmar military's products and services played a significant role in subscribers abandoning the service[43,44] The #Lawan protest in Malaysia, where social media platforms played an important role in organizing the protest, resulted in the resignation of the government of Muhyiddin Yassin. Hashtags such as #WhatsHappeninginMyanmar and #WhatsHappeninginThailand also allow netizens to report on developments in both countries.

The regimes know that they cannot directly remove or censor any content or accounts on social media platforms, and that the only way to do this is to make the platforms do it on their behalf. With Myanmar as an exception, shutting down entire social media platforms can be done, but it is difficult given the serious implications of doing so, including for social media platforms whose purpose lies beyond the political. The fact that there are no alternative social media platforms to replace ones that are currently mainstream also makes it difficult for regimes to ban these platforms completely. As a result, a significant development in 2021 has been the decision of regimes to tighten control over social media platforms through the issuance of laws in many countries throughout the region which target how social media platforms operate.

In February, Cambodia unveiled Sub-Decree No.23 on the Establishment of National Internet Gateway (NIG), a bill to establish a national internet gateway that can control online communications, similar to the Great Firewall of China. When fully implemented, it will

42 Barron, Laignee. "'We Share the Ideals of Democracy.' How the Milk Tea Alliance Is Brewing Solidarity Among Activists in Asia and Beyond." Time, 28 Oct. 2020, time.com/5904114/milk-tea-alliance.
43 "Mytel Loses Millions of Dollars and Subscribers since Coup." Mizzima, 7 Nov. 2021, mizzima.com/article/mytel-loses-millions-dollars-and-subscribers-coup.
44 Hein, Zeyar. "Myanmar Calls for Boycott of Tatmadaw Linked Products and Services." The Myanmar Times, 3 Feb. 2021, www.mmtimes.com/news/myanmar-calls-boycott-tatmadaw-linked-products-and-services.html.

enable the government's efforts on surveillance and censorship to be conducted in a much more coordinated way. The law would put more pressure on social media companies as the government has control over the traffic, which can threaten the companies' operations.

Indonesia issued Ministerial Regulation 5, known as MR5, on December 2, 2020. The Ministry of Communication and Information Technology (KOMINFO) later announced that the law would take effect in 2021 and required all digital services to register with the government or face being blocked or fined. According to the law, digital services and platforms have to also grant the government access to their systems and personal data as well as remove content within 24 hours of being notified by the government. The government has a history of blocking social media platforms for political reasons. WhatsApp, Facebook, and Instagram backend servers were blocked in 2019 to control the spread of disinformation following a riot which took place after the 2019 Presidential Election[45]. Telegram was also temporarily blocked in 2017 as its platforms were being used to spread pro-Islamic State of Iraq and Levant (ISIL) content. Due to its broad scope, the law is highly likely to threaten freedom of expression if it is used excessively.

As with Indonesia, the Thai government has always tried to control social media platforms, particularly over issues related to the monarchy. Facebook, Twitter, and Google were threatened in 2020 for violating Article 112 of the Criminal Code (lèse-majesté offense) and the Computer Crime Act for allowing anti-monarchy content to appear on their platforms. A Facebook page critical of the monarchy called "The Royalist Marketplace" was blocked by Facebook in 2020 following the government's request. In January 2021, YouTube blocked a music video called "Reform" by Rap Against Dictatorship (RAD) from its platform following a legal complaint from the government[46]. The government also turned their attention to Clubhouse, an increasingly important space used by political opponents and activists to discuss political topics[47]. The situation took a turn when a draft law to regulate digital platform service business was unveiled in July 2021 and approved by the cabinet in October 2021[48,49]. According to the draft, the law requires all digital platforms used by Thai users to register in Thailand. If enacted, the government will have more control over digital platforms, particularly those that operate in the country.

In 2021, Vietnam issued a code of conduct on social networks together with Decision No. 874/QD-BTTTT (Decision 847) dated June 17, 2021. The code is non-legally binding, and it is unclear as to which law it is based on. The code, encourages social media users to create accounts using their real identities, share information from official sources, and avoid posting content that violates the law. It prohibits posts that "affect the interests of the state" and targets social media companies in the country, among others. One month later, Vietnam unveiled a new draft decree amending

45 Singh, Manish, and Jon Russell. "Indonesia Restricts WhatsApp, Facebook and Instagram Usage Following Deadly Riots." TechCrunch, 22 May 2019, techcrunch.com/2019/05/22/indonesia-restricts-whatsapp-and-instagram.
46 "Rap Against Dictatorship's Latest MV Blocked in Thailand." Prachatai English, 5 Jan. 2021, prachatai.com/english/node/8999.
47 Tanakasempipat, Patpicha. "Clubhouse Emerges as Platform for Thai Dissidents, Government Issues Warning." Reuters, 17 Feb. 2021, www.reuters.com/article/us-clubhouse-thailand-idUSKBN2AH0VR.
48 Leesa-Nguansuk, Suchit. "Digital Regulation Draft Bill a Double-Edged Sword." Bangkok Post, 14 Jul. 2021, www.bangkokpost.com/business/2148167/digital-regulation-draft-bill-a-double-edged-sword.
49 Reuters. "Thailand to Regulate Digital Platform Service Businesses." Reuters, 25 Oct. 2021, www.reuters.com/world/asia-pacific/thailand-regulate-digital-platform-service-businesses-2021-10-25.
50 Onishi, Tomoya. "Vietnam to Tighten Grip on Facebook and YouTube Influencers." Nikkei Asia, 13 Jul. 2021, asia.nikkei.com/Politics/Vietnam-to-tighten-grip-on-Facebook-and-YouTube-influencers

Decree No. 72/2013/Nd-CP on management, provision, and use of Internet services and online information for public consultation. The new Draft Decree requires social media platforms to provide the state with the contact information of the operating accounts of users with more than 10,000 followers or subscribers[50]. It can also request social media to block or remove content within 24 hours. Based on Vietnam's Cybersecurity Law which has been in place since 2019, the code of conduct and the Draft Decree are both compatible with this existing law. The Vietnamese government has previously threatened Facebook with the removal of anti-state content. Unfortunately, Facebook submitted to these requests after their local servers were temporarily taken offline[51].

In October 2021, Singapore passed the Foreign Interferences (Countermeasures) Act or FICA. The law grants power to the government to be able to officially request social media platforms to help the government investigate and counter communications activities from abroad. It can also block or remove content considered as "foreign interference". With the government's passing of the Protection from Online Falsehood and Manipulation Act (POFMA) or the "Fake News" Law in 2019, both laws pose greater threats to freedom of expression by strengthening the government's effort to crack down on content which is critical of the government. Since POFMA was adopted, it has often been used against political opposition and critics whose content appears on social media platforms. Facebook has a history of following the government's requests, as the POFMA example shows, through aiding the government in labeling posts that are critical to the government as false information.

The draft cybersecurity law that was proposed by the Myanmar military after the coup closely resembles those found in Vietnam and Thailand. The draft requires the online service providers to store data locally and to comply with the government to block or remove information based on the authorities' requests. Although there is no history of the government or the military in Vietnam and Thailand requesting social media platforms to comply, the law represents a significant development where regimes clearly aim to tighten control of the online space.

These developments raise the question of how media platforms will now operate and treat political content. Given the increasing surveillance and demands, social media platforms are likely to be under more pressure than ever, and are likely to find themselves having to choose between holding on to human rights principles or following the requests of repressive regimes in order to maintain their business growth.

50 Onishi, Tomoya. "Vietnam to Tighten Grip on Facebook and YouTube Influencers." Nikkei Asia, 13 Jul. 2021, asia.nikkei.com/Politics/Vietnam-to-tighten-grip-on-Facebook-and-YouTube-influencers

51 Pearson, James. "Exclusive: Facebook Agreed to Censor Posts after Vietnam Slowed Traffic - Sources." Reuters, 21 Apr. 2020, www.reuters.com/article/us-vietnam-facebook-exclusive-idUSKCN2232JX.

Developments in Laws or Codes Related to Social Media Platforms in 2021

Country	Laws/Code	Potential Effects on Social Media Platforms
Cambodia	Sub-Decree No.23 on the Establishment of National Internet Gateway	The law, if fully implemented, will control internet traffic and threaten the operations of the social media platforms.
Indonesia	Ministerial Regulations No. 5	Social media platforms have to ensure there is no content which is broadly defined as "prohibited content".
Thailand	The law to regulate digital platforms*	Social media platforms have to comply with the government's order; otherwise, they may face operational difficulties.
Vietnam	Code of Conduct for Social Media A draft decree amending Decree No. 72/2013/ND-CP on Management, Provision, and Use of Internet Services and Online Information*	Social media platforms have to keep the space void of anti-state content. If adopted, social media platforms will be required to provide the state with the contact information of accounts with more than 10,000 followers or subscribers.
Myanmar	Cybersecurity Law*	Social media has to block or remove information if requested by the government. It also has to localize the personal data of users and hand it to the authorities when requested.
Singapore	Foreign Interference (Countermeasures) Bill (FICA)	Compliance with the government in investigating/censoring content or removing accounts considered as foreign interference.

*still a draft as of 2021

2. Sophisticated State-Sponsored Information Disorders

Information disorders have long been documented in Southeast Asia, and the situation in 2021 shows that the spread of disinformation, misinformation, or mal-information is growing and becoming more sophisticated. Such state-sponsored operations point to how repressive regimes across the region are trying to exercise control over specific situations by drawing on information disorders in order to preserve their power. In 2021, the development of information disorders in Myanmar has expanded to emerging platforms such as TikTok and Telegram. New evidence has emerged regarding Thailand's information operation. Force 47, Vietnam's cyber-troop, has expanded to the sub-national level. Information disorders in the Philippines are also of concern as they have been found to link with the government's red-tagging campaign where political dissidents have been falsely branded as terrorists.

2.1. Expansion of Pro-military Content on Emerging Platforms

Following the coup, the Myanmar military attempted to spread pro-military propaganda on social media platforms to establish their legitimacy in staging the coup. The tactics included duplicating the messages across accounts on Facebook, YouTube, Telegram, and TikTok. Those who were considered to be anti-military would be labeled as "enemies of the state" and "terrorists" with an aim to destroy the military, the country, and Buddhism[52].

The military has attempted to gain legitimacy for staging the coup by claiming that it was necessary due to election fraud, and pro-military posts on social media platforms were created to support and disseminate this narrative in 2021. The pro-military propaganda has also included the denouncing of pro-democracy protestors as traitors. "Tatmadaw True News Information Team" was created as a Facebook page to convey a positive image of the military and the opposite image for protestors. One such item includes an explanation of how the military medics would provide medical assistance while healthcare workers played a lead role in the Civil Disobedience Movement[53]. The page was later banned by Facebook on February 21, with the platform further announcing the banning of all Tatmadaw-controlled state and media entities from Facebook and Instagram on February 24[54,55]. The company later stepped up its efforts by announcing a further ban on all Myanmar-military-controlled businesses from having a presence on its platforms on December 8, 2021. It also announced that over 100 accounts, pages, and groups linked to military-controlled businesses had already been taken down[56]. YouTube also removed five TV channels run by the Tatmadaw in March. The blocked channels included the government-run Myanmar Radio and Television and the Myawaddy Media, channels which broadcast military propaganda[57].

