With civic space in Southeast Asia (SEA) being threatened by governments and their policies, the internet and social media started to be used by human rights defenders (HRDs), activists, journalists and civil society as a free space to share their opinion on their governments and to hold them accountable. With the internet used as a democratic space, governments have also started to control and censor the internet. To do so, a set of laws and policies have been developed to stop and punish the sharing of information critical of the monarchy, the government, or its policies, using the justification of protecting ‘national security’. This leads to the silencing of dissent and the practice of self-censorship even in cyberspace, by those from ASEAN countries. During the COVID-19 pandemic, this has been even more challenging with the use of emergency laws to restrict sharing of opinions of the COVID-19 response or situation in countries, and with internet shutdowns being a barrier to access information related to health risks.

Leading civil society expert voices working on the ground in Southeast Asia will highlight the legal challenges using cases from Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam. This session will also be used as an opportunity to address the rise of digital dictatorship in ASEAN with strategies to fight back violations of online freedom, online privacy, and access to information presented, so digital rights of individuals and national security of a country can coexist in the post COVID world.

National Security & the challenge to Digital Rights in ASEAN countries

In Southeast Asia, an increase in online surveillance, arrests, court trials, punishment, imprisonment, intimidation and threats have become a common occurrence, with ‘protection of national security’ used as a broad excuse. Although under international law, freedom of expression can be restricted for the protection of national security and public order, this can only be done in special circumstances and with proper proof. However, instead of using protection of national security as an exception, governments in Southeast Asia apply this as a rule and claim everything as a threat to ‘national security’. Of these, the most common use of national security by governments has been to protect their interests, both political and economic and so any criticism of the actions governments take is seen as a threat by them. This practice continues as ‘national security’, is not defined by national law, and is open to the interpretation of government officials and bodies.
In Cambodia, the press, netizens, anti-monarchy critics, opposition political parties, social media, as well as telecom & tech companies are all strictly controlled by the government through laws, regulations and task forces that monitor the internet. To start with, changes to Article 42 and 49 of the Constitution of Cambodia in February 2018 used overly broad language to require both Cambodian citizens and political parties to ‘uphold national interests’ and prohibits them from doing ‘any activity’ that will ‘directly or indirectly’ threaten these interests. National interest has been interpreted by the government to include the interest of the ruling party, and so any critic of government policies is seen as a threat to national interest. This completely compromises the basic idea of a democracy, with citizens and opposition political parties not allowed to hold the government accountable for its actions.

To further restrict use of the internet, in 2018, the government took three actions against internet service providers (ISPs) and websites, stating that it was necessary to prevent the spread of information that will cause chaos and threaten national security. The first was the government forcing all ISPs to pass their customers’ data through a state-owned data management centre. The second was the passing of an Inter-Ministerial Regulation on Websites and Social Media Control under which all ISPs have to install surveillance software to filter and block online content and users, according to Clause 7(b). These companies also must assist the Ministry of Information and other ministries to block or close websites or pages on social media with content that harms national security, public interest and social order, as per Clause 7(c). The third was the blocking of at least 15 independent news websites by the government in Cambodia a day before the elections, including the websites of Radio Free Asia (RFA) and Voice of America (VoA) with pro-government websites continuing to operate without restriction. These restrictions were placed using Article 72 of the Law on the election of Members of the National Assembly (LEMNA), which in reality does not cover the media.

On 30 April 2020, a Law on the Management of the Nation in State of Emergency was adopted. This law expands the power of the government allowing to control sharing of information that can scare people, cause unrest or that can negatively affect
national security, with imprisonment up to 10 years and fines of USD 250,000 as punishment. It also allows any measures to
monitor, view and collect information from telecom devices such as phones, laptops and computers using any methods
necessary.

PENALTY FOR SHARING COVID-RELATED INFORMATION OR CRITIQUE OF
GOVERNMENT RESPONSES

Although an emergency has not been declared in the country and the emergency decree is not being implemented, it continues
to be dangerous that the law comes at a time when more than 40 people have been arrested by the Cambodian government for
sharing COVID-related information online or for being critical of the government's response to the pandemic. This includes
supporters of the dissolved Cambodia National Rescue Party (CNRP), a 14-year-old girl who only spoke about being scared that
3 of her classmates had COVID-19, and Koy Sam Ath, a 35-year-old who was arrested for a Facebook video where he shared
that it takes Vietnam to point out the existence of COVID-19 cases in Cambodia.

