JUSTIFYING DIGITAL REPRESSION VIA "FIGHTING FAKE NEWS"

A Study of Four Southeast Asian Autocracies

Janjira Sombatpoonsiri and
Dien Nguyen An Luong

TRENDS IN SOUTHEAST ASIA

The **ISEAS – Yusof Ishak Institute** (formerly Institute of Southeast Asian Studies) is an autonomous organization established in 1968. It is a regional centre dedicated to the study of socio-political, security, and economic trends and developments in Southeast Asia and its wider geostrategic and economic environment. The Institute's research programmes are grouped under Regional Economic Studies (RES), Regional Strategic and Political Studies (RSPS), and Regional Social and Cultural Studies (RSCS). The Institute is also home to the ASEAN Studies Centre (ASC), the Singapore APEC Study Centre and the Temasek History Research Centre (THRC).

ISEAS Publishing, an established academic press, has issued more than 2,000 books and journals. It is the largest scholarly publisher of research about Southeast Asia from within the region. ISEAS Publishing works with many other academic and trade publishers and distributors to disseminate important research and analyses from and about Southeast Asia to the rest of the world.

JUSTIFYING DIGITAL REPRESSION VIA "FIGHTING FAKE NEWS"

A Study of Four Southeast Asian Autocracies

Janjira Sombatpoonsiri and Dien Nguyen An Luong

ISEAS YUSOF ISHAK INSTITUTE

FOREWORD

The economic, political, strategic and cultural dynamism in Southeast Asia has gained added relevance in recent years with the spectacular rise of giant economies in East and South Asia. This has drawn greater attention to the region and to the enhanced role it now plays in international relations and global economics.

The sustained effort made by Southeast Asian nations since 1967 towards a peaceful and gradual integration of their economies has had indubitable success, and perhaps as a consequence of this, most of these countries are undergoing deep political and social changes domestically and are constructing innovative solutions to meet new international challenges. Big Power tensions continue to be played out in the neighbourhood despite the tradition of neutrality exercised by the Association of Southeast Asian Nations (ASEAN).

The **Trends in Southeast Asia** series acts as a platform for serious analyses by selected authors who are experts in their fields. It is aimed at encouraging policymakers and scholars to contemplate the diversity and dynamism of this exciting region.

THE EDITORS

Series Chairman:
 Choi Shing Kwok

Series Editor:
 Ooi Kee Beng

Editorial Committee:
 Daljit Singh
 Francis E. Hutchinson
 Norshahril Saat

Justifying Digital Repression via "Fighting Fake News": A Study of Four Southeast Asian Autocracies

By Janjira Sombatpoonsiri and Dien Nguyen An Luong

EXECUTIVE SUMMARY

- Southeast Asian autocracies of Cambodia, Myanmar, Thailand and Vietnam have politicized vague definitions of "fake news" to justify diverse tactics of digital repression.
- In these countries, what constitutes falseness in "fake news" has hardly been clearly articulated. The governments instead focus on the grave threats the dissemination of "fake news" could pose to national security, public disorder, or national prestige.
- As the governments are vested with the power to bend the labelling of "fake news" to their will, they can criminalize those accused of circulating such information to safeguard public interests.
- There are at least four methods by which the governments have tightened the screws on cyberspace under the banner of curbing "fake news": (i) prosecute Internet users, journalists and dissidents in particular; (ii) pressure Internet Service Providers and social media platforms to block and remove content; (iii) expand and deepen social media monitoring; and (iv) shut down the Internet altogether.
- All four countries have used "fake news" allegations to penalize critics. Cambodia, Thailand and Vietnam are inclined to use such allegations to strong-arm tech companies into removing content at the behest of the governments. Thailand and Vietnam tend to exploit such allegations to beef up online surveillance. Myanmar is the only country that turns to Internet shutdowns.

- The interplay between the methods of digital repression that exploit the pretext of cracking down on "fake news" and the manipulation of online discourse through the deployment of cyber troops would merit further research and in-depth examination.

Justifying Digital Repression via "Fighting Fake News": A Study of Four Southeast Asian Autocracies

By Janjira Sombatpoonsiri and Dien Nguyen An Luong[1]

INTRODUCTION

In mainland Southeast Asia, the governments of Cambodia, Myanmar, Thailand and Vietnam have been using the pretext of curbing "fake news" to control digital space. The phenomenon of "fake news" gained international traction in light of, among other things, the 2016 US elections and Brexit, in which false online information contributed to the rise of hate speech and extremism, political divides and the eroding of democracy.[2] While these concerns are legitimate and have led to the implementation of various regulatory measures and content moderation

---

[1] Janjira Sombatpoonsiri is Visiting Fellow in the Media, Technology and Society Programme at the ISEAS – Yusof Ishak Institute, Singapore and Assistant Professor and Project Leader at the Institute of Asian Studies, Chulalongkorn University, Thailand; Dien Nguyen An Luong is Visiting Fellow in the Media, Technology and Society Programme at the ISEAS – Yusof Ishak Institute, Singapore.

[2] See, for instance, Joshua A. Tucker, Andrew Guess, Pablo Barbera, Cristian Vaccari, Alexandra Siegel, Sergey Saovich, Denish Stukal and Brendan Nyhan, "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature", Hewlett Foundation, March 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144139; Samantha Walther and Andrew McCoy, "US Extremism on Telegram: Fueling Disinformation, Conspiracy Theories, and Accelerationism", *Perspective on Terrorism* 15, no. 2 (2021): 100–24; V-Dem Institute, "Pandemic Backsliding: Democracy and Disinformation. Seven Months into the Covid-19 Pandemic", *Policy Briefing* No. 25, 2 October 2020, https://www.v-dem.net/media/publications/v-dem_policybrief-25_201002_v2.pdf

policies,[3] political leaders, especially autocratic ones, have found it useful to make policy responses to "fake news" as a means to stifle critics.[4] This weaponizing of "fake news" allegations has served to tighten the regimes' grip on information to the detriment of a healthy information environment.[5]

In this article, we show how the regimes in Cambodia, Myanmar, Thailand and Vietnam have used vague definitions of "fake news" to justify diverse practices to suppress digital space. We focus on these four countries because their regime types are characteristically autocratic and have a propensity to intensify digital repression. According to the Varieties of Democracy Institute (V-Dem), Cambodia is an electoral autocracy, while Myanmar, Thailand and Vietnam are identified as closed autocracies.[6] Civil liberties in these four countries are severely constricted, all ranked by Freedom House as "not free".[7] As we shall see, these autocracies have employed diverse methods to narrow digital

[3] See, for instance, Marina Adami, "From Elon Musk to Brussels: Three Leading Experts on the Future of Free Speech Online", *Reuter Institute*, 17 May 2022, https://reutersinstitute.politics.ox.ac.uk/news/musk-brussels-three-leading-experts-future-free-speech-online

[4] Andrew S. Ross and Damian J. Rivers, "Discursive Deflection: Accusation of 'Fake News' and the Spread of Mis- and Disinformation in the Tweets of President Trump". *Social Media+ Society* 4, no. 2 (2018), https://doi.org/10.1177/2056305118776010; Kate Farhall et al., "Political Elites' Use of Fake News Discourse across Communication Platforms", *International Journal of Communication* 13 (2019): 4353–75; Jana Laura Egelhofer and Sophie Lecheler, "Fake News as a Two-Dimensional Phenomenon: A Framework and Research Agenda", *Annals of the International Communication Association* 43, no. 2 (2019): 97–116.

[5] Anna Lührmann and Staffan I. Lindberg, "A Third-Wave Autocratization Is Here: What Is New About It", *Democratization* 26, no. 7 (2019): 1095–113.

[6] V-Dem, *Autocratization Changing Nature?*, 2022, https://v-dem.net/media/publications/dr_2022.pdf

[7] Freedom House, "Freedom in the World 2022: Global Expansion of Authoritarian Rule", February 2022, https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

space. We highlight the governments' increasing use of a "fake news" label to foster four main repressive tactics: legal persecution of users and platforms, content restriction, surveillance, and Internet shutdowns. Across the four autocracies studied, we observed at least four methods in which governments rely on the claim to curtail "fake news" to justify digital repression. First, in all four cases, the government uses the "fake news" claim to charge in court Internet users who have been critics of the regimes. Second, at least in Cambodia, Thailand and Vietnam, the "fake news" threat provides a pretext for compelling Internet Service Providers (ISPs) and social media platforms to block and take down content unfavourable to these governments. Third, in Thailand and Vietnam, the "fake news" claim has fostered extensive surveillance of social media posts and systematic collection of user data. Lastly, Myanmar under the State Administration Council that seized power in 2021 exemplifies how Internet shutdowns can be justified based on tackling "fake news."

In what follows, we first outline definitions of "fake news" enshrined in key legal documents related to countering disinformation in Cambodia, Myanmar, Vietnam and Thailand. The aim is to derive common characteristics subjecting the term "fake news" to politicization. In the second section, we show four patterns in which the anti-fake news rhetoric has been used to support digital repression across these countries. In the last section, we highlight the need for further investigation into what drives these different patterns and how tactics to suppress digital space interact with the other side of the coin: government-backed information manipulation campaigns.

POLITICIZATION AND WEAPONIZATION

By intersecting the study on policy responses to disinformation with digital repression, our article combines two frameworks extracted from these burgeoning fields: politicization and weaponization. We apply the concept of politicization when considering definitions of "fake news" enshrined in legal documents to tackle disinformation. The politicization of "fake news" regards ways in which governments define "fake news" as false information but are vague about what constitutes what is false and what is true. Instead, these governments highlight the dire consequences

of spreading "fake news", ranging from public disorder and national insecurity to damaged national image. These two components—vaguely articulated compositions of false content and the projection of horrendous consequences of endemic "fake news"—endow governments with the power to (1) subjectively flag content unfavourable to them as untrue; and (2) criminalize those accused of spreading "dangerous fake news".[8]

Politicizing "fake news" encompasses the infrastructural control of information flow and the penalization of online critics.[9] In this regard, we apply the concept of weaponization to denote how governments instrumentalize the label of "dangerous fake news"—in many cases in conjunction with other claims related to security and political stability—to justify various draconian measures. In so doing, governments can legitimately persecute "fake news" purveyors; deepen systems to filter supposedly false content while facilitated by around-the-clock content monitoring; and even shut down the Internet.

