

Research Report

Tackling Disinformation, Foreign Information Manipulation and Interference in Southeast Asia and Broader Indo Pacific

Fitriani, Pieter Pandie, Sekar Arum Jannah

TACKLING DISINFORMATION, FOREIGN INFORMATION MANIPULATION AND INTERFERENCE IN SOUTHEAST ASIA AND BROADER INDO PACIFIC



A Research Report by Safer Internet Lab

Fitriani
Pieter Pandie
Sekar Arum Jannah

The views expressed here are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, or any other organization. Please contact the author(s) directly with any comments or questions.

© 2025 Safer Internet Lab
All rights reserved

ABOUT THE STUDY

This study examines the impact of disinformation, foreign information manipulation and interference on democratic processes, social order, and privacy in Southeast Asia and the broader Indo-Pacific region. It analyses how national and regional stakeholders address these challenges through legal regulations, fact-checking and other countermeasures. As Southeast Asian nations navigate democratisation and digital transformation, the research facilitates cross-country learning on FIMI tactics, technological methods, and narratives, with a focus on the Association of Southeast Asian Nation (ASEAN) and its dialogue partners, including Australia, South Korea, India, Japan and Taiwan. The study also evaluates the evolution of FIMI operations before and after the rise of generative AI, drawing comparisons with Indo-Pacific case studies. Ultimately, it provides actionable policy recommendations to counter state-sponsored disinformation through a multi-stakeholder approach. The study runs for two years between 2024 to 2025, with incident data observed for the span of 2019 to 2024. The conceptualisation and data collection for this study took place between March to October 2024. Focus group discussion with academics and experts working on the space of information influence and media is done in November 2024, while gaining feedback for the writing of the report is done in February 2025. The authors would like to thank Chhengpor Aun, Radityo Dharmaputra, Nélon Belo, Harris Zainul, Muhammad Faizal Bin Abdul Rahman, Nasri Tahir, Jerry Yu, Endy Bayuni, Minjun Hong, Noel Hidalgo Tan, Ashutosh Nagda, Amara Thiha, Kulachada Chaipipat, Maria Elize Mendoza, Daisuke Furuta and Trio Wahyu Pramono for their feedback and contribution to this study.

TABLE OF CONTENTS

1. Introduction	1
2. Literature Review	2
Framework	3
Motives and Trends	4
Spread and Reach	5
Current and Emerging Responses and Mitigation Strategies for FIMI	6
3. Research Question and Objective	8
4. Methodology	9
5. FIMI Trends 2019-2024 and Analysis	10
Data Collection Guidances	10
Key Trends	12
Major Timelines	15
6. Countries' Approaches to Addressing FIMI	17
Brunei Darussalam	17
Cambodia	17
Indonesia	18
Laos	18
Malaysia	19
Myanmar	19
The Philippines	20
Singapore	20
Thailand	21
Vietnam	22
Timor Leste	22
Australia	23
India	24
Japan	24
South Korea	25
Taiwan	25
7. Regional Organisations' Approach on FIMI	28
ASEAN	29
Pacific Islands Forum (PIF)	30
8. Conclusion and Recommendation	30

INTRODUCTION

From 2023 to early 2024 the Safer Internet Lab (SAIL) team conducted a Southeast Asia-wide study on regional and cross-border responses to disinformation. The research findings revealed various strategies that countries in the region apply to address the production, propagation and distribution of disinformation materials. These strategies include promoting media literacy, moderating content, empowering journalists, fact checking, tightening government regulations, leaning on international collaboration, limiting access to the internet, and, most commonly, adopting legal approach.

At the report launch, the SAIL team received feedback that further work needs to be done to address regional disinformation, especially with the use of artificial intelligence (AI) and deep fakes, which have been used to manipulate and interfere information to the scale that it impacts democratic processes, social order and one's right to privacy. Additionally, engagement with wider stakeholders, such as civil society groups and industries was also encouraged, in order to gather diverse perspectives and learn of different tools for addressing disinformation.