Following the ban from mainstream social media platforms, the attempt to spread disinformation and misinformation spread to emerging

52 Potkin, Fanny, and Wa Lone. "'Information Combat': Inside the Fight for Myanmar's Soul." Reuters, 2 Nov. 2021, www.reuters.com/world/asia-pacific/information-combat-inside-fight-myanmars-soul-2021-11-01.
53 "A Preliminary Analysis of the Myanmar Military Junta's Media Propaganda." Tea Circle Oxford, 9 Mar. 2021, teacircleoxford.com/research-report/a-preliminary-analysis-of-the-myanmar-military-juntas-media-propaganda.
54 "Facebook Takes down Main Page of Myanmar Military." Reuters, 21 Feb. 2021, www.reuters.com/article/us-myanmar-politics-face
55 Frankel, Rafael. "An Update on the Situation in Myanmar." Facebook, 11 Feb. 2021, about.fb.com/news/2021/02/an-update-on-myanmar.
56 Reuters. "Meta to Ban All Myanmar-Army Controlled Businesses from Platforms." Reuters, 9 Dec. 2021, www.reuters.com/world/asia-pacific/meta-ban-all-myanmar-army-controlled-businesses-platforms-2021-12-08.
57 Mozur, Paul. "YouTube Removes Myanmar Military Channels." The New York Times, 5 Mar. 2021, www.nytimes.com/2021/03/05/business/youtube-myanmar.html.

platforms like TikTok and Telegram. Video clips found on TikTok include pro-military propaganda, misinformation to divide and confuse protestors, and death threats from security forces towards people who go on to the streets to protest[58]. In terms of Telegram, an investigation found that many pro-military accounts that were banned from Facebook even before the coup resurfaced on this platform. These accounts target the Rohingya Muslims, National League for Democracy (NLD), and civilian armed resistance. Women who participated in the pro-democracy movement were also attacked and targeted through hate speech, disinformation, conspiracy theories, and sexual harassment.

The expansion of Tatmadaw's effort on emerging platforms like TikTok and Telegram is a significant development following the coup. These two platforms have been criticized by civil society for not providing enough effort to prevent their platforms from being used to spread harmful content. TikTok started to aggressively remove content associated with the Tatmadaw after the issue was widely covered by the media, while their efforts to apply their community standards still remain inconsistent. Telegram's capacity to enable people to broadcast messages to groups of people as large as 200,000 is also worrying as this makes it easy for the platform to reach out and become a harbor of information disorder and hate speech. The problems are likely to continue for TikTok and Telegram if both platforms do not step up their efforts, such as hiring more Burmese-speaking staff or working more closely with civil society.

2.2. New Evidence Found on Thailand's Information Operations

As a close neighbor of Myanmar, Thailand also has a record of state-sponsored propaganda which is closely associated with the military. One such operation is alleged to be run by the Royal Thai Army and is known as "information operation" or IO. In February 2021, Facebook announced that it had removed 77 accounts, 72 pages, 18 groups, and 18 Instagram accounts that were linked to the Thai Military's Internal Security Operations Command (ISOC). This action followed what happened in October 2020 when Twitter took down 926 Thai Twitter accounts, also found to be military-associated.

The issue of Information Operations was first exposed in the Thai parliament in 2020 by the Future Forward Party (FFP), an opposition political party that later re-formed as the Move Forward Party (MFP). More details have been exposed following the first incident. This issue was raised at least twice in 2021 in the parliament by the opposition party and sparked an information war with the aim of manipulating people's thoughts in order to protect the government and attack critics. In 2020, the party showed evidence that the IO and cyberattacks were systematically supported and funded by the Thai military. The document revealed that ISOC granted a budget to operate a website that promotes pro-government propaganda and frequently attacks people or civil society groups that work on human rights[59].

58 Guest, Peter, et al. "TikTok Is Repeating Facebook's Mistakes in Myanmar." Rest of World, 18 Mar. 2021, restofworld.org/2021/tiktok-is-repeating-facebooks-mistakes-in-myanmar.
59 "Royal Thai Army Linked to 926 Information Operation Accounts, Says Twitter." Prachatai English, 12 Oct. 2020, prachatai.com/english/node/8836.

Later in 2021, the MFP revealed more evidences including video clips and a leaked document[60]. They also alleged that the Thai military's Information Operations is divided into the three categories of "white tasks", "grey tasks", and "black tasks". The white task is to support and promote the government's work. The grey task is to respond to criticism of the government, and the black task is to attack critics with hate speech and to spread disinformation. The party revealed that those in the military who formed part of the operation would receive a mobile sim card and be assigned responsibility for specific social media pages. Those who excelled in their work would be rewarded. The MFP also posted photos claiming to show how the military operates the IO on their official social media channel.

In response to these revelations, the military filed a lawsuit against the opposition party member who exposed the information[61]. The Prime Minister denied knowledge of the issue and ordered a probe following Facebook's announcement on the ban[62]. As for civil society, a group of activists submitted a petition to the Central Administrative Court in March 2021 requesting the court to stop the Thai military's operation. They also wrote to Facebook asking the company to look into the military's alleged operation and take action against those who violate the platform's community standards[63].

2.3. Growth of Force 47 in Vietnam

In Vietnam, 2021 witnessed a significant development related to the state-sponsored cyber-army, Force 47 or Brigade 47. Unveiled in 2017, Force 47 is a military cyber warfare unit that aims to counter anti-state content on the Internet. When it was first unveiled by Lieutenant General Nguyen Trong Nghia, deputy head of the military's political department at that time, the unit had 10,000 members[64]. Despite its clear status as a cyber-army that targets online dissidents in Vietnam and threatens freedom of expression and the right to information, four years later, in 2021, Force 47 continued to show consistent growth, and Nguyen Trong Nghia was appointed as its head on February 19, 2021[65].

Following the appointment of Nguyen Trong Nghia, Force 47 has expanded to the district level where the cyber-army is reported to be well-organized and equipped with devices[66]. These cyber troops are paid and trained on how to exploit and use devices such as smartphones and tablets for their mission. It is reported that Force 47 has established a "secret group" to exchange and unify information, and provide training on how to write news, articles, and gain specific skills for working in the field of cyberspace.

60 Sattaburuth, Aekarach. "MFP Takes Aim at Military Info Ops." Bangkok Post, 20 Feb. 2021, www.bangkokpost.com/thailand/politics/2071327/mfp-takes-aim-at-military-info-ops.
61 "Army Files Complaint against Move Forward MP for Allegedly Falsifying Documents." The Nation Thailand, 2 Sept. 2021, www.nationthailand.com/in-focus/40005589.
62 "Thai PM Orders Probe into Army's Link to Banned Facebook Network." Al Jazeera, 5 Mar. 2021, www.aljazeera.com/news/2021/3/5/thai-
63 "iLaw Petitions against 'Information Ops.'" Bangkok Post, 3 Mar. 2021, www.bangkokpost.com/thailand/politics/2077127/ilaw-petitions-against-information-ops.
64 "Vietnam Unveils 10,000-Strong Cyber Unit to Combat 'Wrong Views.'" Reuters, 26 Oct. 2017, www.reuters.com/article/us-vietnam-security-cyber-idUSKBN1EK0XN.
65 "Vietnam Appoints Military General Country's New Propaganda Chief." Radio Free Asia, 19 Feb. 2021, www.rfa.org/english/news/vietnam/chief-02192021194448.html.
66 BBC News Tiế́ng Việt. "Việt Nam: 'Dú luán viên' tung hoành trên Facebook đã tói cá́p huyén?" BBC News Tiế́ng Việt, 16 Apr. 2021, www.bbc.com/vietnamese/vietnam-56759674.

Vietnam is a communist country and this may offer one explanation as to why the government does not feel the need to hide such efforts. Some of the Facebook groups are also available publicly. However, despite being an open initiative, the question still remains of what efforts social media platforms have taken in order to protect the internet freedom of those living in Vietnam from Force 47. Unlike other information operations in the region, the fact that Force 47 is publicly known as a state initiative probably goes some way to explain its existence, growth and immunity from its removal by social media platforms.

Following a Reuter's investigation, Facebook removed some groups or accounts belonging to Force 47 in July 2021 but still allowed some of the groups to remain active. According to the company, these cyber-army accounts or groups use their real names, so they do not violate Facebook policies. In their statement in response to Reuters, the company explained that its goal was to keep its service in Vietnam online "for as many people as possible to express themselves, connect with friends and run their business." According to the Facebook Papers, Facebook has followed the government's requests on censorship and allowed it to have near-total control of the platform[67]. The cyber-army is also found to be operating on YouTube and Twitter including through the use of anonymous Gmail and Yahoo email addresses[68]. YouTube announced it had removed nine channels for violating its policies on spam, and some of the removed channels are considered to be part of the Force 47 operation.

2.4. Online Red-Tagging Narratives in the Philippines Intensified due to Lack of Accountability of Social Media

The manner in which dissidents are now targeted by state actors is more sophisticated than what has been previously documented. In the Philippines, information disorders have been found to be linked with the government's red-tagging campaign. When an individual or entity is red-tagged, they are considered by the government to be part of dangerous operations such as a terrorist organization or a communist movement that is harmful to national security. Rodrigo Duterte's administration created the National Task Force to End Local Communist Armed Conflict (NTF-ELCAC) in 2018. Online propaganda against activists and human rights organizations that are related to red-tagging have escalated following the implementation of the NTF-ELCAC.

Rappler, a local media outlet in the Philippines, discovered that the official Facebook page of NTF-ELCAC is at the center of an online red-tagging campaign[69]. The pages that work to spread information disorders linked with the red-tagging campaign form a cluster, and the problematic information is circulated through these pages to their followers. These pages, for example, include the Philippine News Agency, PTV, SMNI News, and the official Facebook page of a prominent army office, the Civil Relations Service Armed Forces of the Philippines. The cluster of pages that shared red-tagging narratives was revealed by Rappler's 2021 investigation

67 Dwoskin, Elizabeth, et al. "The Case against Mark Zuckerberg: Insiders Say Facebook's CEO Chose Growth over Safety." Washington Post, 25 Oct. 2021, www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower.
68 Pearson, James. "How Vietnam's 'influencer' Army Wages Information Warfare on Facebook." Reuters, 9 Jul. 2021, www.reuters.com/world/asia-pacific/how-vietnams-influencer-army-wages-information-warfare-facebook-2021-07-09.
69 Macaraeg, Pauline. "Gov't Platforms Being Used to Attack, Red-Tag Media." Rappler, 12 May 2020, www.rappler.com/newsbreak/investigative/260602-government-platforms-being-used-attack-red-tag-

to be large and sophisticated compared to the cluster that spreads facts to counter the red-tagging narratives[70]. As the most popular platform in the country, the spread of information is amplified by Facebook's echo chamber as it reinforces the harm against dissidents. It has been reported that at least 33 dissidents lost their lives after they were red-tagged under the Duterte administration as of May 2021[71].

3. Harassment Against Alternative Media Continues

2021 is another year that has witnessed the continuation of harassment against alternative media. As well as the situation in Myanmar where at least six independent media had their licenses revoked following the coup, significant harassment was observed in 2021 in Malaysia, Singapore, and the Philippines. In Malaysia, Malaysiakini was found guilty of allowing their readers' critical comments towards the judicial system to remain on their official website. In Singapore, the Online Citizen was revoked of its license for not disclosing a list of their subscribers to the authorities. Thum Ping Tjin, manager of the New Naritif, a media outlet, received a stern warning for promoting content critical of the Singaporean government on Facebook during the period of the 2020 General Election. Thum and Kirsten Han, a prominent journalist in Singapore, were also attacked during a parliamentary debate shortly before the government adopted the repressive law on foreign interference. Among other reasons provided in the parliament, the two were alleged to have spread misinformation about the law of which they had been critical. In the Philippines, cyberattacks that have long been documented intensified. Evidence was found that proved that the attacks against Bulatlat and Alter-Midya were linked to the state agencies. The attacks were also expanded later in the year to include ABS-CBN, Rappler, and VERA Files. The attacks against these three organizations represented a new form of more sophisticated attacks.