CRIMINALISING AND PUNISHING ONLINE DISSENT AGAINST THE
GOVERNMENT, ITS REPRESENTATIVES AND ITS POLICIES

This is alongside the increased use of criminal law to silence offline as well as online dissent. Any allegation or charge even if it
does not cause actual harm can be criminalised and punished as defamation, under Article 305 of the Criminal Code. Under this,
truth or public interest cannot be used as defense, and not just a person but also an institution can bring defamation charges.
This was seen in the form of 19 individuals being punished between April 2019 and March 2020, for their criticism of Prime
Minister Hun Sen, the government and its policies. Additionally, incitement charges are also used extensively under Articles 494
to 497 of the Criminal Code against journalists, with their press license being revoked. For instance, journalist Sok Oudom was
charged following a Facebook live report on a land dispute; a TVFB journalist was charged for sharing a quote made by Prime
Minister Hun Sen in response to the COVID impact faced by motorcycle taxi drivers; and journalist Ros Sokhet, publisher of
Khmer Nation was arrested for being critical of the Prime Minister and his poor response to COVID-19. Despite the
development of new laws and regulations, incitement continues to be Cambodia's blanket provision used to quash any form of
political dissent.

OUR CALL TO ACTION

We urge the government of Cambodia to stop misusing broad laws and policies or harmful actions to monitor political
opponents, activists, HRDs and netizens; censor dissent; and compel tech companies to contribute to these violations without
accountability or oversight; and call for the protection of civic space, online freedom and online privacy in line with international
human rights law.

OVERALL CONTEXT OF CIVIC SPACE IN INDONESIA

Internet in Indonesia does not enjoy much openness or safety. Most laws and actions in the online space were taken because of
the spread of misinformation or disinformation and the resulting riots, immediately before or after the elections. Instead of
helping the public, these laws are used to restrict online freedom of expression and information. At the outset, with an
amendment to the Constitution in 2000, Article 28(j) allows the rights of individuals to be restricted based on security considerations amongst other aspects. As an example, the 2011 Intelligence Law expands the powers of security agencies to do online surveillance for gathering ‘intelligence’ against those who oppose national security, which has led to fear and self-censorship amongst internet users.

MISUSE OF THE LAW ON ONLINE INFORMATION EXCHANGE TO RESTRICT ONLINE FREEDOM

The 2008 Electronic Information and Transactions Law (ITE) was developed to regulate exchange of information and other electronic transactions. The stated purpose of the law was for the use of information technology to give security. This law explains the offences of online defamation, hate speech and incitement to violence and punishes them, but with harsher punishments than what is provided by the Penal Code for these actions offline. Distribution of online information which contains insults and defamation is prohibited by Article 27(3) of this law and Article 28(3) of the law prohibits online hate speech. However, various individuals accuse online journalists of these online crimes, simply when they do not like the news coverage or when it accuses them of actions that are corrupt or criminal. The Ministry of Communications and Information Technology (MCI) can also use the law to prevent access to online information by ordering internet service providers to do so, under Article 40.

According to an article by New Naratif titled ‘Silenced by an Elastic Law’, of the 245 complaints filed using the ITE law in 2018, about 35.92% of them have been submitted by government agencies and officials. These cases also have a high conviction rate, with people in only 6% of the cases submitted being declared as innocent. For instance, Muhammad Yusuf, a journalist working with independent news site Kemjuan Rakyat was arrested and charged with hate speech in April 2018 for his critical reporting of a land dispute between farmers and a palm oil company owned by a powerful businessperson, but he died in detention due to failure to provide proper healthcare. In a recent case, Diananta Putra Sumedi, editor-in-chief of media site Banjarhits.id was arrested on 9 September 2019 for reporting on a land dispute between indigenous peoples and a palm oil company in South Kalimantan. On 10 August 2020, he was found guilty of online hate speech and sentenced to 3 months and 15 days in prison by a panel of judges in Kotabaru district court.

INTIMIDATION, HARASSMENT AND THREATS AGAINST GOVERNMENT CRITICS DURING THE COVID-19 PANDEMIC

Targeting government critics, journalists and academics with intimidation, harassment and threats has continued during the COVID-19 pandemic, with many of them becoming victims of cyberattacks. In 2020, at present already 50 cyberattacks have been recorded against individuals from at-risk groups. For instance, activist Ravio Patra's phone was hacked and a WhatsApp message was broadcast from it, following which he was detained and accused of instigating riots. Students, their parents and a teacher from the Gadjah Mada University of Yogyakarta were threatened through messages, their phones, and on social media for organising an online discussion on the steps provided by the Constitution to dismiss a President. This was initiated following growing discussions amongst the public on the poor handling of COVID-19 by the President.