For this research, the International Relations (IR) SAIL team focuses its research on addressing foreign information manipulation and interference (FIMI) in Southeast Asia, examining the trend and tendencies both from the national and regional perspective. FIMI is defined by the European Union External Action Service as a pattern of mostly non-illegal and manipulative behaviour that threatens or has the potential to negatively impact values, procedures, and political processes conducted by foreign state or non-state actors and their proxies inside and outside their territory¹. FIMI often exploits societal divisions, political vulnerabilities, and nascent digital literacy to disseminate false and misleading information. Moreover, in countries where media presence is limited or doubted by the society, social media is commonly used as a tool to share disinformation.

Southeast Asia occupies a critical position in global geopolitics due to its strategic location, economic potential, and diverse cultural landscape. The region has a longstanding norm-shaping organisation of the Association of Southeast Asian Nations (ASEAN) with ten member states² and will soon increase its membership.³ The region consists of varying political systems and economic developmental stages, with one of the busiest sea channels in the world, Malacca Straits carries 40% of global trade has made Southeast Asia's stability and democratic progress a significant interest to global powers. The region's burgeoning digital connectivity has also made it a fertile ground for foreign information manipulation and interference. The Indo-Pacific region, encompassing Southeast Asia, has emerged as a focal point of global geopolitical competition due to its economic dynamism, strategic maritime routes, and diverse political landscapes. This prominence has made the region a prime target for manipulative actions that threaten democratic values, political processes, and societal stability, operating in the "grey zone" – between peace and open conflict – through hybrid tactics, blurring the lines between peace and conflict.

The region's strategic importance is underscored by its position at the nexus of major trade routes, connecting the economies of East Asia, South Asia and the Pacific. This makes it an arena for both cooperation and competition among global powers such as the United States, China and Russia. As these powers vie for influence, FIMI has become a key tool in shaping narratives, undermining adversaries and gaining strategic advantages. In recent years, studies have noted the presence of

¹ European External Action Service, 1st EEAS Report on Foreign Information Manipulation and Interference Threats (EEAS 2023), [Online](#)

² Indonesia, Malaysia, Philippines, Singapore, Thailand (1967 founding members), Brunei Darussalam (1984), Vietnam (1995), Laos, Myanmar (1997) and Cambodia (1999).

³ Timor Leste has been an observer since 2022 and in May 2023 adopted a roadmap to be ASEAN full member through steps, including establishing a national representative to the regional organisation and preparing a financial plan to join.

disinformation campaigns originating targeting the region.⁴ The revealed cases of these disinformation campaigns are often related with broader geopolitical issues in the region and beyond. Examples of this include border tensions in the South China Sea between claimants of Vietnam, the Philippines, Taiwan and China, as well as the war in Ukraine and escalations in the Middle East, showing that such operations are often an extension of physical conflict. To shape perspective, since 2016, Beijing has invited Southeast Asian journalists from established media institutions to months-long all-expense-paid programs to get to know China, providing only positive aspects of the country.⁵ A year later, Chinese state media began to embark on content-sharing agreements and joint productions with Southeast Asian countries, including Singapore⁶, Vietnam, Thailand and Indonesia⁷. These content-sharing agreements may have obscured some content's origins when the news was conveyed to local audiences.

The rapid digital transformation in Southeast Asia and the broader Indo-Pacific has introduced both opportunities and challenges. Digital platforms have revolutionised communication, enabling unprecedented connectivity and economic growth. However, they have also created vulnerabilities. Social media, for instance, has been weaponised to spread false narratives, target specific groups and influence public opinion. The rise of generative AI and deepfake technologies has further compounded these challenges, allowing foreign and domestic actors to manipulate content with unprecedented scale and sophistication

Regional organisations such as ASEAN and the Pacific Islands Forum (PIF), have recognised the urgency of addressing FIMI to differing degrees. The 2023 ASEAN's Guideline on Management of Government Information in Combating Fake News and Disinformation in the Media⁸ represent important steps, but their effectiveness is limited by the technological and political disparities among member states. Similarly, the Pacific Islands Forum has prioritised building community resilience against disinformation, although resource constraints remain a significant hurdle.