3.1. A Crime for Readers' Comme nts in Malaysia

In February 2021, Malaysiakini, an online independent entity in Malaysia, was fined RM500,000, equivalent to approximately $124,000, for five reader comments that appeared on a page of its published article[72]. The five comments centered on an article about the reopening of Malaysian courts published in June 2020 and were critical of the independence of the Chief Justice and the judiciary. The newspaper managed to remove the comments from the article, but it was too late.

Malaysiakini defended itself by claiming that it is not responsible for their readers' comments. However, the judges concluded that the online newspaper bore full responsibility for the comments as they formed part of its website. According to the judges, the case was a reminder to the public not to use online comments to attack the judiciary. The judgment alerted all online newspapers in Malaysia to be careful with what is discussed on their websites, and to the need to monitor and filter. However, it also raises the question of whether this judgement applies to comments on social media platforms as online news outlets also use social

70 Hapal, Don Kevin. "New War: How the Propaganda Network Shifted from Targeting 'addicts' to Activists." Rappler, 3 Oct. 2021, www.rappler.com/newsbreak/investigative/how-propaganda-network-created-online-environment-justifies-shifted-killing-activists.
71 Peña, Kurt Dela. "'Undas' 2021: Red-Tagging as Death Warrant." INQUIRER, 2 Nov. 2021, newsinfo.inquirer.net/1509566/undas-2021-red-tagging-as-death-warrant.
72 Paddock, Richard. "5 Reader Comments Just Cost a News Website $124,000." The New York Times, 19 Feb. 2021, www.nytimes.com/2021/02/19/world/asia/malaysia-press-freedom-guilty.html.

media platforms to publish their content. It should also be noted that the Malaysian judiciary is a public institution that is run using tax payers' money. If the public institution cannot accept criticism from people who are taxpayers, it reflects how democratic or not the country is.

3.2. Singapore's Obsession with Foreign Interference

Another significant development occurred in Singapore following the introduction of the Foreign Interference (Countermeasures) Act (FICA) to the parliament. Alternative media are facing a new threat from FICA due to its broad scope that allows the government to exercise their power to counter anything considered as "foreign interference." Following the introduction of the FICA to the parliament on September 13, 2021, two alternative media, The Online Citizen (TOC) and New Naritif, found themselves in a difficult situation. The Infocomm Media Development Authority (IMDA) announced that the TOC had failed to declare its funding sources, an obligation when registering as an Internet Content Provider (ICP). According to the IMDA's media statement issued on September 14, 2021, ICPs that "engage in the online promotion or discussion of political issues relating to Singapore, are required to be transparent about their sources of funding." It further states that declaring the sources of funding will prevent the ICPs from "being controlled by foreign actors, or coming under the influence of foreign entities or funding, and to ensure that there is no foreign influence in domestic politics"[73].

The problem was actually with the TOC's subscription model, which TOC adopted in 2014. The subscription fee is one of the revenue sources for the news outlet. The IMDA was particularly concerned about foreign influence as the model allowed subscribers to commission articles to be written in exchange for the subscription payment[74]. TOC stated that the authority considered the subscribers as donors in 2019 and started to ask TOC to justify its subscription model in 2020. TOC, in fact, explained to the IMDA how the subscription model worked and stated that it had asked the authority to exclude the subscription model from the declaration of funding sources, as the authority asked the TOC to clarify various elements of it. As the IMDA rejected the request, TOC could not therefore proceed with the declaration. The news portal also said that the authority did not have the right to interfere with the subscription as subscribers signed up with the understanding that their identity would not be shared with the authorities. TOC's license was suspended on September 14, 2021. All of their channels, including their websites and social media channels, have been taken offline following the case.

At around the same time a stern warning was issued by the police to Thum Ping Tjin (a.k.a. PJ Thum), director of Observatory Southeast Asia (OSEA) that publishes New Naratif. This referred to the incident happened during the campaign for the 2020 Singaporean Election when the media outlet spent money on five Facebook posts containing election-related content to boost engagement[75]. The Prime Minister's Office alleged that New Naratif violated the Parliamentary Elections Act and claimed it has "unauthorized paid election advertisements." According to the law, election activity conducted without authorization by a candidate or their

73 "Cancellation of The Online Citizen Pte Ltd Class Licence." Infocomm Media Development Authority, 15 Oct. 2021, www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2021/Cancellation-of-The-Online-Citizen-Pte-Ltd-Class-Licence.
74 Sim, Dewey. "Singapore Website The Online Citizen Goes Offline after Funding Disclosure Row with Government." South China Morning Post, 16 Sept. 2021, www.scmp.com/week-asia/politics/article/3148970/singapore-website-online-citizen-goes-offline-after-funding.
75 "New Naratif Under Attack." New Naratif, 15 Sept. 2021, newnaratif.com/new-naratif-under-attack.
76 Tham, Davina. "Thum Ping Tjin, New Naratif Publisher Issued 'stern Warnings' by Police for Paid Election Ads during GE2020." CNA, 15 Sept. 2021, www.channelnewsasia.com/singapore/thum-ping-tjin-pj-new-naratif-stern-warning-police-election-ads-eld-2179111.

election agent is considered an offense[76]. The authorities further claimed that the advertisements "were intended to prejudice the electoral prospects of a political party during the GE2020".

The posts that were subsequently taken down included a satirical political video of Prime Minister Lee Hsien Loong and four critical posts related to the government's inability to accept criticism, its transparency and accountability, the use of POFMA during the election period, and racial discrimination in Singapore. It did not directly promote any particular political party for the election. In fact, New Naratif was not the only media outlet that boosted its Facebook posts during the election. AsiaOne, which is partly owned by the government-controlled Singapore Press Holdings, boosted around 240 posts, of which 150 were directly related to the election[77]. As part of the investigations, PJ Thum's mobile phone and laptop were also seized by authorities for forensic examination, actions which were claimed to be taken in accordance with the Criminal Procedure Code. A stern warning was then issued to PJ Thum on September 15, 2021. According to the news outlet, the mobile phone and the laptop had not yet been returned to him at the time the warning was issued.

The FICA was then passed on October 4, 2021, after 10 hours of parliamentary debate. No public consultation concerning the bill was conducted, and it was passed within 3 weeks after first being introduced to the parliament on September 13, 2021. During the parliament debate on October 4, 2021, Minister for Home Affairs and Law, K. Shanmugam, also attacked Pj Thum and Kirsten Han for their leading roles in spreading misinformation about FICA. Han is an independent journalist who co-founded New Naratif in 2017 with PJ Thum and Sonny Liew. Shanmugam also declared that New Naratif had received funding from Open Society Foundations (OSF), a foreign source, and further alleged that both individuals had asked Mahathir Mohamad, the prime minister of Malaysia at the time, to intervene in Singapore's politics. All of these accusations were later denounced by Han as misinformation[78].

Alternative media has a history of being targeted by the Singaporean government, and FICA will pose a severe challenge, in a city state where independent journalism exists alongside the highly-controlled and dominant majority of state-owned media. These actions against TOC, as well as criticism towards New Naritif over its funding from OSF, have generated significant concern towards alternative media operating in Singapore and issues related to their source of funding. A practice that is considered as 'normal' in a truly democratic country is exaggeratedly labelled as 'foreign interference' simply due to honest journalism that is critical of the government. What happened to TOC did not involve FICA, but it sent a clear signal that alternative media is truly at risk as the government can always choose to weaponize the concept of "foreign interference" against them.

3.3. Intensification of Cyber-attacks in the Philippines

Cyberattacks against alternative media have received considerable attention in the Philippines. Alternative media such as Bulatlat and Altermidya have experienced distributed-denial

77 "Ad Library: AsiaOne." Facebook, 30 Jun. 2020 – 10 Jul. 2020, www.facebook.com/unsupportedbrowser?active_status=all&ad_type=political_and_issue_ads&country=SG&view_all_page_id=121790674546188&sort_data[direction]=desc&sort_data[mode]=relevancy_monthly_grouped&start_date[min]=2020-06-30&start_date[max]=2020-07-11&search_type=page&media_type=all.

78 Han, Kirsten. "A Response to Claims Made about Me during the FICA Debate." We, The Citizens, 5 Oct. 2021, www.wethecitizens.net/a-response-to-claims-made-about-me-during-the-fica-debate.

-of-service (DDoS) attacks for a long time, and in 2021, DDoS attacks were found to be linked to the Philippine army. Another human rights organization website, Karapatan, discovered that the DDoS attacks against them were connected to an Israeli firm, Bright Data[79]. Also, in 2021, more media outlets, including a fact-checking organization, became victims of DDoS attacks.

According to a report released in June 2021 by Qurium, a digital forensics nonprofit organization that supports independent media outlets with their cybersecurity, cyberattacks against Bulatlat and AlterMidya were found to have links with the country's Department of Science and Technology (DOST) and the army. For example, one attack that occurred in May originated from a machine with an IP address that belongs to the Philippine Research, Education, and Government Information Network (PREGINET), a project under the DOST. DOST denied involvement but stated that it assists "other government agencies by allowing the use of some of its IP addresses in the local networks of other government agencies[80]." Another example is the attacks that have an IP address with the details "acepcionecjr@army.mil.ph Taguig Red Server". The domain name, mil.ph, is known to belong to the Philippine military[81]. The Computer Emergency Response Team (CERT-PH) under the Department of Information and Communication Technology (DICT) in September 2021 confirmed that the attacks against AlterMidya and Bulatlat did indeed originate from the Philippine Army.

In the case of Karapatan, the organization has routinely been attacked by the government and pro-government groups. The Israeli company that was found to be linked with the DDoS attacks against the organization's website was originally known as Luminati Network before rebranding itself in March 2021 as Bright Data[82]. It offers a service of proxy networks for other businesses such as mobile operators and data centers[83]. Qurium was able to trace thousands of IP addresses used in the attack to the Israeli company yet Bright Data denied its involvement. Despite the denial, Qurium stated that it is impossible that IPs from Bright Data's network could be involved in the attack without the use of the company's infrastructure. Furthermore, the attack is estimated to have cost at least $260,000, which points to a significant source of funding.

The attack happened to take place on the day Karapatan launched an online campaign #StopTheKillingsPH on August 16, 2021, which addressed violence against human rights defenders and journalists. Earlier in June 2021, Kodao Productions reported that its website was under DDoS attack again having experienced it already in 2019. The attacks are reported to have started on June 11 and intensified after their coverage of the protest at the Chinese Consulate and Israeli Embassy on June 12, 2021, which is Independence Day in the Philippines[84].

79 "Israeli Firm 'Bright Data' (Luminati Networks) Enabled the Attacks against Karapatan." Qurium, 25 Aug. 2021, www.qurium.org/alerts/israeli-firm-bright-data-luminati-networks-enabled-the-attacks-against-karapatan.

80 Villaruel, Jauhn Etienne. "Alternative News Websites Hit by Alleged State-Backed Cyberattacks: Digital Forensics." ABS-CBN News, 24 Jun. 2021, news.abs-cbn.com/news/06/24/21/alternative-news-websites-hit-by-alleged-state-backed-cyberattacks-digital-forensics.

81 Gonzales, Gelo. "Military, DOST Links Found in DDoS Attacks on Media." Rappler, 23 Jun. 2021, www.rappler.com/technology/qurium-links-dost-military-found-ddos-attacks-altermidya-bulatlat.