INTERNET SHUTDOWNS, CENSORSHIP AND BLOCKING ACCESS TO INFORMATION

Internet shutdowns have been used to crush dissent. In May and then August to September 2019, protests erupted following the arrest and release of 43 students from Papua and West Papua who were found innocent of destroying the national flag. As a result, the MCI blocked internet access and slowed the sharing of videos, voice messages, images on social media platforms
We call on the government of Indonesia to put an end to the misuse of Constitutional provisions, internet regulation policies, and use public panic as an excuse to block the internet or create fear and self-censorship. Online freedom, online privacy and access to information for all must be protected, with a human-centered approach adopted in line with international human rights law, as a way to address any situation even if a threat to public peace.

OUR CALL TO ACTION

Laos PDR

OVERALL CONTEXT OF CIVIC SPACE IN LAO PDR

As a one-party state, online and offline civic space in Lao PDR are under the control of the Lao People’s Revolutionary Party (LPRP). With state control of the media, surveillance of civil society & intimidation of critics, an environment of fear and self-censorship continues to exist with people not able to speak freely in the country. In the context of Lao PDR, national security includes stability of the political regime and its economic policies, with laws and policies in place to protect the LPRP and to ensure it continues to be in power.

MISUSE OF LAWS AND POLICIES MEANT TO INTIMIDATE NETIZENS AND INCREASE SELF-CENSORSHIP

To intimidate internet users and control the information they share, in 2014, the Lao government developed Decree No. 327 on Internet-Based Information Control or Management to stop the sharing of information believed to be a threat to national security. According to this decree, netizens that share information critical of the Lao government or its policies that is believed to be untrue will face criminal charges. Internet providers who allow for such information to be shared will also face the same charges. The 2015 Law on Prevention and Combating of Cyber Crime is another law, developed to prevent cybercrime as a way to protect national security. While national security is not defined in this law, Article 39 restricts sharing information that would harm or go against the political regime causing chaos in society.

CRIMINALISING AND PUNISHING HRDS AND ACTIVISTS FOR ANY CRITICISM OF THE LAO GOVERNMENT AND ITS BAD POLICIES

At present, the Lao government has increased its use of Article 117 of the Penal Code to criminalise any online criticism against their policies and actions. With the purpose of the Penal Code also being to protect national security and public order; Article 117 punishes those who are critical of the LPRP, the Lao government, or its policies with 5 years in prison and a fine of 20 million kip or USD 2,200 for ‘propaganda against the state.’ Articles 56 and 72 of the Penal Code have also been used to arrest and imprison HRDs and other persons.

HRDs and activists who express views that are critical of government policies and actions are targeted, arrested, charged, and imprisoned without a proper trial, so no one else points out the faults of the government. This strategy is specifically used when economic development policies of the government for dams, mines, plantations and other projects are criticised for
destroying the environment, land, homes and livelihood of the Lao people. For example, Houayheuang Xayabouly also known as Muay, a prominent environmental activist and a single mother to a 5-year old is currently serving a 5-year prison sentence for violating Article 117 of the Penal Code, only for speaking out on social media about the harm caused to the Lao people by development projects, businesses and corruption. Other such cases include the 4-year & 9-month imprisonment of Lao-born Polish citizen, Bounthanh Thammavong for criticising the policies and actions of the government on Facebook; and the ongoing prison sentences of three activists Lodkham Thammavong, Soukane Chaithad and Somphone Phimmasone for 12 years, 18 years and 20 years respectively for a Facebook post where they claimed there was no democracy in Lao PDR.

**CRIMINALISATION OF ONLINE EXPRESSION DURING COVID-19**

The violation of online freedom continues even with the COVID-19 public health emergency situation. To illustrate, a 25-year old woman was arrested in February for sharing information that COVID positive individuals were shopping in a Vientiane mall. Additionally, Kot, a 27-year old Lao migrant worker was arrested in March 2020 for a Facebook video, in which he criticized the conditions of the quarantine camp, claiming it was not hygienic, overcrowded and without medical staff.

**OUR CALL TO ACTION**

We urge the government of Lao PDR to stop criminalising legitimate forms of online expression, preventing access to independent information, and forcing self-censorship, that violate the online freedom and online privacy of the Lao people in line with its international human rights obligations.