This report delves into the complexities of FIMI focusing mainly on Southeast Asia and the broader Indo-Pacific where relevant. By evaluating existing national and regional strategies, identifying emerging trends and providing actionable recommendations, the study seeks to contribute to the development of robust policies and practices in addressing FIMI. These efforts, arguably, are essential to safeguarding democratic processes, fostering societal cohesion and ensuring the resilience of one of the world's most dynamic regions.

LITERATURE REVIEW

FIMI is defined as the systematic deployment of manipulative actions in the information environment, often by foreign state or non-state actors, designed to undermine political, societal and economic stability, in pursuit of certain strategic outcomes. The conduct is mostly non-illegal in nature but threatens or has the potential to negatively impact values, procedures and political processes.⁹ FIMI

⁴ Samantha Bradshaw and Philip Howard, *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation* (Oxford Internet Institute, 2021), [online](#); Facebook, *Coordinated Inauthentic Behavior Report* (Meta, September 2020), [online](#); and Ben Nimmo, C. Shawn Eib, Léa Ronzaud, *Operation Naval Gazing*, (Graphika, September 2020), [online](#).

⁵ Bonny Lin, et.al., *Competition in the Gray Zone: Countering China's Coercion Against U.S. Allies and Partners in the Indo-Pacific*, (RAND, 2022), [online](#).

⁶ Shefali Rekhi, *Asia News Network celebrates 20th anniversary, commits to bringing region closer* (The Straits Times, 2019) [Online](#)

⁷ Ibid; Ryan LoomisHeidi Holz, *China's Efforts to Shape the Information Environment in Thailand*, (CNA, 2020), [online](#).

⁸ ASEAN Secretariat, *ASEAN Guideline on Management of Government Information in Combating Fake News and Disinformation in the Media*, (ASEAN, 2023), [online](#).

⁹ European External Action Service, *Tackling Disinformation, Foreign Information Manipulation & Interference*, (EEAS, 2024), [online](#).

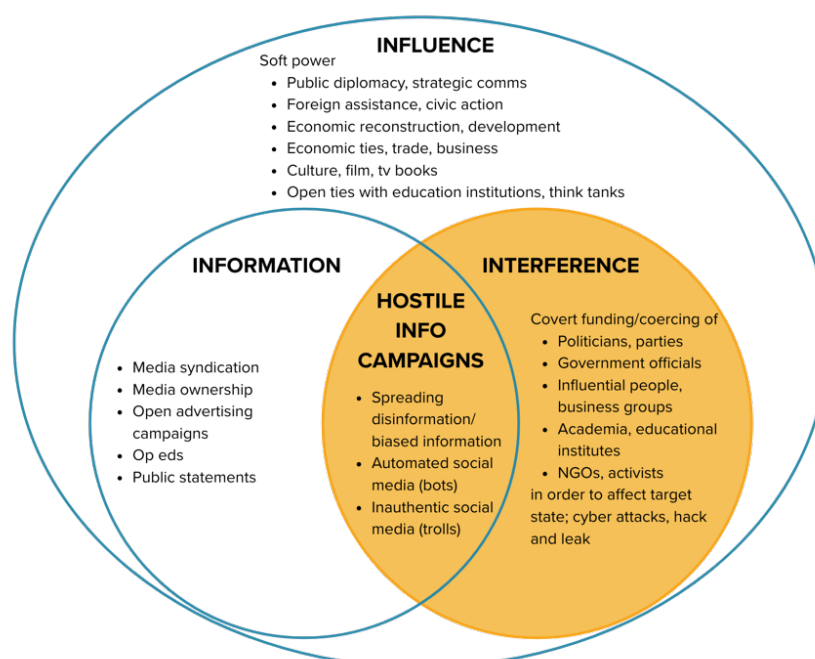
activities exploit societal and national vulnerabilities such as polarised societies, constrained media freedoms and varying digital literacy levels. In the Indo-Pacific, particularly in authoritarian-leaning nations, the term "foreign" introduces sensitivities where concepts like democracy and freedom of expression are sometimes framed as external or even intrusive ideals.