82 "Israeli Firm 'Bright Data' (Luminati Networks) Enabled the Attacks against Karapatan." Qurium, 25 Aug. 2021, www.qurium.org/alerts/israeli-firm-bright-data-luminati-networks-enabled-the-attacks-against-karapatan.

83 Guest, Peter. "'Billions of Requests, Thousands of Dollars': Inside a Massive Cyberattack on a Philippine Human Rights Group." Rest of World, 25 Aug. 2021, restofworld.org/2021/philippines-human-rights-cyberattack.

84 Subingsubing, Krixia. "Alternative Media Site Shuts down after Cyberattack." INQUIRER, 23 Nov. 2021, newsinfo.inquirer.net/1518615/alternative-media-site-shuts-down-after-cyberattack.

Later in the year, Pinoy Weekly, an alternative media, claimed that it was subjected to an "intense" DDoS attack from unknown entities for two days in November 2021. Its website had also been attacked before in 2018 and 2019. ABS-CBN, Rappler, and VERA Files also experienced DDoS attacks against their websites. ABS-CBN reported an attack on December 11, 2021, and its website went down for a total of six hours[85]. Rappler reported an attack on December 15, 2021, and VERA Files reported another on December 16, 2021[86,87]. According to VERA Files, it is not yet known which incident or post triggered the attack. It became evident that the tactics employed against ABS-CBN, Rappler, and VERA Files were new tactics that had never been documented before. This tactic is considered more sophisticated than the other attacks as it could have stemmed from those that provide DDoS-for-hire services[88].

Significant Forms of Harassment Against Alternative Media in 2021

Country	Targeted Media	Forms of Harassment
Malaysia	Malaysiakini	Fined for contempt of court due to readers' comments on its article.
Singapore	The Online Citizen	Its license was canceled by the Infocomm Media Development Authority (IMDA) after it failed to declare sources of funding.
	New Naritif	A stern warning is issued to Thum Ping Tjin, managing director of Observatory Southeast Asia (OSEA) that publishes New Naritif, following the publishing of unauthorized paid election advertisements.
	Kirsten Han and Thum Ping Tjin	Attacked by the Ministry of Law and Home Affairs, K. Shanmugam, during a parliament debate before FICA was passed. They were attacked for spreading misinformation while campaigning against and being critical of the law.
Philippines	Bulatlat, AlterMidya, Kodao Productions, Pinoy Weekly, ABS-CBN, Rappler, and VERA Files	Their websites were violated by DDoS attacks. The tactics against ABS-CBN, Rappler, and VERA Files were found to be more sophisticated than previous attacks against other entities.

85 Buan, Lian. "ABS-CBN News Website Is Latest Victim of Cyberattack." Rappler, 11 Dec. 2021, www.rappler.com/technology/abs-cbn-news-website-latest-victim-cyberattack.
86 "Rappler Website under Cyberattack." Rappler, 15 Dec. 2021, www.rappler.com/technology/rappler-website-under-cyberattack.
87 Berdos, Rick. "VERA Files Overcomes Cyberattack." VERA Files, 16 Dec. 2021, verafiles.org/articles/vera-files-overcomes-cyberattack.
88 Mendoza, Gemma B. "Heightened DDoS Attacks Target Critical Media." Rappler, 24 Dec. 2021, www.rappler.com/technology/cyberattacks-abs-cbn-rappler-vera-files-similar-signatures.

4. Internet Restrictions

The developments of 2021 suggest that the situation in Myanmar and Indonesia is very likely to bring about the normalization of internet restrictions as one component of political repression in these countries. There is also a possibility that other countries will adopt this approach. However, completely restricting the internet is not an easy undertaking in large cities as it can cause great damage to the economy due to the significant role played by the internet.

For Myanmar, the internet restrictions that started in June 2019 in Rakhine and Chin states set an important precedent for the nationwide internet restrictions that followed the coup. Developments in Rakhine and Chin states were the result of the conflict between the Arakan Army (AA) insurgents and the Tatmadaw. The government ordered the shutdown due to "disturbances of peace and use of internet activities to coordinate illegal activities". One aim of the restrictions was also said to be to prevent international NGOs and the media from obtaining information in Rakhine[89]. It was the first time that the government, led by the NLD, justified the restrictions using Article 77 of the 2013 Telecommunications Law to order four mobile operators in the country - MPT, Mytel, Ooredoo, and Telenor - to impose restrictions on the internet. According to the law, the government is allowed to suspend a telecommunications service or restrict certain forms of communication during "an emergency" situation.

The restrictions in Chin and Rakhine states, dubbed as the world's longest internet blackouts, ended in February 2021, shortly after the coup. The restriction affected around 1.4 million people and the effects were far-reaching, including those living in the area not knowing about the COVID-19 pandemic and distribution of medical aid and food facing extreme challenges in terms of reaching those displaced by the conflict. The media also experienced difficulty in gathering information, verifying, and promptly disseminating it. This form of repression has continued on a larger scale following the coup on February 1, 2021. However, the nationwide internet restrictions implemented following the coup constitute an extreme case that other countries will find hard to emulate. This is due to the fact that the situation has moved beyond political suppression. It has also affected businesses and millions of citizens that rely on the internet as a lifeline.

In terms of Indonesia, the constitutional court ruled on October 27, 2021 that the internet restriction during the period of unrest was lawful. In this ruling, reference was made to an incident which took place in August 2019 when Papuan students in Surabaya, a city located in East Java, were reportedly mistreated by police and verbally abused with racist slurs. Following this occurrence, protests broke out in many cities and escalated into violence in which at least six protestors and one soldier were killed[90].

In June 2020, the administrative court in Jakarta ruled that the internet restrictions in Papua were unlawful after a lawsuit was filed by civil society. The ruling represented a landmark decision for internet freedom in the country. However, the recent ruling of the constitutional court in October 2021 represented a significant change. By ruling that the restrictions were indeed lawful as there were threats to public order

89 Chau, Thompson, and John Liu. "100 Days of Internet Blackout Takes Its Toll in Rakhine." The Myanmar Times, 30 Sept. 2019, www.mmtimes.com/news/100-days-internet-blackout-takes-its-toll-rakhine.html.
90 Doherty, Ben. "Up to Seven Dead in West Papua as Protest Turns Violent." The Guardian, 29 Aug. 2019, www.theguardian.com/world/2019/aug/29/west-papua-deaths-as-protest-turns-violent.

following the incident that brought about the restrictions, internet freedom in the country has been severely threatened[91].

As the internet restrictions were deemed to be lawful, this means that similar measures have a high potential of recurring in Indonesia in the future. On April 30, 2021, prior to the ruling, the internet went down again in Papua with the government claiming that the issue, according to PT Telcom Indonesia, a telecommunications conglomerate in the country, was due to a broken underwater cable, and that it would take a month to repair the connection. However, civil society and local people in the area did not believe this claim, given that the internet restrictions happened immediately after the killing of a top Indonesian intelligence official in Papua. Following this situation, President Joko Widodo subsequently vowed to crack down on Papua, and 400 battle-hardened troops were deployed to the region[92].

The political conflict between West Papua and Indonesia has been extensively documented, and internet restrictions, as well as the ruling, are highly likely to intensify the situation, allowing the government to continue using it as a reason for digital suppression. The government may also choose to impose this approach on other areas of the country. Following the 2019 presidential election, the government restricted the use of social media platform online messaging apps between May 22-24 in the aftermath of a violent post-election riot. The government reasoned that this would prevent the spread of information disorders as people were protesting as a direct result of disinformation and misinformation.

The reasons given for the internet restrictions in Southeast Asia are usually political in nature. Governments often justify these restrictions with reference to public safety, national security or to the prevention of the spreading of information disorder. However, this approach towards restricting the internet to curb information disorder is not likely to tackle the problem in the long run if digital literacy is still limited among netizens. Moreover, restrictions in large cities pose greater challenges as potential damage to the economy through such action remains high. Partial restrictions, however, may be more feasible than a complete blackout. Rakhine and Chin states in Myanmar, as well as Papua in Indonesia, are war-torn areas where economic damages from internet blackouts are much less severe than in the cities.

Another area of concern is whether other countries in Southeast Asia will follow Myanmar and Indonesia. The Thai government gave permission to the National Broadcasting and Telecommunications Commission (NBTC) to order internet service providers in Thailand to block the internet access of critical voices based on their IP address in July 2021[93]. This order was issued under the Emergency Decree, and targeted individuals critical of the way the government handled the COVID-19 pandemic. The reason given was that the critical content might "incite fear" among the public, even though the content might not constitute disinformation or misinformation. However, in August 2021, a civil court ruled to suspend this order. According to the ruling, the order breached the rights and freedom of individuals that are enshrined in the constitution[94].

91 Da Costa, Agustinus Beo, and Stanley Widianto. "Indonesian Internet Blocks amid Social Unrest Lawful, Court Rules." Reuters, 27 Oct. 2021, www.reuters.com/business/media-telecom/indonesian-internet-blocks-amid-social-unrest-lawful-court-rules-2021-10-27.
92 Firdaus, Febriana. "Indonesia Said a Broken Cable Caused an Internet Blackout in Papua. Locals Aren't Buying It." Rest of World, 20 May 2021, restofworld.org/2021/west-papua-deliberate-internet-blackout.
93 "Court Accepts Petition against Internet Blocking." Bangkok Post, 2 Aug. 2021, www.bangkokpost.com/thailand/general/2158731/court-accepts-petition-against-internet-blocking.
94 Yuda, Masayuki. "Prayuth's Media Gag Order Raises Doubts on Regard for Constitution." Nikkei Asia, 14 Aug. 2021, asia.nikkei.com/Politics/Turbulent-Thailand/Prayuth-s-media-gag-order-raises-doubts-on-regard-for-constitution.

III
The Right to Privacy

Key Takeaways

- 2021 saw a significant rise in digital surveillance. This is based on key events that occurred in 2021, including the discovery of spyware at tacking Thai activists, surveillance technology in Myanmar, and Meta's discovery of surveillance-for-hire firms where dissidents across South east Asia have been targeted.
- Despite the overall development of laws on personal data protection in Southeast Asia in 2021, existing and upcoming laws across the region are unlikely to protect dissidents from digital surveillance as personal data laws often collide with other laws that allow state surveillance to happen, and these state surveillance efforts are carried out by government agencies.
- Many health experts across the region consider digital contact tracing to have failed as an approach. However, some governments still continue with the initiative, even though its role in controlling the pandemic in their country may be limited. It also carries privacy risks, dicriminates against people who do not have a smartphone, and is a questionable use of resources.

Overview

2021 is a year that saw a sharp rise in the use of digital surveillance. Key incidents during the year include spyware attacks against activists, political opposition, and critics in Thailand; the situation concerning surveillance technology in Myanmar; and surveillance conducted on Meta's platforms by surveillance-for-hire firms that targeted activists across the region. Impending laws and changes in the existing laws in Cambodia and Myanmar, respectively, will also enable greater digital surveillance, due to Cambodia's plans to implement a national internet gateway similar to the Great Firewall of China, and the Myanmar military's amendment of laws to allow for the justification of state surveillance.

As the majority of existing personal data protection laws in the region do not apply to public agencies, protecting citizens from government-led digital surveillance remains very challenging. However, the possibility of establishing laws on personal data protection to protect citizens from digital surveillance is also challenged by existing laws that permit lawful surveillance by the government. The implementation of new personal data laws that prohibit state surveillance will collide with these existing laws unless these laws are amended. Moreover, the most vulnerable groups most likely to be targeted by government-led digital surveillance are activists, journalists, political opposition members, and critics of the regimes. Region-wide repressive laws prescribing activities critical of the repressive regimes as crimes constitute the key factor that drives much of the justification provided for digital surveillance.