**MALAYSIA**

**OVERALL CONTEXT OF CIVIC SPACE IN MALAYSIA**

National security and public order are protected in Malaysia, but at the cost of freedom and privacy on the internet – with race, religion and royalty, often with a political agenda given more importance than individual rights & freedoms.

**CENSORING INFORMATION BY MISUSING LAWS AND AUTHORITIES THAT ARE MEANT TO REGULATE COMMUNICATIONS AND ONLINE MEDIA**

The 1998 Communications and Multimedia Act (CMA) specifically states nothing in the law shall be interpreted as allowing internet censorship. However, in practice the CMA has been used to block websites as well as to arrest and charge individuals sharing information that is critical of the political party in power or the government. In particular, Sections 233 and 236(2) of this law have been used to target online freedom. Section 233 punishes online content shared with the purpose of annoying, abusing, threatening or harassing another person with a year in prison and a fine of up to 50,000 RM (USD 11,730) along with a fine of 1,000 RM (USD 234) for every day it continues to be shared. Additionally, Section 263(2) also forces those who own or provide mobile networks or internet services and applications to assist the Malaysia Communications and Multimedia Commission (MCMC) in preventing any action that violates laws of Malaysia in place to preserve national security. With this, the MCMC has been given broad powers to take control of and shut down mobile operators and internet providers.
The 1948 Sedition Act has also been used to restrict online expression related to the monarchy or even government leaders. In 2015, this law was amended to extend sedition to information shared on the internet allowing the court to order people to remove online content, block access to devices and blocking online content through the CMA if it is found to be sedition. Although the government announced a ban on using this law in October 2018, this ban was lifted and it was stated that the government will use this law but only to punish violations to national security, public order, as well as race and religious relations.

While Malaysia deals with COVID-19, the government has continued to clampdown on any criticism against its policies and actions particularly by the media. For instance, a South China Morning post journalist, Tashny Sukumaran was investigated for her social media posts critiquing the raids and rounding up of migrant workers during the pandemic. Journalists from Al Jazeera are also being investigated on a documentary covering these government raids and the poor treatment of the detained migrant workers in the immigration detention camps. Heidy Quah, an activist who highlighted the conditions in immigration detention through a Facebook post was also questioned by the police. Opposition politicians are also being harassed using these laws, with MP Hannah Yeoh being questioned over a tweet where she only asked about the status of the national road map to fight child marriage; and former youth and sports minister Syed Saddiq Abdul Rahman was questioned for his critical remarks about the PM and his government in an Al Jazeera interview.

The use of national security for surveillance also remains dangerous in two specific situations: (1) Using civilians to police the internet: In August 2019, the MCMC extended surveillance and policing of the internet beyond government agencies to civil society by setting up a WhatsApp hotline for the general public to submit screenshots of social media posts that harm race, religion and royalty; and (2) The absence of oversight when intercepting online communications in a national security situation: Using the 2012 Security Offenses (Special Measures) Act, a police officer who is above the rank of Superintendent may obstruct communication without getting permission from a public prosecutor if it is an emergency.

We condemn the restrictions on individuals' rights and freedoms by the government of Malaysia, and we call for the laws, policies and actions of the government as well as tech companies to protect civic space, to uphold online freedom and online privacy in line with international human rights law, and to allow for checks and balances of authorities.
The 1923 Official Secrets Act preventing collection or communication of information that harms the safety or interests of the State was the first problematic law in the country used to punish journalists. This is done using Section 3(2) of the law, which states that it is not necessary to show that the accused person was guilty of an act harmful to the State, and a person can be convicted if it seems that the purpose of the person's actions was to harm the safety or interests of the State. In February 2018, when Reuters journalists Wa Lone and Kyaw Soe Oo reported and published online human rights violations of the military in Rakhine state, they were arrested, charged and sentenced to seven years under this law. However, the journalists were released from prison in May 2019 following a Presidential pardon.

Section 33 of the 2004 Electronic Transactions Law also punishes as a crime, acts harmful to the security of the State or for receiving, sending and distributing information on state security secrets.

**TARGETING JOURNALISTS AND ACTIVISTS BY MISUSING THE LAW TO REGULATE TELECOM PROVIDERS AND NETWORKS**

The 2013 Telecommunications Law also undermines online freedom, privacy and access to information. While the goal of the law has been to protect telecom providers and users as well as to supervise the services, networks, facilities and equipment for peace, tranquillity and security; the use of this law by the Ministry of Transport and Communications (MOTC) has instead led to violation of rights and fear amongst people. Section 66(d) and 68(a) of this law are used by government authorities to target journalists and activists. Section 66(d) criminalises extortion, defamation, disturbing or threatening of anyone using a telecom network. Since 2013, more than 70 people have been charged with defamation under this provision. Further, Section 68(a) bans communication, receiving, sending or sharing of incorrect information dishonestly.