We study the nexus of politicizing and weaponizing the "fake news" claim in the context of autocratic regimes mainly because autocracies' survival is tied to the ability to contain political challengers. As such, autocracies often resort to suppressing digital space and curbing threatening dissent.[10] According to 2019 Digital Society Project data, the most oft-used forms of digital repression in Cambodia and Vietnam include Internet filtering and persecution of online users respectively, while in Thailand, social media monitoring has been the most common tactic. Also, Myanmar seems to be the only one among its autocratic

---

[8] See Ric Neo, "When Would a State Crack Down on Fake News? Explaining Variation in the Governance of Fake News in Asia-Pacific", *Political Studies* (2021), https://journals.sagepub.com/doi/10.1177/14789299211013984; John Brummette, Marcia DiStaso, Michail Vafeiadis and Marcus Messner, "Read All About It: The Politicization of 'Fake News' on Twitter", *Journalism & Mass Communication Quarterly* 95, no. 2 (2018): 497–517.

[9] Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford: Oxford University Press, 2021), p. 25.

[10] Ibid., p. 26. We also acknowledge that cooptation is also an autocratic tool to deal with political opponents.

counterparts most frequently relying on Internet shutdowns (Figure 1).[11] As we shall see, our analysis that couples these digital repression toolkits with "fake news" justification shows the persistence of these trends.

LEGAL DEFINITIONS OF "FAKE NEWS"

In the four countries analysed, definitions of false and true news are often vague, while its detrimental consequences are linked with, among others, national security, political stability and national reputation. A good place to observe this pattern is the legal texts that the authorities in Cambodia, Myanmar, Thailand and Vietnam often cite when dealing with "fake news". Many legal measures shown below were enforced between 2007 and 2020. They mainly target Internet users, telecommunication companies, and increasingly intermediaries as well, i.e., social media platforms, alleged for being involved in posting, sharing, allowing or hosting "fake news". See Table 1.

Cambodia

The Cambodian People's Party (CPP)-led government has relied on at least two sets of legal measures to supposedly curtail false information, a trend that has been common since the 2013 election in which the CPP nearly lost to the opposition Cambodia's National Rescue Party (CNRP). The first set regards various criminal codes, including Article 425, which penalizes those "communicating or disclosing false information with the intention to create an impression that destructs, deteriorates or damages persons" with a US$900 fine and imprisonment of up to two years. In

---

[11] Based on the Digital Society Project's codebook, the point estimates are the median values of these distributions for each country per year. The scale of the measurement model variable is typically between –5 and 5, with 0 approximately representing the mean for all country-years in the sample. Therefore, a country showing a negative score means that it is performing below the mean for that particular variable, interpreted in this context as less repressive than countries displaying positive scores.

Figure 1: Digital Repression Scores in Cambodia, Myanmar, Thailand and Vietnam
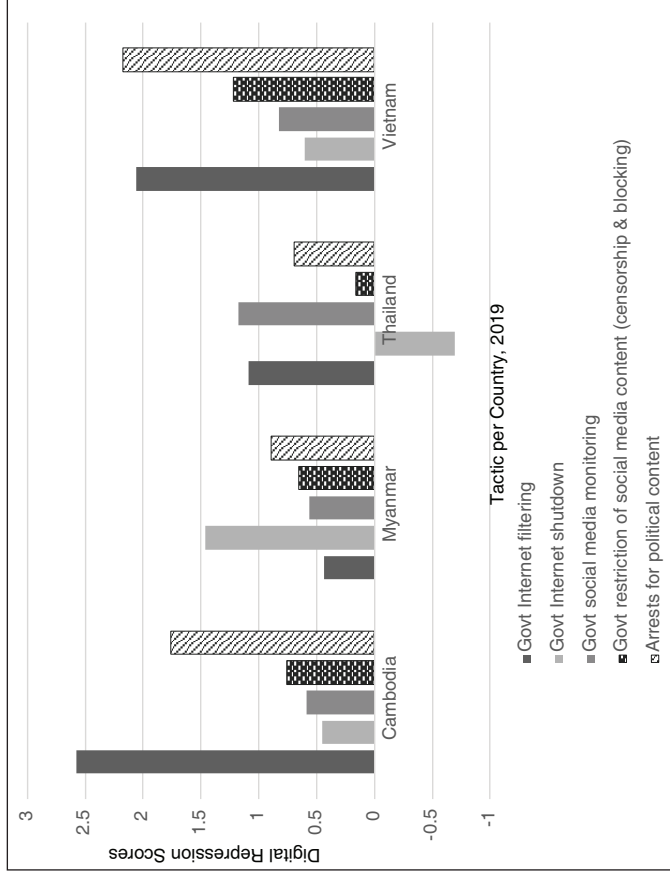
Table 1: List of Legal Measures Used to Charge Purveyors of "Fake News"

Country	Legal Measures	Year of Enforcement
Cambodia	Criminal Codes, Article 425, 453, 494 and 495	2011
	Inter-Ministerial "Prakas" on Publication Controls of Website and Social Media Processing via Internet	2018 (May)
	Cyber crime law (draft)	—
Myanmar	Penal Code	1861
	Electronic Transactions Law	2004, amended in 2021
	Telecommunications Law	2013
Thailand	Criminal Code, Article 112 *lèse majesté*	1957
	Criminal Code, Sections 326 to 328 on defamation	1992
	Computer-Related Crimes Act	2007, amended in 2016
	Anti-fake news regulation (added to the CCA)	2022
Vietnam	Penal Code, Articles 88, 117 and 331	1985, amended in 1999 and 2015
	Decree 72	2013
	Cyber Security Law	2018
	Decree 15/2020/ND-CP	2020

Source: Authors' elaboration.

addition, criminal code Articles 453, 494 and 495 impose additional sentences on violators who post false online content considered as a felony and public incitement.[12] The second set of measures is the May 2018 Inter-Ministerial "Prakas" or Announcement on Publication Controls of Website and Social Media Processing via Internet, and related directives. The laws punish publishers of content considered "unfit" and false content with a two-year jail sentence and fines of up to US$1,000.[13] In 2020, the Ministry of Information announced that it was drafting the "Fake News Law", which was however scrapped later that year. In 2021, the cybercrime law was drafted, imposing criminal liability for the "provision of disinformation".

While these laws are unclear about what "fake news" actually entails and whether government-backed online propaganda is considered a constitutive part of it, they attribute the spread of "fake news" to the occurrence of all things dangerous. These include harms to: (1) national security; (2) public health, safety and finances; (3) diplomatic relations between Cambodia and other countries; (4) the outcome of a national election; (5) social cohesion; (6) public confidence in the government and state institutions.[14] Simply put, online criticisms of the government and questioning an electoral result can be cast as illegally false. In early

---

[12] Asia Centre, "Defending Freedom of Expression: Fake News Laws in East and Southeast Asia", 2020, https://asiacentre.org/wp-content/uploads/Defending_ Freedom_of_Expression_Fake_News_Laws_in_East_and_Southeast_Asia.pdf, p. 24.

[13] Cambodian Centre for Human Rights, "Submission to the Special Rapporteur on the Promotion and Protection of Rights to Freedom of Opinion and Expression", June 2021, https://www.ohchr.org/sites/default/files/Documents/ Issues/Expression/disinformation/2-Civil-society-organisations/Cambodia-Centre-for-human-rights.pdf

[14] Kingdom of Cambodia, "Inter-Ministerial 'Prakas' or Announcement on Publication Controls of Website and Social Media Processing via Internet", 28 May 2018; Cambodian Centre for Human Rights, "Submission to the Special Rapporteur on the Promotion and Protection of Rights to Freedom of Opinion and Expression."

March 2020, Prime Minister Hun Sen compared individuals spreading "fake news" with terrorists.[15]

Myanmar

Overall, Myanmar has largely relied on its previously enacted laws and amended them to crack down on what is deemed "false" or "fake" news. These laws include the Penal Code, the 2004 Electronic Transactions Law, and the 2013 Telecommunications Law. Article 68 of the Telecommunications Law criminalizes "communication, reception, sending, distribution, or sharing of incorrect information with dishonest intention".[16] Under the Telecommunications Law, violators could face fines, imprisonment of up to one year or both. The law has been used as a primary framework for licensing mobile and Internet Service Providers, giving the authorities *carte blanche* to temporarily block and remove content on behalf of the people. In the wake of the 2021 coup, the State Administration Council amended the Electronic Transactions Law, a section of which envisages criminalizing the dissemination of "fake news or disinformation" online with jail terms of up to three years.[17] The coup also provided a pretext for the Myanmar junta to amend the 1861 Penal Code on 14 February 2021. Under the amendments, Section 505A was added to outlaw the dissemination of "false news", with violators subject to a fine, a jail term of up to three years, or both.[18]

---

[15] Cambodian Centre for Human Rights, "Submission to the Special Rapporteur on the Promotion and Protection of Rights to Freedom of Opinion and Expression".