Digital contact tracing is still ongoing in Southeast Asia after being first rolled out in 2020. However, health experts across the region claimed in 2021 that this approach has not helped to control the pandemic. It is also an approach that has put privacy at risk, discriminates against those who do not own a smartphone in terms of participating in the scheme and is extremely resource-sapping. Despite these weaknesses, governments across Southeast Asia are still moving forward with the initiative. Singapore is a leading country on this initiative and is considered the most successful; nevertheless, for various reasons, other countries have not been able to follow the Singaporean model. Furthermore, some health experts in Singapore also question whether digital contact tracing is still necessary after vaccinations, given that more than 90 percent of the population has been vaccinated. It must also be noted that, Singapore's digital contact tracing effort is unlikely to be easily dismissed as the government announced that the data collected would be used for criminal investigations in early 2021 and even issued a law to support this.

1. 2021 : The Rise of Digital Surveillance

Digital surveillance expanded rapidly in 2021. A significant number of Thai activists who participated in pro-democracy movements found themselves being targeted by spyware. GPS devices were also used on some of them. Hundreds of individuals in Thailand were also accused of opposing the monarchy, a highly sensitive issue in the country, and found their personal information appearing on Google Maps. Digital surveillance is also on the rise in Myanmar following amendments of the laws that have paved the way for the military to conduct lawful digital surveillance. It is now highly likely that privacy will continue to be at great risk as all telecommunications service providers in the country must follow the junta's requests to intercept their users' communication. The possession of surveillance tools by the military is also concerning. In Cambodia, as the country also plans to implement the national internet gateway, this will lead to the increased sophistication and coordination of digital surveillance in the country. Meta's discovery that dissidents around the world have been targeted by surveillance-for-hire firms also reveals the extent to which digital surveillance efforts are employed against dissidents in Southeast Asia.

In November 2021, Thailand came under the spotlight when a number of pro-democracy activists and academics reported receiving an email from Apple, informing them that their devices had been targeted by "state-sponsored attackers"[95]. These devices are believed to be attacked by Pegasus spyware sold by an Israeli company, the NSO Group, whose products are sold to governments across the globe. The spyware is considered to be one of the most well-known and most sophisticated spyware in the world. More than 20 dissidents have reported receiving the notification email from Apple, but the number of those who were attacked is believed to be much higher, including Android users.

Other attacks in 2021 on the privacy of dissidents involving technology include incidents related to the personal information of hundreds of people appearing on Google Maps and the arbitrary installation of GPS devices on activists' cars. In June 2021, the personal information of nearly 500 people claimed to be opposers of the monarchy was found on Google Maps. The data, including names, addresses, and photos was placed on the maps by royalist activists. These activists also declared their intention to report the names to the police for insulting the monarchy. Many of those whose information was included on the map were students. In August, one of the political opposition figures and at least three activists reported that a GPS tracking device was found installed in their cars without their consent[96].

In the same month of August, a document containing a watchlist of 183 people and 19 social media accounts was also leaked[97]. This list included opposition politicians, pro-democracy activists, civil society members, journalists, exiled dissidents wanted for lèse-majesté, and at least two minors aged 15 years old. Apart from the names, the list included ID photos, ID and passport numbers, criminal records and data confirming whether they were in the country or abroad. The records of flight numbers and destinations of those who were abroad were also included on the list.

95 Wongcha-Um, Panu, and Fanny Potkin. "Apple Warns Thai Activists 'State-Sponsored Attackers' May Have Targeted IPhones." Reuters, 25 Nov. 2021, www.reuters.com/technology/apple-warns-thai-activists-state-sponsored-attackers-may-have-targeted-iphones-2021-11-24.

Another issue of concern in Myanmar is the amendment of the 2004 Electronic Transactions Law and Law Protecting the Privacy and Security of Citizens in February 2021, shortly after the coup. The amendment of the laws has opened opportunities for greater threats towards the right to privacy. The combined effects of the amendments allow the Myanmar military to arbitrarily arrest and indefinitely detain individuals in the country, seize or destroy devices and properties, intercept communications, access personal data wherever it is located, and demand information from telecommunications service providers. Following the amendments, the government under the Myanmar military reportedly introduced an "AI system" that allows the monitoring of calls, text messages, and locations of selected users in real time. According to the report by Frontier Myanmar, the system has the ability to detect words considered as anti-Tatmadaw, such as "protest" or "revolution"[98]. On detection of such words, the system will reportedly automatically record the communication, and police will be notified by the system to review the conversation. This system was reportedly installed by the military-linked operators, Mytel and MPT, in July 2021.

This development corresponds with Telenor's reported reason for leaving Myanmar. As one of the major telecommunications service providers in the country, the company stated that they were obliged to activate intercept equipment as requested by the Myanmar authorities[99]. This incident suggests that other service providers are likely to find themselves in the same situation, which, in turn, represents a serious threat from digital surveillance for Burmese citizens. The possession of surveillance tools by the Myanmar military, revealed by Justice for Myanmar, is also concerning, although the use of these tools is still largely undisclosed to the public.

Cambodia passed the Sub-decree on the Establishment of National Internet Gateway (NIG) on February 16, 2021, and, when fully implemented, the government's digital surveillance efforts are expected to become much more coordinated and sophisticated vis-a-vis people's online activities. Due to the close relationship between Cambodia and China, it is highly likely that the NIG will be modeled after the Great Firewall of China to monitor people's internet activities in Cambodia. Telecommunications service providers, as well as social media companies, are likely to face intense pressure in terms of their operations in the country as they will be required to choose between the government's requests and their users' human rights.

In December 2021, Meta announced that it had identified six firms and two unknown entities that had conducted surveillance on its users. The surveillance was divided into three stages: Reconnaissance, Engagement, and Exploitation. According to Meta, Reconnaissance is when firms collect, retain, analyze, and search for information pertaining to their targets. Engagement is when firms aim to establish contact with the targets or people close to them to build trust, gain information, or trick them into clicking on links or downloading files. Exploitation is when the firms "hack" or access the personal information of the targets[100].

96 "Aabtid GPS Nak Kitjakam Tammaidai Maimee Kotmai Rongrub." iLaw, 18 Aug. 2021, freedom.ilaw.or.th/blog/GPDnotlegal.
97 Ngamkham, Wassayos. "Immigration Bureau Denies Political Watchlist." Bangkok Post, 10 Aug. 2021, www.bangkokpost.com/thailand/general/2163231/immigration-bureau-denies-political-watchlist.
98 "Junta Steps up Phone, Internet Surveillance – with Help from MPT and Mytel." Frontier Myanmar, 5 Jul. 2021, www.frontiermyanmar.net/en/junta-steps-up-phone-internet-surveillance-with-help-from-mpt-and-mytel.
99 "Continued Presence in Myanmar Not Possible for Telenor." Telenor Group, 15 Sept. 2021, www.telenor.com/media/announcement/continued-presence-in-myanmar-not-possible-for-telenor.
100 Dvilyanski, Mike, et al. "Threat Report on the Surveillance-for-Hire Industry." Facebook, 16 Dec. 2021, about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

Accounts from Myanmar, Vietnam, the Philippines, Thailand, Indonesia, and Singapore, reportedly belonging to journalists, activists, government critics, and political opposition, appear to have been targeted. According to the report by Meta, accounts in Indonesia and Thailand were targeted by an Israeli-based company called Cognyte, formerly known as WebintPro. Meta states that Cognyte sells access to its platform, using fake accounts across social media platforms to collect data and socially-engineer people. The surveillance stages attributed to Cognyte are Reconnaissance and Engagement. Vietnam and the Philippines are reported to be targeted by Cytrox, a North Macedonian company that develops and sells surveillance tools and malware. The company enables its clients to access information from iOS and Android devices. Users in Myanmar are reported to be targeted by an unknown entity in China. The phases of attacks are Reconnaissance and Exploitation and are believed to target ethnic minorities in the country. Regarding Singapore, DigitalReach has been informed that activists in the country have also received a notification from Meta although the country did not appear in the report. Even though the attacks focus on dissidents, it has not been confirmed whether the attacks are from state actors or not.

2. Privacy (without) Protection Continues

Despite the rise in digital surveillance in Southeast Asia, the privacy of dissidents across the region is unlikely to be protected by any law or mechanism. On the surface, Southeast Asian countries have appeared to step up their efforts to protect personal data. Several countries have adopted, amended, or drafted a law related to personal data in recent years. However, despite these developments, a closer look reveals that protection of personal data in the majority of Southeast Asian countries has not provided people with protection from state surveillance.

On February 9, 2021, Vietnam proposed a draft personal data law. This represents a significant development in the country, as it will lead to the first comprehensive personal data law when enacted. However, as expected, government agencies are exempted from the law, which paves the way for state surveillance[101]. Its drafted Article 10 states that all personal data, including data of a sensitive nature, is subject to being processed without consent in situations which relate to national security, public security, and public order; investigations and convictions of legal violations; and other circumstances according to the law.

In the case of Indonesia, no personal data protection law was passed in 2021, even though it had been keenly anticipated. In Thailand, the enforcement of the Personal Data Protection Act (PDPA) was postponed for the second time in 2021, with very little progress made after the law was first passed in 2019, including the setting up of an official committee to enforce the law. The reason given for the first postponement was that "the public and private sectors are not yet ready for the full enforcement as there are high technology requirements for its compliance and the COVID-19 pandemic." The reason for the second postponement was due to the multiple challenges posed by the creation of the law for both local and foreign businesses. The country officially announced the exemption

101 Long, Trinh Huu. "9 Takeaways from Vietnam's Draft Decree on Personal Data Protection – The Vietnamese." The Vietnamese Magazine, 19 Feb. 2021, www.thevietnamese.org/2021/02/9-takeaways-from-vietnams-draft-decree-on-personal-data-protection.