**MISUSE OF THE LAW FOR INTERNET SHUTDOWNS IN THE COUNTRY**

The Telecommunications Law was amended in 2017, but Section 77 still allows the MOTC to block internet and mobile services during an emergency. The language in this provision also allows the government to do this without any review by the court system. Accordingly, a year ago, the government imposed an internet shutdown in the conflict prone Rakhine and Chin states claiming it was necessary due to national security concerns. This has made it difficult to get information and ensure timely reporting of human rights violations committed against people living in conflict affected areas such as ethnic cleansing by the military. During the public health emergency brought on by COVID-19, the internet shutdown has blocked information about the disease and does not allow aid to reach people.

Currently, the country is in the unenviable position of having imposed the longest running internet shutdown. Additionally, in March 2020 under the Telecommunications Law, the MOTC ordered 2,147 websites to be taken down by internet providers. It was claimed that this step was necessary to prevent the spread of COVID-19 related misinformation, during the public health emergency. However, it was discovered that Voice of Myanmar, Narinjara News, Karen News, Mekong News and other websites of media outlets belonging to the Rakhine, Karen and Rohingya communities were taken down, further depriving these communities of their only source of information during the pandemic.

**OUR CALL TO ACTION**

We denounce the actions by the government of Myanmar to restrict the rights to online freedom, privacy and access to information of its netizens, journalists, and critics of the government or the military in violation of international human rights law, and call on them to ensure protection of these rights and accountability for human rights violations.
Internet freedom in Philippines has taken a sharp downturn with a political regime that operates the country with an iron fist, placing the law over people. Criticism against the government and its actions are not taken lightly, with threats and harassment issued verbally as well as through the law.

MISUSE OF THE CYBERSECURITY LAW TO VIOLATE ONLINE FREEDOM AND ONLINE PRIVACY

The most widely used law to censor online dissent, the 2012 Cybercrime Prevention Act was punishing online crimes under Articles 6 and 7, that the Revised Penal Code also punishes offline, however with heavier sentences. This law specifically will punish actions against computer systems and networks that harm security, which is explained as national and economic security. In 2015, a set of rules was developed to explain some powers under the law that relate to surveillance. Under this regulation, internet providers have to collect and retain data for up to six months on request.

WEAPONIZING THE TERM ‘FAKE NEWS’ DURING THE COVID-19 PANDEMIC

Between February and March 2020, Department Order No. 052 gave power to the National Bureau of Investigation (NBI), to investigate and prosecute COVID-19 related fake news shared online, even though there is no law in the country that defines what ‘fake news’ actually is. Article 154 of the Revised Penal Code on the unlawful use of publications has also been used to charge those arrested for spreading COVID-19 ‘fake news’ which is also prohibited by the Bayanihan to Heal One Act or the law which gives President Duterte emergency powers during the pandemic. Several people have been arrested, but most of the people charged are those who were critical of the government’s COVID-19 response or the President’s violent attitude towards those who do not follow lockdown measures.

MISUSE OF THE ANTI-TERRORISM LAW TO VIOLATE RIGHTS AND FREEDOMS

Modelled on the Anti-Terrorism Laws in Australia and France, the Anti-Terrorism Act of Philippines became law on 3 July 2020. The actions can be punished as terrorism are broad, with even just interference with a national security agencies online infrastructure also seen as a crime. The law has also been criticised for its long arrests and detention of suspects for 24 days without a warrant, extensive surveillance for 90 days through wire-tapping technology, and even impunity of officials under the law since all decisions under this law are made by a body of government officials called the Anti-Terror Council.

In these circumstances, it is believed that the law could be used to target government critics. To illustrate, in June 2020, critics of this law, particularly students were victims of an online disinformation campaign, with their Facebook accounts cloned and threats sent to them from the clone account leading to a rise in public panic.