[16] Other problematic provisions in the Telecommunications Law (2013) include Articles 4, 5–8, 18, 40, 68, and 75–77. See "Telecommunications Law", *Free Expression Myanmar*, 8 October 2013, https://freeexpressionmyanmar.org/wp-content/uploads/2017/07/telecommunications-law-en.pdf

[17] "Amended Law Throws Myanmar Back into Media Dark Age", *Myanmar Now,* 19 February 2021, https://www.myanmar-now.org/en/news/amended-law-throws-myanmar-back-into-media-dark-age

[18] "Republic of the Union of Myanmar State Administration Council State Administration Council Law No. (5/2021) Law Amending the Penal Code". *Global New Light of Myanmar*, 15 February 2021, https://cdn.myanmarseo.com/file/client-cdn/gnlm/wp-content/uploads/2021/02/15_Feb_21_gnlm_1.pdf

All those laws contain vaguely worded provisions that do not clearly articulate what merits false content. "Fake" or "false" news is instead defined in terms of its detrimental consequences. According to the amended Electronic Transactions Law, "false" or "fake" news is information that poses a grave threat to national security, "disrupts" the military or defames government officials, and could potentially sabotage foreign relations.[19] Under the same amended law, "fake news" is also defined as information that could also cause fear or alarm to the public or "destroy public trust".[20]

Thailand

The key to curtailing online "fake news" in Thailand is the Computer-Related Crimes Act (CCA), which was enforced in 2007 and amended in 2016. With its original aim to tackle online scams and pornography, the CCA primarily penalizes those importing into a computer system "forged or false computer data".[21] Especially Articles 14(1) and 14(2) directly target "fake news" deemed to deceive others and convey malicious intention against individuals or the public at large. In 2022, the Cabinet passed anti-fake news regulations under the CCA that empower ministerial and provincial authorities to take down false content and file complaints against those circulating it.[22] In addition, the Criminal Code, Sections 326 to 328 on defamation can be cited against purveyors of online "fake news" that damages the reputation of an individual or a public entity. Meanwhile, Article 112 of the Criminal Code on *lèse majesté* deals with (online and offline) false and defamatory information

---

[19] "Myanmar's New Electronic Transactions Law Amendment", *Free Expression Myanmar*, 18 February 2021, https://freeexpressionmyanmar.org/myanmars-new-electronic-transactions-law-amendment/

[20] Ibid.

[21] Computer-Related Crimes Act, B.E. 2550 (2007), *Royal Gazette* no. 124, sect. 27 *kor*, 18 June 2007, p. 4.

[22] "(Amended) Computer-Related Crimes Act B.E. 2560 (2016)", *Royal Gazette* no. 134, sect. 10 *kor*, 24 January 2016, p. 24.

regarding the monarchy. The CCA- and defamation-related sentences may be considered mild, with between one and five years of imprisonment and THB20,000 to THB200,000 fines (around US$600 to US$3,000). However, violating Article 112 is a serious crime, leading to a maximum fifteen-year jail sentence.[23]

Based on the CCA and its related regulations, "fake news" denotes the information that appears on social media platforms or in a computer system, and that is entirely or partially false. As with the three other cases, what constitutes falseness is unclear. Instead, "fake news" is identified in terms of its consequences such as causing public panic, undermining public safety, the economy and public infrastructure,[24] instigating national disunity, and damaging the country's reputation, traditions, and key institutions.[25] These definitions coincide with security policies that consider "fake news" to threaten national security and distort public perceptions about the monarchy.[26] Social media posts against the monarchy can lead to severe sentences related to cyber terrorism.[27]

[23] Janjira Sombatpoonsiri, "Securitizing Fake News: Policy Responses to Disinformation in Thailand", in *From Grassroots Activism to Disinformation: Social Media in Southeast Asia*, edited by Aim Sinpeng and Ross Tapsell (Singapore: ISEAS – Yusof Ishak Institute, 2020), p. 117.

[24] "(Amended) Computer-Related Crimes Act B.E. 2560 (2016)", *Royal Gazette* no. 134, sect. 10 *kor*, 24 January 2016.

[25] "ประกาศกระทรวงดิจิตัลเพื่อเศรษฐกิจและสังคม เรื่องหลักเกณฑ์การเก็บรักษาข้อมูล จราจรทางคอมพิวเตอร์ของผู้ให้บริการ" [Announcement of Digital Economic and Society Ministry on regulations of service providers' storage of traffic data], *Royal Gazette* no. 138 special sect. 188 *gnor*, 13 August 2021, www.ratchakitcha. soc.go.th/DATA/PDF/2564/E/188/T_0009.PDF

[26] National Security Council, "National Security Policy, 2015–2021", http:// www.nsc.go.th/Download1/policy58.pdf; Internal Security Operations Command (ISOC), "ISOC Strategy, B.E. 2555–2559 (A.D. 2012–2016), http:// www.isocthai.go.th/GorPorRor/4YearsPlan(2555-2558)Completed.pdf; Internal Security Operations Command (ISOC), "ISOC Strategy, B.E. 2560–2564 (A.D. 2017–2021)", https://www.isoc.go.th/wp-content/uploads/2018/01/ strategy2560-2564.pdf

[27] iLaw, "พ.ร.บ.คอมพิวเตอร์ฯ มาตรา 14(3) เวอร์ชันใหม่ความผิดหมิ่นกษัตริย์ฯ แทนที ม. 112" [Computer-related Crimes Act Article 14(3): New Version Tackling Royal Offence in Place of Article 112], 21 February 2020, https://freedom.ilaw. or.th/en/node/793

Vietnam

Vietnam has utilized a raft of Internet regulations, the Penal Code and other laws to clamp down on what the authorities perceive to be "wrong" or "distorted" views, "toxic content" and "fake news". When it comes to Internet regulations, Decree 72, which was enacted in 2013, and the 2018 Cybersecurity Law are applied to pressure tech companies for content restriction (further discussed in the following section). But at times, Decree 72 can be slapped on local media outlets accused of hosting false information on their websites. In addition, against the backdrop of the pandemic, the government enforced Decree 15 in February 2020, which aims to, among other things, criminalize the creation and dissemination of false and misleading information. Violations of Decree 15 could lead to fines ranging from VND10 million to VND20 million (US$432 to US$865).[28] Besides Internet regulations, the Penal Code's Articles 88 and 117 have also been invoked frequently to charge bloggers, journalists and online activists with spreading false news about the Vietnamese state. The jail terms range from five to twenty years.

Similar to the other three countries, the notion of false content has never been clarified in Vietnam's regulatory framework. At the outset of the arrival of the Internet in Vietnam in 1997, the authorities broadly characterized fake news as "toxic content" that entailed false ads for contraband merchandise, state secrets or anti-state content. This connotation has, however, been narrowed down and shifted over the years. As analysed above, "fake news" has been chiefly associated with anti-state content, one that "opposes the Socialist Republic of Vietnam" or "threatens the national security, social order, and safety".[29] In the wake of COVID-19, "fake news" has also been defined as information that

---

[28] "Decree 15/2020/NĐ-CP", Thu vien Phap Luat, 15 April 2020, https://luatvietnam.vn/khoa-hoc/nghi-dinh-15-2020-nd-cp-xu-phat-vi-pham-hanh-chinh-linh-vuc-buu-chinh-vien-thong-180259-d1.html

[29] Mong Palatino, "Decree 72: Vietnam's Confusing Internet Law", *The Diplomat*, 8 August 2013, https://thediplomat.com/2013/08/decree-72-vietnams-confusinginternet-law

could cause fear or alarm to the public or go against the benefits of the country and its people.

In these four autocracies, the meaning of "fake news" is stretched from its initial connotation of merely false information to dangerously untrue information that threatens national pillars. This rhetorical transformation endows governments and security apparatuses with the power to determine any facts inconvenient for them as false information, and criminalize those circulating them in the name of defending the public. This politics of interpretation sets the stage for power holders—be it the ruling parties in Cambodia and Vietnam, the military and monarchy in Thailand, or the incumbent junta in Myanmar—to justify a wide range of policies under the presumption of curtailing "fake news".

HOW TACKLING "FAKE NEWS" IS USED TO SUPPRESS DIGITAL SPACE

There are at least four patterns in which the claim to combat "fake news" gives governments a pretext to tighten control over digital space: (i) persecute Internet users; (ii) pressure ISPs and social media platforms to block and remove content; (iii) expand and deepen social media monitoring; and (iv) shut down the Internet altogether. These patterns vary across different countries.

Legal Persecution of Internet Users: Cambodia, Myanmar, Thailand and Vietnam

In line with a global trend of governments charging dissidents and journalists with "fake news" allegations,[30] the authorities in Cambodia, Myanmar, Thailand and Vietnam have charged Internet users for

---

[30] Neo, "When Would a State Crack Down on Fake News?"; Caroline Lees, "Fake News: The Global Silencer", *Index on Censorship* 47, no. 1 (2018): 88–91; International Press Institute, "Rush to Pass 'Fake News' Laws during Covid-19 Intensifying Global Media Freedom Challenges", 3 October 2020, https://ipi. media/rush-to-pass-fake-news-laws-during-covid-19-intensifying-global-media-freedom-challenges/

spreading "fake news". Targets include ordinary netizens violating legal measures against disinformation, especially in times of COVID-19, journalists and civil society members, and opposition politicians who challenge official narratives online. The latter two groups show how anti-fake news allegations serve as an instrument for quelling oppositional voices.