Framework

In Southeast Asia, ASEAN does not have a formal approach to FIMI (Foreign Information Manipulation and Interference). The term "foreign" itself can be contentious, as some stakeholders in the region interpret democracy and freedom of expression as Western imports. This perspective complicates discussions around disinformation, as governments may deflect scrutiny by framing information campaigns as a defense of national values rather than external influence.¹⁰ Authoritarian-leaning states, in particular, often use the ambiguity around FIMI to suppress dissent, labelling domestic opposition as foreign agents or puppets. However, a useful framework to examine foreign influence is offered by Muhammad Faizal Bin Abdul Rahman *et al.* (2020), which divides between what defines "influence", "information" and "interference", and from there defines which actions are deemed hostile.

Southeast Asian states generally accept open and transparent information flows, such as syndicated media, foreign-owned channels, advertisements, op-eds and public statements. However, they are sometimes intolerant of covert and hostile information operations aimed at deliberately disrupting politics and policies, although the responses vary across the region. These "hostile information campaigns" include tactics like covert funding, coercion and deceptive activities targeting politicians, officials, influential individuals, NGOs, academics and institutions. For instance, Singapore identifies hostile information campaigns (HICs) as a significant threat, while in Malaysia and the Philippines allegations of foreign interference in elections have been previously raised.

Figure 1: Framework for Influence, Information and Interference



Source: Muhammad Faizal Bin Abdul Rahman, Gulizar Hacıyakupoglu, Benjamin Ang, Dymples Leong, Jennifer Yang Hui, Teo Yi-Ling, "Cases of Foreign Interference in Asia", *RSIS Policy Report*, 2020, [online](#).

¹⁰ Ryan Loomis and Heidi Holz, *China's Efforts to Shape the Information Environment in Thailand*, (CNA, 2020), [online](#).

The Pacific Islands Forum (PIF) adopts a more community-focused approach, emphasising resilience through education and capacity-building initiatives. Given the limited resources and smaller digital footprints of Pacific nations, their primary concern is the spillover of geopolitical tensions, particularly between great powers, into their domestic contexts. The PIF frames disinformation as both a security and developmental challenge, highlighting the need for regional solidarity and tailored strategies. The *Boe Declaration on Regional Security* expands the concept of security to recognise the increasingly complex regional security environment driven by multifaceted challenges. It did not mention disinformation directly but noted the principle of non-interference in the domestic affairs of its members.¹¹

While both ASEAN and PIF recognise the risks posed by FIMI indirectly, their responses diverge in scale and focus, reflecting the varying political, technological and cultural landscapes across the Indo-Pacific. Addressing these gaps requires a nuanced understanding of regional priorities and the interplay between global and local dynamics, as well as political will of the countries to recognise the issue openly and respond to it.

Motives and Trends

The motives for FIMI in Southeast Asia and the greater Indo-Pacific are varied, often driven by the geopolitical and economic ambitions of the influencing actors. One key objective is shaping political landscapes by influencing elections and undermining political stability. Fragile democracies, such as Indonesia, Thailand, the Philippines¹² and Myanmar¹³, are particularly vulnerable to FIMI campaigns that exploit societal divisions and erode trust in governance systems. These operations aim to weaken democratic institutions and bolster the power of the regimes aligned with the perpetrator's interests.

Economic influence is another significant motive behind FIMI. By targeting critical industries, foreign actors can undermine regional competitors and gain economic leverage. This strategy has been observed in operations directed at Australia, Japan and Taiwan, where Chinese influence campaigns sought to weaken local industries and disrupt economic stability.