THREATS FACED BY INDEPENDENT MEDIA IN THE COUNTRY

Threats also extend to those by private militia, hired by local politicians to silence journalists, without accountability. The government has also gone after independent media in the country, such as media houses, media persons and journalists that were critical of the government, using all means necessary. For instance, Rappler editor Maria Ressa and journalist Reynaldo Santos Jr. were tried and convicted for cyber-libel on a story accusing businessman Wilfred Keng of a connection to illegal drugs and human trafficking, as well as a link to a judge. The charges could be filed under the Article 4(c)(4) of the Cybercrime

\[ \text{OUR} \]
Prevention Act that became law in 2012 only after the story was published, only because a typo in the article was corrected in 2014. Their conviction is currently being appealed. Also, ABS-CBN, a long-time critic of the President, specifically of his violent anti-drug campaign was asked to cease their operations and has also been refused the renewal of their franchise license after years of the Congress not taking action on bills requesting their renewal.

**OUR CALL TO ACTION**

We urge the government of Philippines to stop its attacks on individual rights and freedoms, creating an environment of fear, and destroying civic space in the country, and appeal for a restoration of digital democracy, online freedom, and online privacy with independent checks and balances in place in line with international human rights law.

**SINGAPORE**

**OVERALL CONTEXT OF CIVIC SPACE IN SINGAPORE**

In Singapore, the People’s Action Party (PAP) has built the portrait of their country as one where economic success has been hard to achieve, it’s the most important thing, and something only the PAP and its leaders can give them. Using this view as a basis, PAP has closed all physical spaces for expressing any alternative view, dissent or even public discussion.

**MISUSE OF THE CYBERSECURITY LAW TO VIOLATE ONLINE PRIVACY**

The 2018 Cybersecurity Act of Singapore proves dangerous, with a cyber threat including national security threats. Also, owners of computer systems for essential services in relation to national security must allow officers to take or make copies of hard disks to assess threats.

**CENSORSHIP, INFORMATION TAKEDOWN AND CRIMINALISING INFORMATION IN THE NAME OF ‘NATIONAL SECURITY’ AND TO ‘MAINTAIN PUBLIC CONFIDENCE’ UNDER POFMA**

In October 2019, the Protection from Online Falsehoods and Manipulation Act (POFMA) was adopted into law to prevent publishing or sharing of information online that is false or misleading, without defining what a false or misleading statement is. Additionally, Section 7 specifically punishes publishing or sharing of false or misleading information online, which is harmful to the security of Singapore or any part of the country. It also punishes publishing or sharing any information online, which reduces confidence of the general public in the ability of the government, its authorities and bodies to perform their duty or function.

POFMA can be used to correct or remove false or misleading online content, under Sections 11 and 12. POFMA also covers private chat groups and social media groups, which could undermine the online privacy of persons in a country where there is no law protecting it. In serious cases, internet service providers and social media platforms may be ordered to block access to websites or content, and the platform where the information is shared is declared as an ‘online location’. However, the powers under this law can only be used by government ministers or by bureaucrats during the election. POFMA cannot be used if information shared by government officials online is false or misleading, instead individuals will have to file a case under the 2014 Defamation Act or under Section 499 and 500 of the Penal Code. Compliance with an order under POFMA is compulsory, but it can be appealed against before the High Court. Unfortunately, these appeals are expensive and the burden to prove that
POFMA is not meant to cover opinions, criticism, satire or parody, but whether information shared online is a fact or not is decided by government authorities based on what they believe a reasonable person will think. Therefore, information covered by POFMA is not always a fact, as can be seen from the cases brought against online opinions and online criticisms against the government or its policies. Using POFMA, the law can also punish internet service providers and others allowing for the false or misleading information to be shared.

**MISUSE OF POFMA DURING THE COVID-19 PANDEMIC**

Actions taken under POFMA have not slowed down during COVID-19 leading to self-censorship, blocking of independent media and other independent sources of information. Between October 2019 and July 2020, there have been more than 70 separate POFMA orders. Several types of POFMA orders were passed, including: (1) a POFMA order issued against a video shared by New Naratif and its founder, historian Thum Ping Tjin claiming that POFMA did not allow any criticism of the government; (2) 6 POFMA orders were issued against Alex Tan and Facebook pages he manages for his criticism of POFMA as well as the government response to COVID-19; and (3) 4 POFMA orders issued on estimates of the salary of the Prime Minister's wife. Orders have also been sent to Facebook to block access in Singapore to pages that do not comply with a POFMA order, such as in the case of Alex Tan.

**OUR CALL TO ACTION**

We condemn these attempts to restrict civic space and individual freedoms, by labelling all information critical of the government and its policies as false or misleading and forcing tech companies to assist them in censoring information. We call for the government of Singapore to protect the online freedom and online privacy of netizens, ensure independent oversight for their actions, and allow for tech companies to respect individual rights in accordance with the UN Guiding Principles on Business and Human Rights.