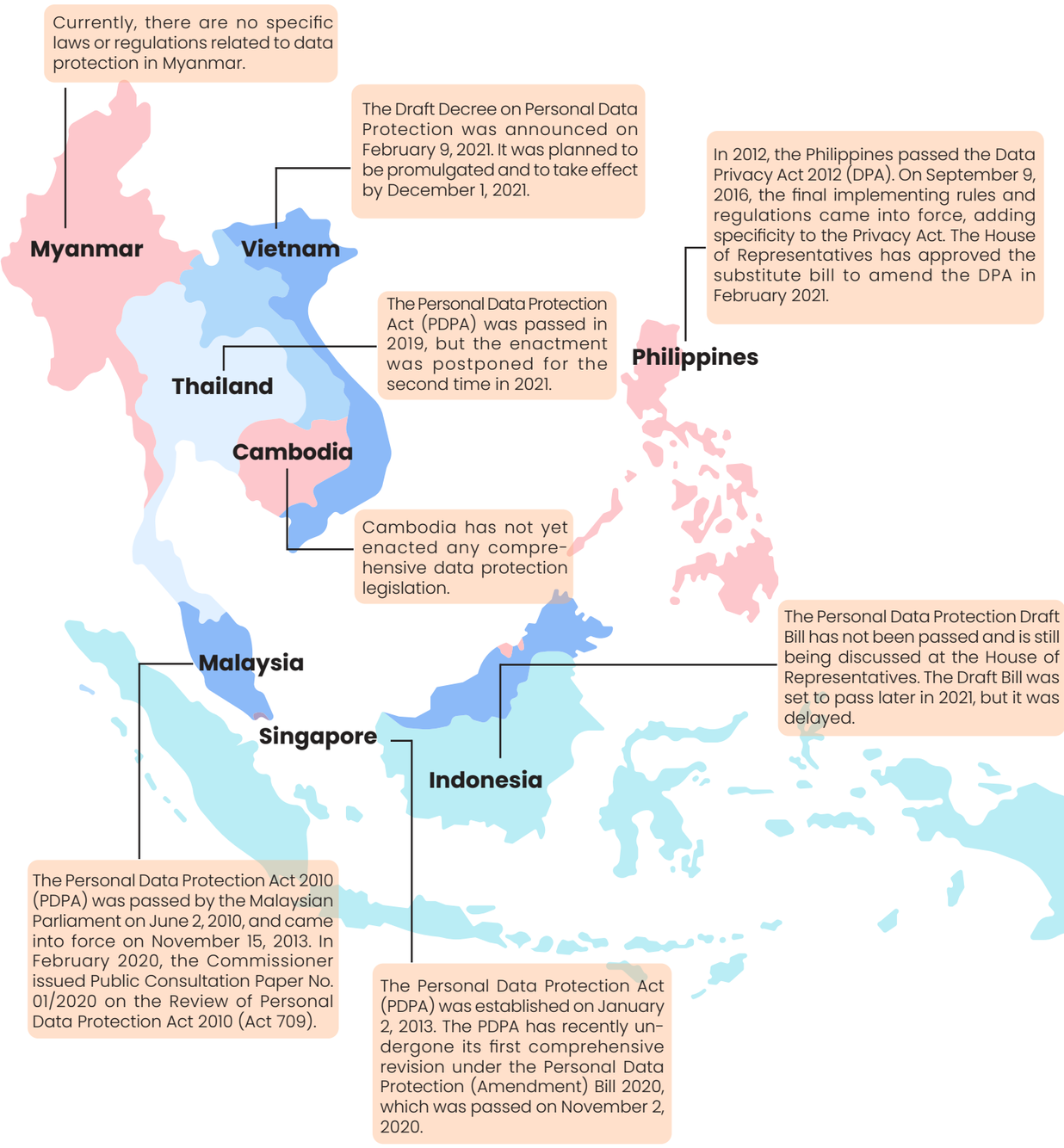
of 22 businesses and agencies, which included government agencies, following the first postponement in 2020[102]. This announcement raised significant concerns related to which businesses or agencies the law would apply to when it takes effect.

Singapore amended the 2012 Personal Data Protection Act, with the amended law coming into effect on October 1, 2021[103]. The amendment brought minor changes to the law without significantly affecting the original content. It applies to only private agencies, while data management in the public sector is governed by the 2018 Public Sector (Governance) Act (PSGA). However, in terms of the PSGA, it also remains for the government to decide whether personal data is threatened by a public agency. In terms of Malaysia, there was no significant development related to the 2010 Personal Data Protection Act in 2021, while Cambodia does not have a specific personal data law in place.

The Philippines is the only country in the region that experienced positive developments concerning personal data protection in 2021, as the Data Protection Act 2012 (DPA) is set to be amended to incorporate more comprehensive personal data protection. The substitute bill to amend the DPA was approved by the House of Representatives on February 4, 2021[104]. The personal data law in the Philippines is currently the only personal data law in Southeast Asia that includes the state agencies. This amendment would empower the National Privacy Commission (NPC), a committee that oversees personal data protection in the country. The law would also empower the NPC to bring action against violators.

102 "Thailand Delays Data Law by a Year as Pandemic Stalls Preparations." Reuters, 22 May 2020, www.reuters.com/article/us-thailand-data-idUSKBN22Y262.
103 "Personal Data Protection Act 2012." Singapore Statutes Online, 30 Sept. 2021, sso.agc.gov.sg/SL-Supp/S734-2021/Published/20210930?DocDate=20210930.
104 "A Stronger Data Privacy Law Sought in Proposed Amendments." National Privacy Commission, 25 Jun. 2021, www.privacy.gov.ph/2021/06/a-stronger-data-privacy-law-sought-in-proposed-amendments.

The State of Personal Data Law in Southeast Asia in 2021



When the laws on personal data do not include public agencies, it creates an opportunity for repressive regimes to conduct state surveillance lawfully, and these state surveillance efforts often involve the use of technology. Also, this usually means that there is no regulation or entity that regulates how the state agencies respect privacy or take care of, and use, the personal information of citizens. However, ensuring the laws on personal data in these countries include public agencies is challenging. This is largely due to other existing laws that already allow state surveillance to take place in that country, and the ability of repressive regimes to make state surveillance justifiable under these laws. Therefore, if the law on personal data protection includes public agencies, it can collide with other existing laws that are already in existence.

In Southeast Asia, state surveillance is often carried out as part of criminal investigations. Consequently, while it is still a crime for people to exercise their rights to express criticism of repressive regimes or to play a role in a human rights movement, state surveillance is conducted on these people. Unless these repressive laws that make these kinds of actions a crime are repealed, individuals such as activists, political opposition, journalists, and government critics will always find themselves a target of government-led digital surveillance.

3. The Failed Approaches of Digital Contact Tracing in 2021

Even though digital contact tracing has not been in the spotlight to the same extent as when it was first rolled out in 2020, it is still an important initiative to discuss. Its significance lies in the fact that the majority of countries that have adopted this approach implemented it quickly and without transparency. There was also no legal mechanism to protect data collected from this government initiative even in those countries where laws on personal data information are in place.

Digital contact tracing was rolled out to respond to COVID-19 and to help control the pandemic. This involves tracing where people have been and their timeline of activities in order to prevent the spread of the virus. This approach started in Singapore before spreading to other countries both within and outside Southeast Asia. However, in 2021, many countries experienced failure by adopting this strategy. As well as posing a threat to privacy, there is also very limited evidence to prove that digital contact tracing has helped healthcare workers to control the pandemic.

In Singapore, TraceTogether is no longer seen as necessary, as more than 90 percent of the population has been vaccinated, thus rendering contact tracing impractical or redundant[105]. Singapore is considered the most successful nation in Southeast Asia in adopting digital contact tracing efforts. In order to overcome the technical limitations of a smartphone and also to be able to trace those who do not own a smartphone, Singapore decided to roll out its own digital contact tracing device, the TraceTogether Token, in 2020, to cover the whole population. The factors that led to Singapore's success stem from its status as a relatively small island nation with a population of only 6 million, its capacity to use its own technology for digital contact tracing, and its economic advantage as a wealthy nation that ranks as one of the

105 Kurohi, Rei. "Experts Question Relevance of SafeEntry, TraceTogether amid Endemic Covid-19." The Straits Times, 22 Nov. 2021, www.straitstimes.com/singapore/experts-question-relevance-of-safeentry-tracetogether-amid-endemic-covid-19.

world's highest in terms of GDP per capita[106]. These factors also point to the reasons why other countries in Southeast Asia cannot follow this model in general. The relatively small population of Singapore meant the country could swiftly implement the initiative to cover the whole population. Its geographical advantage as a small island made the logistics of distributing the device more convenient. The ability to develop its own digital contact tracing technology also meant that those in charge of the initiative possessed a thorough knowledge of the software. They could therefore ensure its effectiveness in achieving the government's objectives and overcome any weaknesses found in the software in a prompt manner. Also, as the most technologically advanced and economically strong Southeast Asian nation, the country could draw on its resources to spend on the development and implementation of the initiative.

However, in January 2021, the Singaporean government announced that the information collected would also be used to support criminal investigations, leading to deepening concerns towards the right to privacy being threatened by digital contact tracing[107]. When it was introduced to the public in 2020, the government stated that TraceTogether would not be used for any purposes outside of the public health domain. Nonetheless, the government subsequently passed the COVID-19 (Temporary Measures) (Amendment) Bill in February 2021 to legally allow the use of data for criminal investigations without the need for any recourse to public consultation. According to the bill, the police are able to access the data directly without a warrant. The government seems to have therefore taken advantage of a situation where almost the entire population carries a TraceTogether device. Given that the device played only a minor role after the arrival of the vaccines in 2021, the question of what is going to happen after the pandemic ends remains. Perceptions of Singapore as a surveillance state would certainly become reinforced should this contact tracing device evolve into a tracking device that no longer bears any relation to the pandemic.

In terms of Indonesia's PeduliLindungi, health experts have claimed that the app did not provide many benefits in relation to controlling the pandemic in the country. A number of health experts have also stated that PeduliLindungi had a limited role in bringing about a decrease in the number of infected cases. Not everyone in the country can afford a smartphone to install the app, and those who cannot participate in the digital contact tracing scheme are usually discriminated against. Health experts explained the limitations of the app in controlling the pandemic, as it can only inform users whether people around them are virus-free or not. The government, however, is still persisting with the app. In December 2021, the government announced that it would revoke operation licenses and fine those who did not participate in the scheme. This prompted concern among citizens, especially those who run small businesses. Owners of ***warteg***, a small local food stall, for example, described the adverse impact the policy had had on their businesses, as their customers are usually low-income individuals[108].

Indonesia is also an important example of how privacy can face great risk when there is no legal mechanism to protect it. In August 2021, the data of

106 "GDP per Capita (Current US$)." World Bank, data.worldbank.org/indicator/NY.GDP.PCAP.CD?most_recent_value_desc=true. Accessed 10 Jan. 2022.
107 Illmer, Andreas. "Singapore Reveals Covid Privacy Data Available to Police." BBC News, 5 Jan. 2021, www.bbc.com/news/world-asia-55541001.
108 BBC News Indonesia. "Sanksi pelanggar aplikasi Pedulilindungi menuai kritik: 'negara ini senang sekali menghukum warganya.'" BBC News Indonesia, 23 Dec. 2021, www.bbc.com/indonesia/indonesia-59759975.

1.3 million users related to the government's digital contract tracing scheme, eHAC and PeduliLindungi, was leaked[109]. As Indonesia does not have a personal data protection law, a full investigation to hold accountable those involved in the incident, including the Ministry of Health, has not been carried out. People expressed their anger over the incident, and the Ministry did not even issue a public apology over the situation.

In the Philippines, StaySafe.ph was in the hands of its developer, Multisys, before it was handed to the government on March 3, 2021, after a long delay. According to Resolution No.45 issued by the Inter-Agency Task Force on Emerging Infectious Disease (IATF-EID) on June 10, 2020, the IATF-EID ordered a Memorandum of Agreement (MOA) to be established between Multisys and the Department of Health. Under this MOU, Multisys is required to donate the app to the DOH, which includes source code, data, data ownership, and related intellectual property, within 30 days. The Resolution further mandated this version of the app. However, as the app was only handed to the government in March 2021 after an 8-month delay, this meant that the clause in Resolution No. 45 was violated. The fact that Multisys is a private firm with collected personal data of users in their possession is concerning as the company was alleged to have close ties with government agencies, in particular the National Intelligence Coordinating Agency (NICA) and the National Security Council (NSC)[110].

However, there were improvements in terms of privacy in 2021 on StaySafe.ph. The Google/Apple Exposure Notification (GAEN) system, a decentralized approach to contact tracing, was implemented in May 2021. Multisys also removed the GPS feature which allows a user's location to be tracked in late 2020[111]. However, despite the improvements, Francis Duque III, Health Secretary, stated in August 2021 that StaySafe.ph had virtually no impact on controlling COVID-19 in the country[112]. The reason for this is that the app only seems to act as a digital log when people enter public places and does not have any significance beyond that role. Only 6.4 million people have adopted the system in a country of more than 100 million people[113].