A third motive is narrative control, particularly by authoritarian regimes seeking to promote state-favoured ideologies while countering criticisms. These campaigns often involve disinformation about international relations, economic partnerships, or governance systems, with the aim of shaping public perceptions to align with the instigating actor's objectives.¹⁴

Meanwhile, we observed that in Covid-19 pandemic and after the trends in FIMI activities include a marked increase in event-driven campaigns, where activities intensify during elections, international conflicts or crises, and periods of geopolitical tension. For instance, at the start of the Russia-Ukraine War in 2022, disinformation campaigns surged across the Indo-Pacific, targeting public opinion on alliances such as NATO, AUKUS and the Quad, while also questioning the legitimacy of sanctions against Russia.¹⁵ Similarly, during the Covid-19 pandemic, state-sponsored disinformation sought to manipulate narratives about the virus's origins and vaccine efficacy, undermining trust in public health systems and

¹¹ Pacific Islands Forum, *Boe Declaration on Regional Security*, (PIF, 2018), [online](#).

¹² Jonathan Corpus Ong and Ross Tapsell, "Mitigating disinformation in Southeast Asia's elections: lessons from Indonesia, Thailand and the Philippines", *NATO Strategic Communications Centre of Excellence*, 2020, [online](#).

¹³ Reuters, "China promises aid for elections in Myanmar, junta-run media says", *Reuters*, 15 August 2024, [online](#).

¹⁴ W Lance Bennet and Steven Livingstone, "The disinformation order: Disruptive communication and the decline of democratic institutions", *European Journal of Communication*, Vol. 33, No. 2, April 2018, [online](#).

¹⁵ Rebecca Marigliano, Lynnette Hui Xian Ng and Kathleen M. Carley, "Analyzing digital propaganda and conflict rhetoric: a study on Russia's bot-driven campaigns and counter-narratives during the Ukraine crisis", *Social Network and Analysis Mining*, Vol. 14, No. 170, August 2024, [online](#).

multilateral cooperation.¹⁶ In Southeast Asia, information campaigns during the 2022 Philippines elections amplified the standing of particular candidates¹⁷ and influence voter behaviour¹⁸. In Singapore, during the 2020 General Elections, Facebook “took action against several accounts for misrepresentation as part of measures to protect the integrity of Singapore's general election” including the “Critical Spectator” page run by a Polish national in Singapore.¹⁹ In Taiwan, Chinese operations have intensified around key elections, using disinformation to undermine confidence in democratic processes and promote Beijing's preferred outcomes.²⁰ These event-driven campaigns highlight how FIMI actors exploit moments of vulnerability to destabilise societies, weaken democratic institutions, and advance geopolitical agendas.

The integration of advanced technologies is another trend. Influence actors increasingly leverage artificial intelligence (AI) and automation to create sophisticated content, including deepfakes and generative materials that shape the narratives of how candidates are perceived. The use of AI in elections in the Indo-Pacific is detected in India, Indonesia, South Korea and Taiwan.²¹ These developments in generative AI enhances the speed of which disinformation is generated and propagated, as well as the sophistication of disinformation, which complicates detection efforts.²² Additionally, foreign information influence campaigns are adopting more localised approaches, incorporating cultural and linguistic elements to resonate with specific audiences.²³ This localisation strategy increases engagement and reduces skepticism, making it easier for disinformation to spread undetected.

Spread and Reach

For this study, we categorise the spread and reach of FIMI in the Indo-Pacific region using three levels: local, national, and international issues. At the local level, disinformation often exploits community-level vulnerabilities, such as ethnic or religious divides, to incite conflict and erode social cohesion. For example, information campaigns in Indonesia have targeted existing religious tensions between the Muslim majority and other groups, given Indonesia's large Muslim population and diversity of minority religious groups.²⁴ Local level disinformation can also impact critical aspects of the national economy. For example, strategic industries such as the mining industry are often targeted by foreign information operations to influence which investors could partake in the project and gain access to supply chains

¹⁶ Steven Lloyd Wilson and Charles Wiysonge, “Social media and vaccine hesitancy”, *BMJ Global Health*, Vol. 5, No. 10, October 2020, [online](#).