Ordinary Netizens

Ordinary netizens are primary targets of "fake news" allegations. Their online re-posts and re-tweets criticizing governments or their policies, especially in light of the pandemic, are usually accused of distorting the "real facts", thus inciting unrest. This is the case in Cambodia where in 2021, the authorities charged 199 persons out of a total of 215 fake news-related lawsuits for engaging in incitement, criticisms against the government, and distorting and fabricating information.[31] COVID-19 also provided a pretext for the Vietnamese authorities to utilize Decree 15 to telegraph a message to the broader public that any social media user could face the music for what they posted online. In early April 2020, two months after the decree took effect, the police in Hanoi said they had received more than 70 reports of online users sharing "fake news".[32] Less than a month earlier, state media reported that 700 people had been subjected to "working sessions" with the police over circulating "fake news" about COVID-19 on social media. Those invited to the "working sessions" at a police station would need to sign a statement promising to "refrain from engaging in the impugned action" to avoid fines or jail

---

[31] Sar Socheath, "525 Fake News Found in First Quarter of This Year", *Khmer Times*, 17 May 2021, https://www.khmertimeskh.com/50857692/525-fake-news-found-in-first-quarter-of-this-year/

[32] Minh Cuong and Nguyen Hai, "Hanoi to Jail Those Spreading Fake News on Covid-19", *VnExpress*, 7 April 2020, https://e.vnexpress.net/news/news/hanoi-to-jail-those-spreading-fake-news-on-covid-19-4080964.html

sentences.[33] Several other cases, however, were met with more severe legal threats, with one Facebook user facing a fine of VND15 million (US$540) for allegedly posting "false" criticisms of the government.[34]

Concurrently, the Thai government-established Anti-Fake News Centre has been flagging false information online, leading to lawsuits against 1,193 individuals accused of spreading "fake news" between 2019 and 2020. Of this total, at least 287 persons were convicted in 2021.[35] However, this flagging system can be politically subjective by, for instance, citing official narratives as true news vis-à-vis false unofficial rumours. An implication of this practice is that some of those charged with spreading "fake news" may simply have shared stories deviating from the official storyline.[36]

Journalists

Anti-fake news laws are highly politicized and weaponized when used to persecute journalists, and without detailing what content is considered false. Instead, the impact of this falseness on national pillars is emphasized. For instance, Cambodia's 2018 Inter-Ministerial Announcement "Prakas" can force publishers to remove online posts that

---

[33] Amnesty International, "'Let Us Breath': Censorship and Criminalization of Online Expression in Vietnam", 2020, https://www.amnesty.org/en/wp-content/uploads/2021/05/ASA4132432020ENGLISH.pdf, p. 46.

[34] Cuong and Hai, "Hanoi to Jail Those Spreading Fake News on Covid-19".

[35] "ดีอีเอสโชว์ตัวเลขคนไทยแชร์ข่าวปลอมมากถึง 23 ล้านคน พบสื่อมวลชนให้ความสนใจปัญหาข่าวปลอมมากขึ้น" [DES shows statistics of 23 million Thais sharing fake news, finds media pays more attention to the problem of fake news], Anti-Fake News Centre Thailand, 31 December 2021, https://www.antifakenewscenter.com/activity/ดีอีเอส-โชว์ตัวเลขคนไทย-แชร์ข่าวปลอมมากถึง-23-ล้านคน-พบสื่อมวลชนให้ความสนใจปัญหาข่าวปลอมมากขึ้น/

[36] See Janjira Sombatpoonsiri, "Labelling Fake News: The Politics of Regulating Disinformation in Thailand", *ISEAS Perspective*, no. 2022/34, 7 April 2022, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-34-labelling-fake-news-the-politics-of-regulating-disinformation-in-thailand-by-janjira-sombatpoonsiri

authorities consider false. Publishers and journalists who take no action upon receiving a notice would have their licences revoked, exemplified by the cases of two online news outlets, Youth Techo and Stoeng Charl, which in August 2021, were accused of spreading "false information that would cause social unrest".[37] This trend adds to the existing crackdown on the press and journalists; at least eight media outlets had their licences revoked for spreading so-called false information in 2018,[38] and in 2020, 1,343 lawsuits were filed against sources of "fake, objectionable news".[39] Similarly, in Vietnam, the authorities dangled the veiled threat of shutting down any news outlet for publishing what they considered "incorrect" information. As a part of the 2013 Decree 72, a circular requires website owners to eliminate "incorrect" content within three hours of receiving a request from relevant authorities. Website owners' non-compliance can lead to hefty fines and website shutdown, as evident in the case of the newspaper *Phụ nữ TPHCM* (Ho Chi Minh City Women), for alleged publishing of "wrongful information".[40]

The situation is no better in Myanmar. In October 2018, when the National League for Democracy (NDL) was still in government, three journalists were jailed after publishing a story that accused the Yangon regional government of misusing public money. The officials bristled at the coverage, saying it was false.[41] They further argued that the journalists

[37] Nath Sopheap, "Ministry Revokes Two Media Licences on Grounds of Serious Professional Abuse", *VOD*, 26 March 2021, https://www.vodkhmer. news/2021/03/26/ministry-of-information-revokes-license-of-two-online-media-outlet-for-spreading-fake-news/

[38] Socheath, "525 Fake News Found in First Quarter of This Year".

[39] Cambodian Centre for Human Rights, "Submission to the Special Rapporteur on the Promotion and Protection of Rights to Freedom of Opinion and Expression".

[40] An Hai, "Arrests, Suspension of Vietnam Media Signal Crackdown", *Voice of America*, 18 June 2020, https://www.voanews.com/a/press-freedom_arrests-suspension-vietnam-media-signal-crackdown/6191339.html

[41] "3 Myanmar Journalists in Court over Story Gov't Calls False", *Associated Press*, 17 October 2018, https://apnews.com/article/e7d951b 784ac48208000d2609435dbab

and their news outlets violated Section 505A of the Penal Code, which prohibited the publication of "incorrect information" that causes "fear or alarm to the public".[42] Most recent figures show that from February 2021, when the coup occurred, to August 2021, nearly 100 journalists were arrested for either covering anti-coup protests or calling the State Administration Council a "junta".[43] Of the journalists arrested, five were convicted of violating Section 505A, which has been utilized to curb what the authorities deemed "false information".[44]

Opposition Activists and Politicians

"Fake news" allegations also target opposition activists and politicians whose criticisms of governments and their policies are branded as false. In Cambodia, for instance, dozens of political activists, including figures linked with the opposition CNRP have been detained on the charge of spreading "fake news" in criticizing government responses to COVID-19.[45] Likewise, in Thailand, those accused of disseminating "fake news" have been high-profile opposition politicians, scholars, and activists who have criticized government policies. A case in point is the leader of the dissolved Future Forward Party, Thanathorn Juangroongruangkit, who, in March 2021, criticized the government for mishandling the vaccine campaign and giving an unfair advantage

---

[42] Moe Myint, "Yangon Sues Eleven Media for Offenses against the State", *The Irrawaddy*, 10 October 2018, https://www.irrawaddy.com/news/burma/yangon-govt-sues-eleven-media-offenses-state.html

[43] "Myanmar: Junta Escalates Media Crackdown", *Human Rights Watch*, 27 July 2021, https://www.hrw.org/news/2021/07/27/myanmar-junta-escalates-media-crackdown

[44] Ibid.

[45] Business and Human Rights Resource Centre, "Cambodia: Rights Group Concerns over Arrests and Harassment of Activists Amid the COVID-19 Pandemic Measures", 3 April 2020, https://www.business-humanrights.org/en/cambodia-rights-group-concerns-over-arrests-harassment-of-activists-amid-the-covid-19-pandemic-measures

to Siam Bioscience, a domestic producer of the AstraZeneca vaccine owned by King Vajiralongkorn. Soon after this exposé, the authorities filed the complaint that his "fake news" damaged the royal reputation, thus violating both Article 112 and the CCA.[46] Supposedly independent bodies, including the Election Commission (EC), have similarly weaponized "fake news" allegations against those accusing them of being involved in irregularities during the 2019 elections.[47]

Similarly, the Vietnamese authorities have sought to make the most of Articles 88 and 117 of the Penal Code by fusing "anti-state" with "fake news" allegations. As the case of Pham Doan Trang, one of the most high-profile Vietnamese activists, shows, she was convicted of—among other things—"spreading fake information that sow confusion for the people [and] propagandizing information that distort the guidelines and policies of the State of the Socialist Republic of Vietnam".[48] According to the human rights group 88 Project, 17 activists were charged under Article 117 of the Penal Code in 2021 alone.[49]

In Myanmar, journalists and activists were charged with "incitement" and publishing of "incorrect information" under Section 505A of the Penal Code, even though the authorities did not clearly explain what they did wrong.[50] Examples abound. In September 2021, Win Naing Oo, a former

---

[46] "Thai Police Charge Thanathorn with Insulting over Vaccines", *Nikkei Asia*, 30 March 2021, https://asia.nikkei.com/Politics/Thai-police-charge-Thanathorn-with-insulting-king-over-vaccines

[47] Amnesty International Thailand, "'มีคนจับตาอยู่จริงๆ' ข้อจำกัดเสรีภาพในการแสดงออกออนไลน์ในประเทศไทย" ['We are really watched': Restrictions of freedom of online expression in Thailand], March 2020, https://www.amnesty.org/en/documents/asa39/2157/2020/th/, p. 11.

[48] Human Rights Watch, "Vietnam: Free Prominent Blogger", 13 December 2021. https://www.hrw.org/news/2021/12/13/vietnam-free-prominent-blogger

[49] The 88 Project for Free Speech in Vietnam, "2021 Human Rights Report Vietnam", https://the88project.org/wp-content/uploads/2022/05/Annual-Report-2021_final.pdf

[50] "Repression of Activists and Journalists Persists in Myanmar Despite ASEAN Rebuke", *CIVICUS*, 9 November 2021, https://monitor.civicus.org/updates/2021/11/09/repression-activists-and-journalists-persists-myanmar-despite-asean-rebuke/

chief correspondent for Channel Mandalay, was charged with incitement under Section 505A although he had reportedly stopped doing journalism since the coup began in February.[51] Also invoking Section 505A with no clear accusations, the authorities in September 2021 arrested Ma Thuzar, who had filmed many of the major anti-protests for the Myanmar Pressphoto Agency and the *Friday Times News Journal*.[52] Activists who were student union leaders or human rights advocates too became the casualties of Section 505A. For instance, in September 2021, Min Thukha Kyaw, the former chair of the Dagon University Students' Union faced a similar charge. He got a ten-year jail term despite Section 505A's maximum sentence of three years in prison.[53]

Content Block and Takedown: Cambodia, Thailand and Vietnam

The Cambodian, Thai and Vietnamese governments have blocked, filtered and requested takedowns of content they label as false. To this end, these governments cite local laws related to curtailing "fake news" to demand compliance with requests for content removal from ISPs or telecommunication companies, and social media platforms such as Facebook/Meta, Twitter, and YouTube/Google. Specifically, Thailand has increasingly pressured platforms to take down content against the backdrop of anti-government protests, reflecting how the "fake news" claim can restrict the flow of oppositional information.