In 2021, Thailand's digital contact tracing efforts, Mor Chana and Thai Chana, disappeared almost entirely from the scene. The general population no longer pays them any attention despite the efforts of the government in 2020 to push for both apps to be widely used. The government faced a public uproar in January 2020 when they stated that those who did not install the app would go to jail. The announcement was later explained to be a misstatement[114]. Since its launch in April 2020, Mor Chana's downloads have only been adopted by around 20 percent of smartphone users in the country as of February 2021[115].

The situation is relatively better in Malaysia and Vietnam in terms of the adoption rate despite the lack of transparency on how their digital contract tracing systems work. MySejahtera in Malaysia is a primary app for digital contact tracing, which claimed to have around 25 million users in April 2021 or 76 percent of the total population[116]. On December 26, 2021, the government rolled out MySJ Trace as part of MySejahtera's features to help users trace close contacts of those who tested positive for COVID-19[117]. They also reportedly developed their own digital contact tracing tokens similar to TraceTogether in Singapore to support those without a smartphone in September 2021[118]. In the same month of September, the Vietnamese government launched a new digital contact tracing app, PC-Covid, that unified all the earlier apps for more comprehensiveness and convenience in contact tracing in the country. The app was developed based on the previous primary digital contact tracing app, Bluezone[119]. As of May 2021, the government claimed that Bluezone had around 33 million downloads which accounted for 34 percent of the total population[120].

Cambodia also launched its own digital contact tracing called "Stop COVID-19" in February 2021, a QR-code-based contact tracing app. Following the launch, it was alleged that China requested access to personal data collected via the app. The Chinese government allegedly needed the data to support the monitoring of citizens who traveled between the two countries. In return, China would help the Cambodian government to upgrade the existing system to be more efficient with support from the well-known tech company Huawei[121]. The Cambodian government later denied the allegation by stating that there was no request from the Chinese authorities[122]. As a country without a personal data protection law, the personal data of Cambodian citizens is exposed to great risk regardless of whether the allegation is true or not. The app also lacks transparency, as little information is publicly available regarding how the system works. As of May 2021, the government claimed that more than 77 percent of the 21 million mobile phone users had adopted the system[123].

However, despite these efforts, any country whose digital contact tracing still relies on smartphones will continue to encounter problems as the majority of the population cannot participate in digital contact tracing, and face technical limitations. It will also continue to raise concerns among health experts over its effectiveness, regardless of the government's efforts. Moreover, vaccines arrived in 2021, and despite the successful adoption of digital contact tracing in a country like Singapore, the question arose as to whether the initiative is still necessary given that the majority of the population has been vaccinated and rarely show serious symptoms. As the initiative does not provide us with any solid evidence of how it can control the pandemic, it may be concluded that digital contact tracing is a privacy-risk initiative, a very questionable use of resources, and lacks effectiveness in controlling the pandemic.

109 Chandra, Grace Nadia. "Gov't Launches Investigation After Data of 1.3m Reportedly Leaked From Its Covid-19 Tracking App." Jakarta Globe, 31 Aug. 2021, jakartaglobe.id/tech/govt-launches-investigation-after-data-of-13m-reportedly-leaked-from-its-covid19-tracking-app.

110 Ranada, Pia. "'Borderline Spyware': IT Expert Raise Alarm over Duterte Admin Contact-Tracing App." Rappler, 8 June 2020, https://www.rappler.com/newsbreak/in-depth/263090-borderline-spyware-information-technology-experts-alarm-stay-safe-app.

111 Ferreras, Vince. "No More GPS, Bluetooth in StaySafe System Following Data Privacy Concerns." CNN Philippines, 14 Dec. 2020, cnnphilippines.com/news/2020/12/14/StaySafe-remove-GPS-Bluetooth-data-privacy-concerns-.html.

112 Gonzales, Cathrine. "Duque Admits 'StaySafe' Contact Tracing App Had 'Almost No Impact.'" INQUIRER, 14 Dec. 2021, newsinfo.inquirer.net/1478717/duque-admits-staysafe-contact-tracing-app-had-almost-no-impact.

113 Romina, Alexis, and Cabrera Romero. "StaySafe App Useless? DICT Told to Explain." Philstar, 27 Aug. 2021, www.philstar.com/headlines/2021/08/27/2122902/staysafe-app-useless-dict-told-explain.

114 Bangprapa, Mongkol, and Apinya Wipatayotin. "Govt U-Turns on Mor Chana." Bangkok Post, 8 Jan. 2021, www.bangkokpost.com/thailand/general/2047263/govt-u-turns-on-mor-chana.

115 Promchertchoo, Pichayada. "Data Privacy Concerns over Thailand's COVID-19 Contact Tracing App amid New Wave of Cases." CNA, 8 Feb. 2021, www.channelnewsasia.com/asia/transparency-thailand-covid19-contact-tracing-app-mor-chana-297901.

116 "Saifuddin: MySejahtera Can Be Expanded to Become Super App." The Star, 7 Apr. 2021, www.thestar.com.my/tech/tech-news/2021/04/07/saifuddin-mysejahtera-can-be-expanded-to-become-super-app.

117 Daim, Nuradzimmah, and Teoh Pei Ying. "MySJ Trace: Switch on Bluetooth for Your Safety." NST Online, 28 Dec. 2021, www.nst.com.my/news/nation/2021/12/758476/mysj-trace-switch-bluetooth-your-safety.

118 Alfiq, Faris. "M'sia Is Developing Its Own Contact Tracing Token, Similar to S'pore's TraceTogether." Mothership, 29 Sept. 2021, mothership.sg/2021/09/malaysia-developing-contact-tracing-token.

119 "National Single App for COVID-19 Control PC-Covid Debuts." VietnamPlus, 30 Sept. 2021, en.vietnamplus.vn/national-single-app-for-covid-19-control-pc-covid-debuts/208910.vnp.

120 "HCMC, Vietnam Uses Tech to Monitor People Under Home Quarantine." OpenGov Asia, 9 July 2021, opengovasia.com/hcmc-vietnam-uses-tech-to-monitor-people-under-home-quarantine.

121 Lintner, Bertil. "China Squeezes Cambodia for Its Covid App Data." Asia Times, 10 Jun. 2021, asiatimes.com/2021/06/china-squeezes-cambodia-for-its-covid-app-data.

122 Sochan, Ry. "'Stop Covid' QR Code Report Denounced." Phnom Penh Post, 13 Jun. 2021, phnompenhpost.com/national/stop-covid-qr-code-report-denounced.

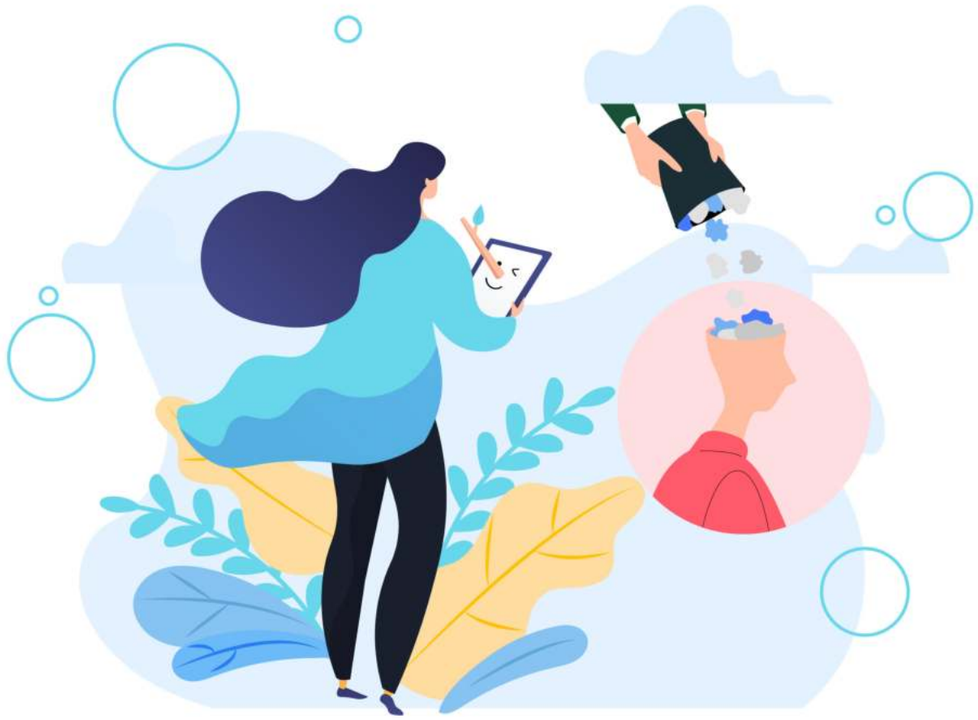
123 Chheng, Niem. "Cambodia Rebuffs Concerns on 'Stop Covid' QR Code." Phnom Penh Post, 21 May 2021, www.phnompenhpost.com/national/cambodia-rebuffs-concerns-stop-covid-qr-code.

The Development of Digital Contact Tracing in Southeast Asia in 2021

Country	Laws/Code	Potential Effects on Social Media Platforms
Cambodia	Stop COVID	Launched in 2021. The app has been criticized for its transparency issues and alleged to have provided the Chinese authorities with access to the collected data.
Indonesia	PeduliLindungi	Involved in data breach incidents at least twice since it was first introduced in 2020. Health experts also claimed that the app does not help in controlling the pandemic.
Malaysia	MySejahtera MyTrace Gerak Malaysia (dismissed)	My Sejahtera became a primary app for Malaysia. The government has rolled out a new feature.
Philippines	StaySafe.ph	The app has shown positive developments in terms of privacy. However, health experts have stated that it has had a limited role in controlling the pandemic.
Singapore	TraceTogether (token) TraceTogether (app) SafeEntry	Health experts expressed that digital contact tracing might no longer be necessary as more than 90 percent of the population has been vaccinated. However, dismissing its use might be challenging following the government's adoption of the bill to use the collected data for criminal investigations.
Thailand	Mor Chana Thai Chana	Both apps almost completely disappeared from the government's approach to controlling the pandemic.
Vietnam	Bluezone	Merged with the new app, PC-Covid.

*The names are based on when they were first introduced in 2020.

IV
Digital Security



Key Takeaways

- The rise of digital surveillance in 2021 has exposed dissidents to greater digital-related threats. More work on this issue is needed in Southeast Asia as digital-related threats are a significant new challenge to dissidents across the whole region.
- Security threats from state-sponsored information disorders are a cause of great concern given specific developments in 2021. More fact-checking initiatives are required in the region, while existing fact-checking organizations need to be empowered as they are also threatened and experience limited resources and tools.
- Threats against individuals from repressive policies will continue to happen. Apart from policy advocacy, pragmatic approaches, such as training targeted dissidents and those who provide legal assistance on the laws, as well as support through funding and legal procedures, are also needed.

Overview

Threats against the digital security of dissidents in 2021 can be divided into three strands: digital-related threats, threats from information disorders, and threats from repressive policies. In 2021, dissidents have experienced an increase in digital-related threats and are likely to be more exposed to these threats in the future.

Dissidents in Southeast Asia need support in terms of understanding how best to respond to digital-related threats due to the often complex technical aspects involved. More work on this issue is needed to understand its extent in the context of Southeast Asia so that civil society and those who are targeted can better respond to the situation.