**THAILAND**

**OVERALL CONTEXT OF CIVIC SPACE IN THAILAND**

In Thailand, 'national security' has been used to justify the restriction of online information and to encourage self-censorship, in relation to critical opinions on the monarchy and the government. The earliest provision targeting critics of the monarchy was Article 112 of the Criminal Code. The Thai government has even claimed its harsh penalties are necessary for national security and public order, without clarifying how the law protects these aspects. Although arresting and charging critics of the monarchy under this lèse-majesté provision has reduced, action is now being taken against them using the Computer-related Crimes Act (CCA)

**MISUSE OF THE CYBERCRIME LAW TO RESTRICT AND PUNISH ONLINE EXPRESSION CRITICAL OF THE GOVERNMENT OR MONARCHY, CONTINUING DURING THE COVID-19 PANDEMIC**

CCA regulates the internet, to prevent information which would damage national security, public safety or cause public panic. Section 14 (2) of this law criminalizes the entering of false computer data into a computer system which will harm national
security, public safety, or cause panic to the general public and is used to punish all online criticism against the monarchy and government policies. Starting in November 2019, an Anti-Fake News Centre was set up to investigate and take action against false and misleading information, particularly under Sections 14(2) and (3) of the CCA. Under Section 26, the government also has the power to order internet service providers, to retain user data for at least 90 days.

With this system in place to criminalise online expression, there has been an increase in action against pro-democracy activists, HRDs, as well as critics of the monarchy or government, particularly against student activists and continuing during the COVID-19 pandemic. For instance, 25-year old activist, Karn Pongphrapan was arrested and charged under CCA in October 2019, for sharing on Facebook a post highlighting the violent endings that foreign kings faced. Although he deleted the post, he still faces a trial but is out on bail. Additionally, a Twitter user called ‘Niranam’ was arrested in February 2020 for sharing pictures and messages on the King. He faces 8 charges under the CCA and has finally been let out on bail, after being denied twice. If convicted, they could face 5 years for each charge against them.

Critics of the government’s COVID-19 response and netizens sharing information on the COVID-19 were also arrested under Section 14(2) of the CCA. To illustrate, a Thai artist, Danai Ussama was charged for his criticism of the COVID-19 screening process at Suvarnabhumi airport in March 2020. In another example, the administrator of an investigative Facebook page, Queen of Spades is under investigation for pointing out the corruption around a mask hoarding scandal which also implicated Sonthiya Sawasdi from the Palang Pracharath Party.

**ABUSE OF THE CYBERSECURITY LAW TO PROTECT A BROADLY DEFINED ‘NATIONAL SECURITY’**

Another problematic law, the 2019 Cybersecurity Act of Thailand is meant to protect national security, but also economic security, military security and public order, without defining any of these terms. Thus, the excessive powers granted to the bodies made up of government officials as a majority could be misused to collect information in the case of a threat, and then used against government critics and that too without proper scrutiny of the court.

**VIOLATIONS OF RIGHTS IN CYBERSPACE FOR THOSE IN THE SOUTH OF THAILAND**

In the conflict prone South of Thailand, several steps have been taken in the name of national security. First, the 2019 National Intelligence Act allows the National Intelligence Agency to get information from an individual if it impacts national security, and to use any means to get the information if not provided. Second, the collection of biometric data and re-registration of SIM cards was ordered, with phones disconnected in April 2020 amid COVID-19 if they did not do so. This is dangerous since the data could be used with 8,200 CCTV cameras equipped with AI technology in the region.

**OUR CALL TO ACTION**

We condemn the collective efforts by the government to punish online expression and violate online privacy to protect the interests of the government and the monarchy, while forcing internet providers and tech companies to assist them in these violations. We call for a restoration of internet democracy, with the online freedom and online privacy of all individuals protected and respected, in line with the international human rights obligations of the country.
OVERALL CONTEXT OF CIVIC SPACE IN VIETNAM

With the jailing of dozens of activists and journalists amid a crackdown on online dissent, the internet in Vietnam is under the complete control for the benefit of government authorities. As a one party state, all actions taken are in protection and promotion of the interests of the Communist Party of Vietnam.