---

[51] "Detained Former Journalist Charged with Incitement in Mandalay", *Myanmar Now*, 17 September 2021, https://www.myanmar-now.org/en/news/detained-former-journalist-charged-with-incitement-in-mandalay

[52] "Journalist Missing for One Month Held in Yangon Police Station, Charged with Incitement", *Myanmar Now*, 1 October 2021, https://www.myanmar-now.org/en/news/journalist-missing-for-one-month-held-in-yangon-police-station-charged-with-incitement

[53] "Military Tribunal Sentences Former Student Union Chair to 10 Years in Prison", *Myanmar Now*, 8 September 2021, https://www.myanmar-now.org/en/news/military-tribunal-sentences-former-student-union-chair-to-10-years-in-prison

Content Block and Local ISPs

Since the early 2010s, content block is one of the initial toolkits for Internet control by Southeast Asian autocracies against the proliferating anti-government content. But the rhetoric of tackling "fake news" has recently provided a new pretext for intensifying content restrictions. For instance, according to Article 20 under Thailand's CCA, the court can demand ISPs to "suppress and remove computer data" considered to be false and violating public order.[54] As a result, more than 10,000 URLs were blocked in 2010, more than 74,000 URLs were blocked in 2012, and 56 URLs were blocked between May and June 2014 after the 2014 coup. In these instances, most blocked content belonged to critical media and oppositional groups.[55] The use of "fake news" rhetoric was seen at the height of the 2020 anti-establishment protests when the National Broadcasting and Telecommunications Commission (NBTC) pressured ISPs to block websites alleged of distributing "fake news", including those of critical media outlets.[56] Moreover, at the peak of the COVID-19 wave in 2021, the Thai government, granted with powers of the emergency decree, mandated the NBTC to order ISPs to block Internet access to individual IP addresses accused of disseminating false news that caused public fear and interfered with the government's pandemic management.[57]

---

[54] Open Observatory of Network Interference (OONI), "The State of Internet Censorship in Thailand", 20 March 2017, https://ooni.org/post/thailand-internet-censorship/

[55] Poetranto and Senft, "Internet Governance during Crisis", p. 8.

[56] Apornrath Phoonphongphiphat, "Thailand to Block 2,000 Websites ahead of Democracy Protests", *Nikkei Asia*, 18 September 2020, https://asia.nikkei.com/Politics/Turbulent-Thailand/Thailand-to-block-2-000-websites-ahead-of-pro-democracy-protests

[57] "Thailand Bans 'False Message' Amid Criticism of Handling Coronavirus", *Reuters*, 30 July 2021, https://www.reuters.com/world/asia-pacific/thailand-bans-false-messages-amid-criticism-handling-coronavirus-2021-07-30/

Similarly, Cambodia has blocked websites that the government deems provocative, unpatriotic and false, a practice particularly common during electoral campaigns. On the eve of the 2018 national election, for instance, the CPP-led government requested that ISPs, which were under the tight control of the government,[58] block access to at least 17 news websites, including the Voice of America, Radio Free Asia, the Voice of Democracy, and the *Phnom Penh Post*. The authorities claimed that these websites were politically "provocative", something that was apparently prohibited by an electoral regulation on the eve of an election. It is noteworthy that news outlets less critical of the government were not blocked.[59] The prospect of Cambodia installing the National Internet Gateway (NIG) could mean further extensive blocking of websites the government believes to disseminate false content that undermines "social order, national security … and culture".[60]

In Vietnam, regulations have placed the legal onus on ISPs to act as gatekeepers against "toxic", "false" or "incorrect" information. These ISPs are either state-run groups or private tech conglomerates, but the interests of the latter have been increasingly aligned with the government's. According to the Ministry of Information and Communications, over 1,200 sites and 20,000 posts were removed in 2021 for hosting information that sought to "sabotage or disrupt public

[58] Freedom House, "Freedom on the Net. Cambodia", 2021, https://freedomhouse.org/country/cambodia/freedom-net/2021

[59] Erin Handley, "Cambodia Blocks 17 Media Websites Before Vote", *Aljazeera*, 28 July 2018, https://www.aljazeera.com/news/2018/7/28/cambodia-blocks-17-media-websites-before-vote

[60] "Cambodia Steps up Surveillance with New Internet Gateway", *France 24*, 14 February 2022, https://www.france24.com/en/live-news/20220214-cambodia-steps-up-surveillance-with-new-internet-gateway; Cambodian Centre for Human Rights, "Submission to the Special Rapporteur on the Promotion and Protection of Rights to Freedom of Opinion and Expression". The NIG would facilitate government oversight of all incoming and outgoing domestic and international web traffic through a single, national Internet gateway (NIG), an idea experimented on through China's Internet Firewall.

security and social order; cause fear and alarm to the public".[61] Besides, 516 other sites with over 2,000 posts were also scrubbed for containing "distorted" and "fabricated" information about Vietnam's handling of the COVID-19 pandemic.[62] The authorities never singled out any specific website whose content was blocked or removed, and instead only stated generally that certain "fake" and "false" news had been scrubbed from the Internet.

Content Takedown and Social Media Platforms

With the rise of social networking platforms, governments have scrambled to control what is to be seen or not on social media. This is particularly the case for Thailand and Vietnam, with the former submitting more than 700 requests to Facebook for content takedown between 2018 and 2021. In Vietnam, stringent regulations, especially the Cyber Security Law, resulted in Facebook and YouTube removing 93 and 90 per cent respectively of the content on their platforms during the first quarter of 2022. The authorities in both countries cited the fact that the content contained false information relating to COVID-19 and defamation against the governments, the Communist Party, and the monarchy.[63] For instance, in June 2021, the Thai courts issued an order to Facebook to block or remove eight Facebook accounts for allegedly disseminating "fake news". These accounts were run by activists, journalists and

---

[61] "Bộ Trưởng Bộ Thông Tin và Truyền Thông: Phản Bác Các Luận Điệu Xuyên Tạc, Sai Sự Thật về Phòng, Chống Dịch Bệnh COVID-19" [Minister of Information and Communications: Refuting Distorted and Wrong Information on the Fight against the COVID-19 Pandemic], *Vietnam National Assembly's News Portal*, 19 January 2022, https://quochoi.vn/tintuc/Pages/tin-doan-dai-bieu-quoc-hoi.aspx?ItemID=61914

[62] Ibid.

[63] "Facebook sẽ chặn quảng cáo chính trị từ các tài khoản phản động" [Facebook will block political ads from subversive accounts], *Cong an Nhan dan*, 8 October 2020, https://congan.com.vn/tin-chinh/facebook-se-chan-quang-cao-chinh-tri-tu-cac-tai-khoan-phan-dong_100905.html

organizations that had been outspoken about the monarchy.[64] The same court orders also compelled platforms to take down what was believed to be false content, and threatened to ban online media outlets (i.e., Voice TV, Prachatai, the Standard, and the Reporters) as well as one Facebook page belonging to the pro-democracy group "Free Youth". These outlets broadcasted the scandal that associated the monarchy with the country's vaccine mismanagement, which the government denounced as untrue and defamatory.[65] For Google, the takedown is even more severe than for Facebook. From 2009 to 2020, 28,595 items were removed from Google Search and YouTube.[66] In the context of the 2020 protests, the government requests skyrocketed, citing the need to crack down on "illegal" and "fake" content.[67]

Likewise, according to the Vietnamese Ministry of Information and Communications, major Western social media platforms continued to entertain government requests to remove what was deemed "illegal". The compliance rate for Facebook was 90 per cent and Google 93 per cent during the first quarter of 2022.[68] Since 2017, the transparency reports of both platforms have revealed that the Vietnamese government sometimes identifies illegal content as "incorrect", "false" or "distorted" information. These are, however, related to either criticisms against the government or ones that "oppose the Communist Party and the

---

[64] "Social Posts Prompt Charges", *Bangkok Post*, 25 May 2021, https://www.bangkokpost.com/thailand/general/2120927/social-posts-prompt-charges

[65] Nontarat Phaicharoen and Wilawan Watcharasakwet, "Thailand Orders News Outlet Shut Down Amid Protests", *Benar News*, 20 October 2020, https://www.benarnews.org/english/news/thai/court-order-10202020174349.html

[66] Feldstein, *The Rise of Digital Repression*, p. 119.

[67] Access Now, Article 19, ASEAN Regional Coalition to #StopDigitalDictatorship and Manushya Foundation, "Joint UPR Submission to the UN Universal Periodic View: Digital Rights in Thailand", March 2021, https://www.article19.org/wp-content/uploads/2021/04/Joint-UPR-Submission-Digital-Rights-in-Thailand.pdf

[68] Phuong Nguyen and Fanny Potkin, "EXCLUSIVE Vietnam Plans 24-hour Take-own Law for 'Illegal' Social Media Content—Sources", *Reuters*, 21 April 2022, https://www.reuters.com/business/media-telecom/exclusive-vietnam-plans-24-hour-take-down-law-illegal-social-media-content-2022-04-20/

Government of Vietnam".[69] So far there has been no reported permanent takedown of high-profile Facebook accounts.[70] See Figure 2.