As state-sponsored information operations continue to become more sophisticated, as seen in the situations documented in 2021, threats from information disorders against individuals are also likely to become more sophisticated. However, the region still does not have enough independent fact-checking organizations, while such existing organizations are subjected to harassment and lack sufficient resources and tools.

Dissidents will continue to be targeted by repressive laws related to digital space for their digital-related activities. Pragmatic approaches, such as informing and training dissidents and those who provide legal assistance to them to learn more about these laws, can be helpful, as well as assistance in terms of funding and other issues related to legal procedures. These approaches can help targeted individuals to respond more effectively to the situation given the complex technical aspects of repressive laws related to digital security.

1. Unprecedented Exposure to Digital Threats

The rise in digital surveillance, as witnessed through key incidents documented in 2021, has led to the greater exposure of dissidents to digital-related threats. Spyware-driven phone hacking in Thailand, the emergence of state surveillance in Myanmar, the plan to establish the national internet gateway in Cambodia, and the discovery by Meta of attacks on dissidents across the region by surveillance-for-hire companies are all incidents that have threatened the security of dissidents in the region. Other digital-related threats include the discovery of the arbitrary installation of GPS tracking devices and exposure of personal information on Google Maps in Thailand, as well as new tactics employed in cyberattacks in the Philippines.

From the discovery of spyware, believed to be Pegasus, in Thailand, it is evident that dissidents need to first and foremost understand these types of threats and how to protect themselves. A positive first step would be to build an understanding of basic digital security, such as ensuring that one's phone's operating system is up-to-date, using secured messaging applications and enabling the disappearing feature, and using two-factor authentication. Gathering more evidence in order to hold the attackers accountable can be difficult due to the nature of these incidents. Pegasus's manufacturing company, the NSO Group, for instance, long criticized for the sale of their products by repressive governments, have always ensured the confidentiality of the purchasing process as well as its use by the purchasing party.

Threats made against Burmese citizens are also sophisticated due to the different tactics used by the Myanmar military. This includes the ordering of telecommunications service providers to install interception technology, as well as an alleged plan to implement the internet firewall following the Chinese model, tactics which are applied not only to dissidents but to the whole Burmese population. Different tactics and strategic approaches have to work together to respond to each specific situation. However, as these security threats apply to the whole population, it is extremely challenging to keep everyone safe. Another challenge is offering assistance to those who are inside the country, due to the high risk involved.

Future changes to the national internet gateway plan in Cambodia are likely to be implemented stepwise. As with Myanmar, the threats also apply to the whole population and not only dissidents. Surveillance efforts will be much more coordinated, even though it is still unclear as to how this will evolve. Given the specific local context of Cambodia, it is unlikely that the tactics will be a carbon copy of the Great Firewall of China. Apart from policy advocacy, civil society in Cambodia must also consider an approach to both monitoring the situation and protecting themselves from these looming threats.

Meta's discovery of the attacks by the surveillance-for-hire firms, which included dissidents in Southeast Asia among their targets, has introduced a new kind of threat against digital security. Even though Meta has taken action against these companies, dissidents who received a notification from the company should take the time to fully understand the three-phased tactics

of Reconnaissance, Engagement, and Exploitation. Engagement and Exploitation are the two tactics that can be visibly observed by the targeted users, and basic digital security knowledge can help them, before turning to assistance from experts, to initially respond to the situation in case it, or a similar situation, happen again.

Overall, these incidents should alert civil society groups that work on digital security to assess their approaches towards helping targeted activists, lawyers and critics to best respond to these situations, which are likely to become more intense in the near future. More work on this issue has to be carried out to gain a better understanding of the full extent of the situation. As the rise of digital-related threats continues, dissidents in the region are likely to encounter challenges in dealing with these types of threats due to the need for specific technical knowledge. However, accessing the inner circle of these targeted dissidents can also be challenging in some countries as most digital security work in Southeast Asia is carried out by international organizations.

Language barriers can also be a restrictive factor for targeted dissidents in the region, as the majority do not speak English as their first language. Based on DigitalReach's experience, these targeted dissidents who are non-native English speakers feel more comfortable discussing their situation with people they trust and who speak the same language. This also influences the likelihood of their reaching out when they have concerns or when they report a situation on being approached for a follow-up. Moreover, younger dissidents tend to need more emotional support apart from the consultation on how to protect and prepare themselves from potential threats. Their fear of being targeted is more intense, especially if the individual is new to activism. To ensure its effectiveness, digital security protection should also be approached as an ongoing process, and not simply end with a one-time consultation after a threat is discovered.

2. Threats from Information Disorders Are Concerning

Based on what the organization has explored, ranging from the state-sponsored information operations in the Philippines linked to red-tagging campaigns and the expansion of Force 47 in Vietnam, to the spread of information disorders in Myanmar onto emerging social media platforms such as TikTok and Telegram and the discovery tactics of information operations used against dissidents in Thailand, information disorders are likely to evolve and become more sophisticated with time.

Dissidents targeted by state-sponsored information disorders represent an acute challenge due to the often unknown tactics and structures employed. In addition, when these elements are unknown, it is very difficult to assess their potential and prepare for possible attacks. To develop a fuller understanding of these operations, further research, study and documenting is needed. This includes, for example, the patterns of attacks, their development, and the consequences of the attacks.

Furthermore, the lack of independent fact-checking organizations in the majority of Southeast Asian countries is also a factor that allows information disorders to spread unchecked. The harassment against existing fact-checking organizations and those who work there, as well as insufficient resources and tools, are also important factors that can affect the efficiency of their fact-checking. A network of fact-checking organizations in the region might also help in responding to the threats, as organizations can brace themselves for the threats within a unified network, as well as collaboratively share fact-checking tactics with each other.

Expecting social media platforms to successfully tackle false, fake, and misleading information can also be challenging based on the aforementioned situations. However, information disorders overlooked by the platforms can lead to dangerous threats to an individual's online and offline security. As documented, both mainstream and emerging platforms still need to step up their efforts to tackle information disorders and hate speech in Southeast Asia. Given the highly diverse cultures of the region, tackling information disorders and hate speech often found in native languages can be a real challenge which requires social media platforms to work with civil society to a certain degree. Given Southeast Asia's status as an important market for smartphone users, with Indonesia, Vietnam, the Philippines, and Thailand boasting some of the highest numbers of users in the world, social media platforms need to show accountability to protect their users' human rights[124].

3. Threats Against Repressive Policies Will Continue

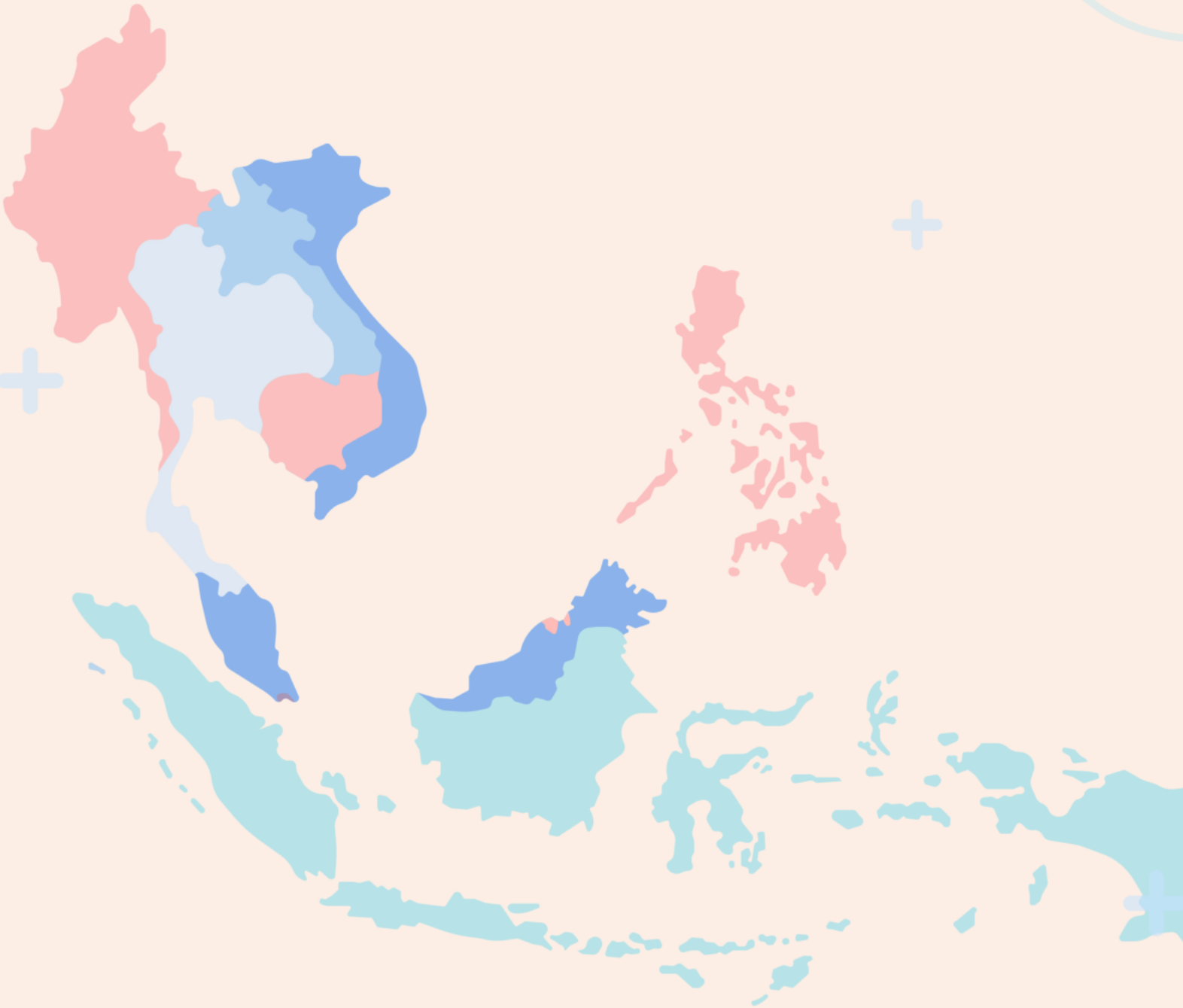
Dissidents will continue to be harassed by repressive laws based on their digital-related activities. Over the past few years, individuals across the region have been harassed, arrested, detained, charged, and imprisoned as a result of these repressive policies. As long as these specific laws exist and as long as these regimes continue to wield power, these laws will continue to be used to threaten dissidents.

2021 is no exception. As more repressive laws are being proposed and adopted, from laws to control social media in countries across Southeast Asia to the law on foreign interference in Singapore and the law to build the national internet gateway in Cambodia, dissidents will face new menaces while continuing to be threatened by existing repressive policies.

Apart from policy advocacy, knowing and understanding what threats are being faced is also important to protect digital security. Consideration should be given to strategic approaches to raise awareness, inform or train dissidents and those who provide legal assistance to ensure a fuller understanding of the possible threats posed by these laws. Some of these repressive laws that threaten digital security require specific technical understanding, the knowledge of which would lead to greater confidence and empowerment. Another approach may consist of preparatory measures to save these dissidents, through funding and assistance for other issues related to legal procedures. All these suggested approaches are crucial elements which require careful consideration for online and offline security protection.

Assessing the impact of such approaches that rely on human rights principles on policy advocacy can be challenging. Often, this is a long-term process, as culture plays a crucial role in how these laws are constructed in the first place within the broader culture of authoritarianism in the region.

124 "Smartphone Users by Country Worldwide 2021." Statista, 24 Jun. 2021, www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users.



DigitalReach

www.digitalreach.asia