CRIMINALISING ONLINE CRITICISM OF THE GOVERNMENT OR THE COMMUNIST PARTY OF VIETNAM

Article 117 of the 2015 Criminal Code has been used to target information that is critical of the State, particularly through Facebook. According to these provisions, developing, storing or sharing distorted information about the government to oppose it can be punished with 5 to 12 years in prison. Between June and December 2019, at least 15 activists were charged under these provisions, tried by the court, punished, and imprisoned for sharing information on social media that was critical of the Communist Party of Vietnam or of the government’s policies. One such case is that of pro-democracy activist, Nguyen Ngoc Anh who was sentenced to six years in prison in November 2019 for reporting on a toxic waste spill, writing about issues around the election and for discussing political prisoners through his Facebook account. Other regularly used provisions include Article 118 which bars disrupting national security and Article 331 which does not allow the abuse of democratic freedoms to violate state interest.

CONTROL OF THE INTERNET USING STATE POLICY

Another harmful regulation is Decree No. 72 on the Management, Provision, Use of Internet Services and Internet Content Online of 2013, which specifically bans online information that opposes the State and undermines national security under Article 5. This policy does not allow bloggers and social media users to quote, gather and summarise information from the press or government websites. It forces internet providers and platforms to regulate third parties and to work with the government take down content.

MISUSE OF THE CYBERSECURITY LAW TO PROTECT STATE INTERESTS WITH THE COMPLICITY OF TECH COMPANIES

Developed from Decree No. 72, the Law on Cybersecurity (LOCS) came into effect in 2019. This law defines cybersecurity as including national security, with provisions protecting the Communist Party and to keep it in power. To illustrate, Article 4(2) specifically states that it is applied not by the State, but instead by the Communist Party of Vietnam, for the continuance of the same government and to strengthen the political system. Articles 8 and 15 do not allow developing, posting or sharing information that is propaganda against the state, defames the government, or distorts security amongst other aspects, with Article 26 specifically banning websites, web pages or social media pages from posting or sharing information that harms national sovereignty and security. Online information has to be stored by service providers and internet companies in servers located in Vietnam, with user information handed over to the government when it requests for the same leading to online privacy concerns.

The LOCS also requires service providers and internet companies to take down content within 24 hours after government authorities ask them to. Although Facebook resisted earlier requests by the government to take down anti-government content that violates the LOCS, at the beginning of this year, Facebook finally gave into pressure when its servers were taken offline by...
the government till the company agreed to comply contributing to state censorship. This is particularly worrying since this is at a time when people rely more on the internet during the COVID-19 pandemic.

RESTRICTION OF RIGHTS DURING THE COVID-19 PANDEMIC

The Department of Information and Communications investigated more than 650 people and fined more than 160 people, of which 3 were celebrities for COVID-19 related information shared online which they were also forced to delete. In addition, 47 bloggers, activists and journalists were arrested for online information and placed in pre-trial detention in 2020, even with the public health risk they could face.

OUR CALL TO ACTION

We call on the government of Vietnam to refrain from misusing anti-democratic laws and policies to create self-censorship, punish legitimate online expression, while forcing tech companies and service providers to assist them in these violations. We urge them to protect online freedom and online privacy of all, particularly critical voices, in accordance with international human rights law and in order for the country to be a real democracy.

ADDITIONAL READINGS

CAMBODIA


INDONESIA


LAO PDR

• UPR factsheet on civic space to support the 3rd Cycle of the Universal Periodic Review, Manushya Foundation, January 2020, available at: https://bit.ly/2CHUr6N

• Joint Submission to the UN Universal Periodic Review (UPR) for Lao PDR on civic space, Manushya Foundation, 18 July 2019, available at: https://www.manushyafoundation.org/joint-lao-upr-submission

MALAYSIA


• The real news of Malaysia’s ‘fake news’ law, Asia Times, 17 April 2018, available at: https://asiatimes.com/2018/04/real-news-malaysias-fake-news-law/


MYANMAR


• Scorecard assessing Freedom of Expression in Myanmar, PEN Myanmar, 3 May 2017, available at: https://en.penmyanmar.org/2017/05/03/hello-world/
PHILIPPINES

- Spotlight on 2 Anti-Democratic laws passed in Hong Kong and the Philippines in the name of ‘national security’, Manushya Foundation, 17 July 2020, available at: https://www.facebook.com/ManushyaFdn/posts/269626897322910

SINGAPORE

- Singapore’s online falsehoods bill will deepen a culture of self-censorship, New Mandala, 26 April 2019, available at: https://www.newmandala.org/singapores-online-falsehoods-bill-will-deepen-a-culture-of-self-censorship/

THAILAND

- Thailand’s Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats, Manushya Foundation, September 2019, available at: https://www.manushyafoundation.org/study-on-cybersecurity-act

VIETNAM