Digital Surveillance: Thailand and Vietnam

Under the banner of combating "fake news", systematic surveillance of online content and activities has been streamlined in part to make the persecution of Internet users more targeted. This is particularly the case for Thailand and Vietnam which have recently added the need to counter "fake news" to the existing reasons (e.g., national security) for boosting the surveillance infrastructure. Two specific aspects show how the "fake news" claim provides a legitimate pretext for this practice: social media monitoring, and collection of users' data.
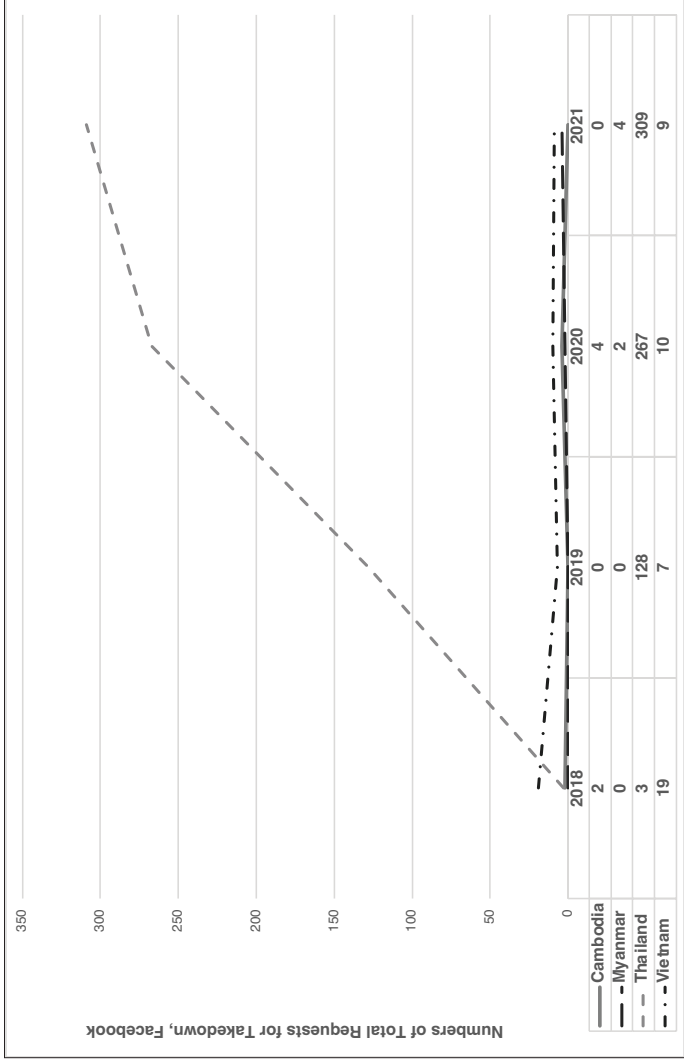
Social Media Monitoring

Flagging content deemed false and penalizing its purveyors necessitates extensive systems of manual and automatic monitoring of social media conversations. In Thailand, cyber units, including the police "cyber scouts" and the Internal Security Operations Command's (ISOC) tens of thousands of cyber troopers are mandated to manually monitor and flag anti-monarchy content, including "distorted information".[71] In addition, in 2016, the Thai military established the Army Cyber Centre that,

[69] Dien Nguyen An Luong, *A Study of Vietnam's Control over Online Anti-State Content*, Trends in Southeast Asia, no. 5/2022 (Singapore: ISEAS – Yusof Ishak Institute, 2022), p. 20.

[70] When certain prominent Facebook accounts were suspended, their owners were quick to appeal to the social media giant and had them reinstated after a certain amount of time, which could range from one to several months. On the other hand, Vietnamese authorities also seemed more inclined to have Facebook or YouTube suspend certain accounts on a case-by-case basis. This dynamic has perpetuated a cat-and-mouse game between Vietnamese censors and Facebook users.

[71] Eglé Juodyté, "Editorial: Thailand", *Nord VPN*, 22 June 2017, https://nordvpn. com/ar/blog/an-overview-surveillance-practices-in-thailand/. The mandate of these units is often two-pronged: social media monitoring and content manipula- tion, a topic to which we return in the conclusion. Janjira Sombatpoonsiri,

Figure 2: Total Numbers of Government Requests for Facebook's Content Takedown

	2018	2019	2020	2021
Cambodia	2	0	4	0
Myanmar	0	0	2	4
Thailand	3	128	267	309
Vietnam	19	7	10	9

Numbers of Total Requests for Takedown, Facebook

while aiming to bolster capacities against cyber attacks, sought to tackle "fake news". General Chalermchai Sittisart, then army chief, suggested that robust surveillance was crucial for bolstering cybersecurity and tackling endemic "fake news", stating that: "I worry about the distorted information which has been widely disseminated. [The army has to] build mechanisms to promote understanding with the people."[72] He was also of the opinion that Thais should be trained to show more discretion before forwarding messages on social media because they might not know whether "[these] messages were true or false".[73] Following in these footsteps, the police's Technology Crime Suppression Division set up a team of 60–70 officers in 2017 initially to keep taps on anti-monarchy feeds on social media.[74] But in 2020 when this unit was formalized as the cyber police bureau, the need to crack down on "fake news" became an additional objective of the unit.[75] With the Cabinet's 2022 approval of the new anti-fake news regulations, the manual monitoring of social media is expected to expand nationwide, as "fake news" monitoring agencies will soon be created in each ministry and across 76 provincial governors' offices.[76]

"'We are Independent Trolls': The Efficacy of Royalist Digital Activism in Thailand", *ISEAS Perspective,* no. 2022/1, 5 January 2022, https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-1-we-are-independent-trolls-the-efficacy-of-royalist-digital-activism-in-thailand-by-janjira-sombatpoonsiri/

[72] "Army Tightens Monitoring of Social Media", *Bangkok Post*, 1 November 2016, https://www.bangkokpost.com/thailand/general/1124460/army-tightens-monitoring-of-social-media

[73] Ibid.

[74] Juodytė, "Editorial".

[75] "Cyber Cops Unit to be Set up", *Bangkok Post*, 12 June 2020, https://www.bangkokpost.com/thailand/general/1933404/cyber-cops-unit-to-be-set-up

[76] "Prawit Tells Officials to Clamp down on Fake News", *Bangkok Post*, 10 June 2021, https://www.bangkokpost.com/thailand/politics/2129671/prawit-tells-officials-to-clamp-down-on-fake-news; "ข่าวปลอม: ร่างระเบียบสำนักนายกฯ ปราบเฟคนิวส์ ความพยายามล่าสุดของรัฐบาลในการกลบเสียงวิจารณ์" [Fake news: Draft by Prime Minister's Office to crackdown on fake news, latest government's attempt to stifle criticisms], *BBC News Thai*, 4 February 2022*,* https://www.bbc.com/thai/thailand-60239430

On top of manual surveillance, the Anti-Fake News Centre (founded in 2019 under the Ministry of Digital Economy and Society) has reportedly introduced an automated system akin to social media listening tools to mine and screen massive amounts of social media data.[77] To be sure, these surveillance units have leveraged the systematic monitoring of social media "big data" to buttress lawsuits against those accused of distributing "fake news".[78]

Similar to Thailand, the Vietnamese government has invested massively in strengthening online monitoring efforts. These were done by the state-sponsored 10,000-strong cyber troops. In the view of the authorities, the cyber military unit engages in "well-qualified and loyal" work to scour and collect information on social media, participate in online debates to maintain "a healthy cyberspace"[79] and to protect the regime from "wrong", "distorting" or "false news". The operation of the cyber unit appears to have been buttressed by a web-monitoring centre that was set up in late 2018. The centre is capable of automatically scanning up to 300 million news items per day for "false information".[80] The cyber troops often flag what they label as anti-state content and "wrong, distorted opinions" on Facebook, and remove them.[81] The

[77] "ประวัติตรวจศูนย์ต้านข่าวปลอม สั่งตั้ง บก.ควบคุมฯ ดูแลทั่วประเทศ" [Prawit Order to Set up Anti-fake News and Nationwide Command Centres], *Komchadluek*, 22 April 2020, https://www.komchadluek.net/news/428278

[78] See, for instance, "Army Tightens Monitoring of Social Media".

[79] James Pearson, "How Vietnam's 'Influencer' Army Wages Information Warfare on Facebook", *Reuters*, 9 July 2021, https://www.reuters.com/world/asia-pacific/how-vietnams-influencer-army-wages-information-warfare-facebook-2021-07-09/

[80] Linh Pham, "Vietnam Vows to Identify Social Network Users", *Hanoi Times*, 11 November 2020, http://hanoitimes.vn/vietnam-vows-to-identify-social-network-users-314784.html

[81] Pearson, "How Vietnam's 'Influencer' Army Wages Information Warfare on Facebook"; "Hơn 10.000 người trong 'Lực lượng 47' đấu tranh trên mạng [More than 10,000 people in 'Force 47' struggle online]", Tuoitre Online, 25 December 2017, https://tuoitre.vn/hon-10-000-nguoi-trong-luc-luong-47-dau-tranh-tren-mang-20171225150602912.htm

accounts that host such content could also become a target of removal or suspension if they are influential and high-profile. The cyber troops do so by capitalizing on loopholes in Facebook's community policies that allow for automatic rejection of content if enough people lodge complaints about certain accounts.[82]

Organized troops aside, the authorities have also enlisted the wider Vietnamese society in countering "toxic information" about the regime in digital space.[83] Their method reflects a crossover between public opinion shapers and cyber troops, as they scour social media for "wrong", "distorting" or "false news" and then either rebuke online critics or have their posts and accounts removed.[84] In going after online dissidents or critics accused of spreading "false news" about the regime, cyber troops or public opinion shapers are even encouraged to compile dossiers on those people, including their online behaviours and other personal details, and then report their possible violations of Vietnamese laws to the authorities for real-life actions.[85]

Collection of Users' Data

An emerging trend observed is the rhetoric of countering "fake news" partly used to justify governments' collection of Internet traffic data

---

[82] See more in Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation", Working Paper 2019.2, Oxford, Project on Computational Propaganda, 2019, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf, p. 13; Sam Biddle, "Facebook Lets Vietnam's Cyberarmy Target Dissidents, Rejecting A Celebrity's Plea", *The Intercept*, 22 December 2020, https://theintercept.com/2020/12/21/facebook-vietnam-censorship; and David S. Cloud and Shashank Bengali, "Facebook Touts Free Speech. In Vietnam, It's Aiding in Censorship", *Los Angeles Times*, 22 October 2020, https://www.latimes.com/world-nation/story/2020-10-22/facebook-censorshipsuppress-dissent-vietnam

[83] Pearson, "How Vietnam's 'Influencer' Army Wages Information Warfare on Facebook".

[84] Sam Biddle, "Facebook Lets Vietnam's Cyberarmy Target Dissidents, Rejecting A Celebrity's Plea".

[85] Ibid.

and users' "metadata" (i.e., information which gives insights into the identities of end-users and is stored by ISPs). For instance, in Thailand, the CCA, primarily instrumental in cracking down on "fake news", grants power to relevant monitoring bodies to access users' data without a court order and compels ISPs to retain user-related or traffic data. In 2019, Thailand passed the Cybersecurity Act to handle cyber threats, enabling state apparatuses to use interception technologies to obtain personal data. While the law does not directly attribute "fake news" to a cyber threat, security policies and white papers described earlier clump these together in the same category of threat. Based on this security framework, the authorities can cite the Act to acquire users' personal data in the name of countering dangerous "fake news".[86] Moreover, the 2022 anti-fake news regulations refer to "fake news" as the key threat to national stability, thereby, among other things, forcing ISPs, platforms, and computer software providers (e.g., App Stores) to store users' traffic data.[87] The impact of these measures on shrinking digital space remains to be seen, but against the backdrop of the Thai government's alleged use of spyware such as Pegasus, it is likely that this extensive collection of users' data through legal and technological tools would potentially make legal persecution of dissidents more targeted.[88]

In Vietnam, Article 26 of the Cyber Security Law that is premised on the task of fighting false information and "fake news" contains vaguely

---

[86] "ร่าง พ.ร.บ. มั่นคงไซเบอร์ฯ 62: เปิดช่องเจ้าหน้าที่รัฐ 'สอดส่อง' คนเห็นต่างได้" [Draft Cybersecurity Law 62: Possibility of State Surveillance of Dissidents], *iLaw*, 25 February 2019, https://ilaw.or.th/node/5173

[87] Suchit Leesa-nguansuk, "Data Legal Upgrade Sparks Concern", *Bangkok Post,* 17 August 2021, https://www.bangkokpost.com/business/2166227/data-legal-upgrade-sparks-concerns (accessed 2 March 2022).

[88] "ดีอีเอสฮึมออกร่างประกาศฯ แก้ 'ข่าวปลอม' ทะลักโซเชียลมีเดีย" [DES Set to Pass New Regulation to Address Spread of Fake News in Social Media], *Bangkokbiz,* 20 May 2021, https://www.bangkokbiznews.com/tech/939130. See also Janjira Sombatpoonsiri, "Digital Surveillance in Thailand: When the Pegasus Takes Flight", *Fulcrum*, 24 February 2022, https://fulcrum.sg/digital-surveillance-in-thailand-when-pegasus-takes-flight/

worded provisions that enable the authorities to access Internet users' personal data—ranging from names, birth dates, nationality to identity cards, credit card numbers and health records. They do not need to get users' explicit content or inform them of it, as long as it is justified on the grounds of national security, public security and public order. Most recently, also in the name of curbing "fake news", the draft amended version of Decree 72 that is pending government approval seeks to force "cross-border" social media platforms to hand over the contact information of account operators that run live streaming programmes and amass over 10,000 followers or subscribers.[89] In the draft decree, the Ministry of Information and Communications justified this requirement by blaming Western social media platforms for not being fully compliant with Vietnamese laws in fighting fake news: "A lot of content posted there is disinformation, causing instability and frustration in the society and inequality between domestic and foreign companies."[90]

Internet Shutdowns: Myanmar

The last trend we observe is a government's shutdowns of the Internet and communication applications under the pretext of deterring "fake news"—evident in the case of Myanmar in the wake of the 2021 coup. Internet shutdowns are generally characterized by the restriction of access to an existing operating site of the Internet and communication platforms.[91] Shutdowns can be partial (e.g. the disruption or slowdown of mobile service in certain areas or during certain hours in a day, or the selective blocking of some platforms) or complete (also known as "blackout" in which online connectivity is fully severed at times

---

[89] Tomoya Onishi, "Vietnam to Tighten Grip on Facebook and YouTube Influencers", *Nikkei Asia*, 13 July 2021, https://asia.nikkei.com/Politics/Vietnam-to-tighten-grip-on-Facebook-and-YouTube-influencers

[90] "Vietnam to Tighten Grip on Social Media Livestream Activity", *Reuters*, 14 July 2021, https://www.reuters.com/world/asia-pacific/vietnam-tighten-grip-social-media-livestream-activity-2021-07-14/

[91] Ibid.

nationwide).[92] When resorting to Internet shutdowns, governments generally claim the necessity to prevent the spread of unfavourable information and specifically "fake news" that may fuel riots and civil war, interfere with elections, and derail military coups.[93] In the latter, the claim to combat "fake news" provides a convenient justification for obstructing information flows that may facilitate mass mobilization against a new period of military rule. Achieving this can contribute to entrenching the junta's ruling power.[94]

Among the four Southeast Asian autocracies, Myanmar provides the most glaring example of the most draconian response in the name of fighting "fake news": to shut down the Internet altogether. Myanmar had first introduced subnational Internet shutdowns in Rakhine and Chin States in 2019, but after the 2021 coup, the State Administration Council opted for full-scale nationwide shutdowns (lasting for 30 hours) in light of mass protests against the putsch. It invoked the 2013 Telecommunications Law previously detailed to order all mobile operators to temporarily shut down the Internet networks.[95] The written directives sent to ISPs such as Telenor and the state-owned Myanmar Posts and Telecommunications cited the occurrence of an emergency, but relevant to our analysis is how the justification for Internet shutdowns was also based on the "fake news" rhetoric. According to the Ministry of Communications and Information, shutdowns were necessary because "[c]urrently these

[92] Steven Feldstein, "Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?", Carnegie Endowment for International Peace, 31 March 2022, https://carnegieendowment.org/publications/86687

[93] Ibid.; Rofi Rahman and Shu-Mei Tang, "Fake News and Internet Shutdowns in Indonesia: Systems of Failure to Uphold Democracy", *Constitutional Review* 8, no. 1 (2022): 151–83.

[94] Darrell M. West, "Shutting Down the Internet", *Techtank*, 5 February 2021, https://www.brookings.edu/blog/techtank/2021/02/05/shutting-down-the-internet/

[95] "Myanmar's Internet Shutdown: What's Going on and will it Crush Dissent", 17 February 2021, https://www.theguardian.com/world/2021/feb/17/myanmars-internet-shutdown-whats-going-on-and-it-crush-dissent

people who are troubling the country's stability … are spreading fake news and misinformation and causing misunderstanding among people by using Facebook".[96] In another statement by the same ministry, the term "rumour" was used in place of "fake news", but the warning sent to anti-coup protesters ringed a similar tone to that conveyed to ISPs:

> Some media and public are spreading rumours on social media conducting gatherings to incite rowdiness and issuing statements which can cause unrest. We would like to urge the public not to carry out [these] acts … [and] to cooperate with the government in accordance with the existing laws.[97]

The junta also imposed various measures of partial shutdowns. These included night-time Internet blackouts for almost 50 days, suspended wireless broadband services for around 18 days,[98] blocked mobile Internet access in cities and towns where mass mobilization was ongoing,[99] and slowed Internet service which made it difficult to post or watch protest-related videos (see Figure 3).[100] Moreover, by blaming Facebook for

---

[96] "Junta Issues Daily Directives to Further Block Internet Access, Telecoms Providers Say", *Myanmar Now*, 20 March 2021, https://www.myanmar-now.org/en/news/junta-issues-daily-directives-to-further-block-internet-access-telecoms-providers-say

[97] Kim Lyons, "Myanmar Order Internet Providers to Block Twitter and Instagram in the Country", *The Verge*, 6 February 2021, https://www.theverge.com/2021/2/6/22269831/myanmar-orders-block-twitter-facebook-instagram-military-coup

[98] "Myanmar Orders Wireless Internet Shutdown Until Further Notice: Telecoms Sources", *Reuters*, 1 April 2021, https://www.reuters.com/article/us-myanmar-politics-internet/myanmar-orders-wireless-internet-shutdown-until-further-notice-telecoms-sources-idUSKBN2BO5H2?il=0; Rebecca Radcliffe, "Myanmar Coup: Military Expands Internet Crackdown", *The Guardian*, 2 April 2021, https://www.theguardian.com/world/2021/apr/02/myanmar-coup-military-expands-internet-shutdown

[99] Access Now, "Update: Internet Access, Censorship, and the Myanmar Coup", 18 March 2022, https://www.accessnow.org/update-internet-access-censorship-myanmar/

[100] Feldstein, "Government Internet Shutdowns Are Changing".

Figure 3: Internet Disruptions in Myanmar from 18 January to 29 March 2021
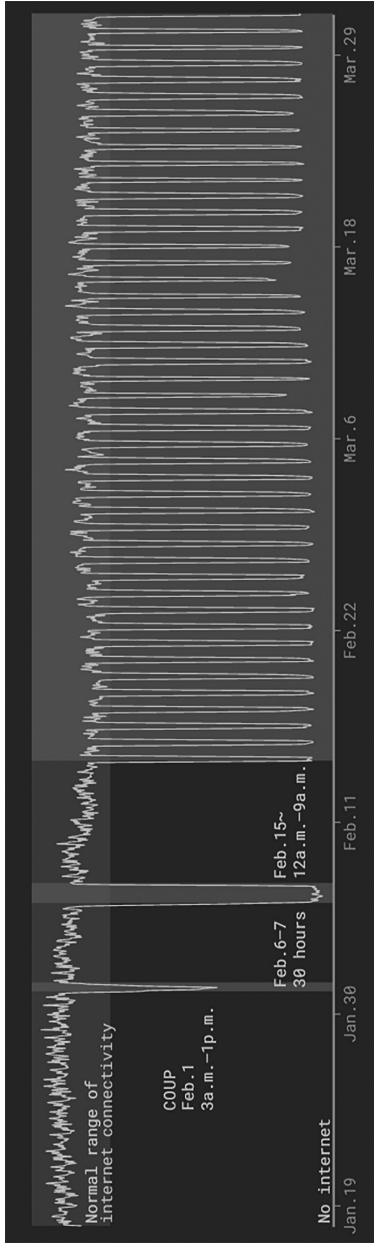
Note: The graph shows the volatility of service connection, with most connectivity drops taking place at night.
Source: Monash IP Observatory, cited in Reuters Graphics (https://graphics.reuters.com/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/).

ongoing disinformation-induced "instability", the junta moved to primarily block Facebook. Later Twitter, WhatsApp and Instagram were also blocked, as shown in Figure 4.[101]

Restricting access to Internet service and communication applications contributes to hampering anti-coup campaigns that are also conducted online.[102] The blockage resulted in a steep drop in the "reachability" of key mobilizing platforms, especially Facebook and Twitter. This forced anti-coup protesters to rely mainly on offline mobilization, including banging pots and pans, and analogue technologies such as shared radio frequencies and landline phones.[103] Many could circumvent the blockage by using virtual private networks (VPNs)—a common workaround for Internet users to circumvent online censorship. But they risked facing penalties after the junta's Directorate of Telecommunications imposed daily directives prohibiting the use of VPNs.[104]

CONCLUSION

"Fake news" allegations have provided rhetorical ammunition for autocratic control over digital space. Vague definitions of what constitutes false content and the association of "fake news" to horrendous consequences have rendered governments the power to identify critics
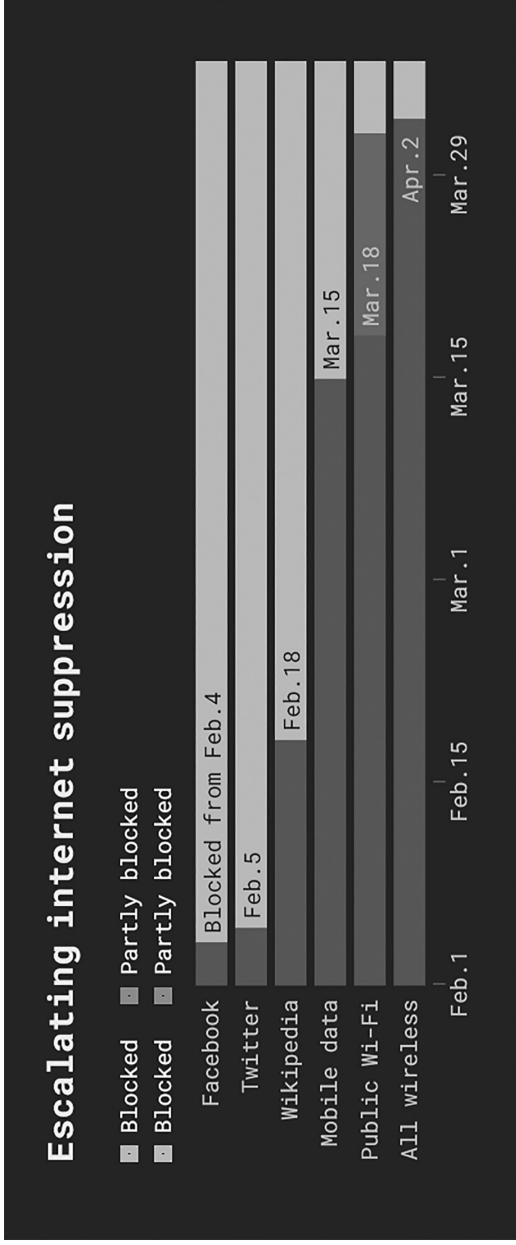
---

[101] "Myanmar's Digital Regime Foreshadows SE Asia", *Bangkok Post*, 15 March 2021, https://www.bangkokpost.com/opinion/opinion/2083615/myanmars-digital-regime-foreshadows-se-asia; Caitlin Thompson, "Myanmar Sets a Dangerous Precedent with the New Draft of its Cyber Security Bill", *Coda,* 8 February 2022, https://www.codastory.com/newsletters/myanmar-vpn-bfacebook/

[102] Andrea Januta and Minami Funakoshi, "Myanmar's Internet Suppression", *Reuters Graphic*, 7 April 2021, https://graphics.reuters.com/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/

[103] Ibid.

[104] "Junta Issues Daily Directives to Further Block Internet Access, Telecom Providers Say", *Myanmar Now*, 20 March 2021, https://www.myanmar-now.org/en/news/junta-issues-daily-directives-to-further-block-internet-access-telecoms-providers-say

Figure 4: The Length of Blockage of Social Networking Sites and Websites Central to Anti-Coup Efforts

Escalating internet suppression

- Blocked   ■ Partly blocked
- Blocked   ■ Partly blocked

Facebook	Blocked from Feb.4
Twitter	Feb.5
Wikipedia	Feb.18
Mobile data	Mar.15
Public Wi-Fi	Mar.18
All wireless	Apr.2

Feb.1   Feb.15   Mar.1   Mar.15   Mar.29

Source: Monash IP Observatory, cited in Reuters Graphics (https://graphics.reuters.com/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/).

and political opponents as "fake news" purveyors. This politics of defining "fake news" leads to its weaponization to undergird diverse practices to constrict digital space, beyond mere legal charges. We have shown four patterns through which this development has emerged in Cambodia, Myanmar, Thailand and Vietnam. In addition, we have found that these autocracies rely on the "fake news" claim to justify specific policies, but not others:

Pattern 1: in all four autocracies, governments use the "fake news" claim to charge critical Internet users, including ordinary netizens, journalists, pro-democracy activists, and opposition politicians.

Pattern 2: in Cambodia, Thailand, and Vietnam, the "fake news" threat provides a pretext for governments to compel ISPs to block and filter content unfavourable to governments. Especially Thailand and Vietnam have pressured social media platforms to take down dissenting content.

Pattern 3: Particularly Thailand and Vietnam include the "fake news" claim to foster extensive surveillance of social media posts and systematic collection of users' data.

Pattern 4: In the face of anti-coup mobilization, Myanmar under the State Administration Council has blocked and restricted access to Internet connections and communication platforms, blaming companies for accommodating "fake news" detrimental to national stability. Table 2 summarizes these patterns.

Analysing factors that shape these different patterns would warrant further research, but for now, we expect that the digital capacities of each autocracy to carry out different degrees of digital repression could play a role. Thailand and Vietnam, for instance, possess a large extent of bureaucratic capacities that might enable extensive social monitoring. The countries' emerging cyberinfrastructure also facilitates state use of technological tools to collect users' data at scale. Furthermore, growing exposure to the digital economy constitutes a potential explanatory factor. Thailand and Vietnam rely on platforms for their digital economies such as online trade and the platform-based advertisement industry.

Table 2: Four Patterns of Digital Repression under the Pretext of Tackling "Fake News"

Pattern	Tactic vis-à-vis fake news claim	Country			
		Cambodia	Myanmar	Thailand	Vietnam
1	Legal persecution of online users	X	X	X	X
2	Content block and takedown	X		X	X
3	Surveillance			X	X
4	Internet shutdowns		X		

Source: Authors' elaboration.

Conversely, platforms such as Facebook/Meta and Google/YouTube depend on millions of users in Thailand and Vietnam for extracting behavioural data valuable to the furthering of these tech giants' profits. This interdependency may explain why the two countries prefer to pressure and incentivize tech companies to take down some content, rather than opt for the wholesale shutdown of platforms and the Internet as in the case of Myanmar whose digital economy is developing.[105] In this regard, the difference is stark when comparing Thailand and Myanmar that similarly faced anti-regime mobilization in online and offline spaces in 2020 and 2021. Although Thailand cajoled platforms to curb "fake news" the authorities believed to have stemmed from protesters, it hardly considered shutting them down.[106]

Future research is needed to shed light on the interplay between autocracies' suppression of digital space under the banner of combating "fake news" and their campaigns to manipulate social media through cyber trooping. So far, all four autocracies studied in this article have deployed cyber troops to drown out online dissent, while injecting government narratives into social media.[107]

How this practice of "social manipulation" that actually needs a vibrant social media environment interacts with the governments' suppression of digital space deserves in-depth examination.

---

[105] Peter Guest, "They Want Us to Disappear", *Rest of World*, 11 May 2021, https://restofworld.org/2021/they-want-us-to-disappear/

[106] The Thai junta allegedly shut down Facebook for about 30 minutes upon its seizure of power in 2014, but it was quick to backtrack. See "Thai Ministry Sparks Alarm with Brief Block of Facebook", *Reuters*, 28 May 2014, https://www.reuters.com/article/thailand-politics-facebook-idINKBN0E80U520140528

[107] See, for instance, Astrid Norén-Nilsson, "Fresh News, Innovative News: Popularizing Cambodia's Authoritarian Turn", *Critical Asian Studies* 53, no. 1 (2021): 89–108; Janjira, " 'We Are Independent Trolls'"; Dien Nguyen An Luong, "How Hanoi Is Leveraging Anti-China Sentiments Online", *ISEAS Perspective*, no. 2020/115, 13 October 2020, p. 2.