¹⁷ Japhet Quitzon, “Midterm outlooks: Digital proxy warfare in the Philippines”, *CSIS Commentary*, 21 February 2025, [online](#).

¹⁸ Aries Aruguay, “Foreign Policy & Disinformation Narratives in the 2022 Philippine Election Campaign”, *ISEAS Perspective*, No. 59, 2022, [online](#).

¹⁹ Rei Kurohi, “Facebook takes down Critical Spectator page for violating its policies”, *The Straits Times*, 9 July 2020, [online](#).

²⁰ Tzu-Chieh Hung and Tzu-Wei Hung, “How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars”, *Journal of Global Security Studies*, Vol 7, Issue 4, December 2022, [online](#).

²¹ Pranshu Verma and Cat Zakrzewski, “AI deepfakes threaten to upend global elections”, *The Washington Post*, 23 April 2024, [online](#) and Council of Asian Liberals and Democrats and Friedrich Naumann Foundation for Freedom, *AI in elections in East and Southeast Asia: Opportunities, challenges, and ways forward for democrats and liberals*, Bangkok, 2024, [online](#).

²² Momina Masood, Marriam Nawaz, Khalid Mahmood Malik, Ali Javed and Aun Irtaza, “How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars”, *Arxiv*, November 2021, [online](#).

²³ Antonina Sinelnik and Dirk Hovy, “Narratives at Conflict: Computational Analysis of News Framing in Multilingual Disinformation Campaigns”, *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics*, August 2024, [online](#).

²⁴ DFRLab, “Indepth: Iranian Propaganda Network Goes Down”, *Medium*, 26 March 2019, [online](#).

and natural resources. This was allegedly the case for a refining facility in Kuantan, Malaysia which was targeted by controversy over its toxic waste management to discredit the Western investors.²⁵

At the national level, FIMI is deployed to undermine trust in government and disrupt political stability especially during elections or other major political events that can affect the political or economic trajectory of a country. Thailand has witnessed coordinated disinformation efforts targeting its election, often aimed at discrediting pro-democracy activists, endorsement of the authoritarian regime and building anti-Western sentiment.²⁶ Influence on media, be it electronic or traditional media, to sway different parts of society – academia, politics and business – was done through various ways, including partnership with state-run foreign media and pressuring student-led press.²⁷

Meanwhile, on the international level, FIMI takes on a broader geopolitical dimension, influencing public perceptions on international issues or disputes. This is exemplified in the South China Sea dispute, the issue of Taiwan independence, the Ukraine-Russia war, and the Israel and Gaza conflict, where the issues have been used for state-sponsored disinformation campaigns designed to shape regional narratives and sway public opinion in favour of specific actors. A specific case of this information operation is when Tribun Timur, Indonesian local news company shared around 8,000 videos with pro-Russian narratives on Ukraine-Russia war and images from Russian Telegram channels on its official YouTube channel between 2022-2023.²⁸ Similarly, the South China Sea dispute was targeted by operation Naval Gazing where inauthentic accounts on social media posted that the US military should not be in the Indo-Pacific, while in the Philippines information space, inauthentic accounts expressed their support for politicians with a favourable stance toward China.²⁹

Current and Emerging Responses and Mitigation Strategies for FIMI

Responses to FIMI in the Indo-Pacific region have evolved to address both immediate threats and long-term vulnerabilities. National strategies often focus on regulatory measures. Most often, the approach in countering foreign influence depends heavily on national policy. Countries that are aware of foreign influence operations would have national policies which address such activities, for example Australia and Singapore. The Australian Foreign Influence Transparency Scheme mandates disclosure of foreign affiliations in political lobbying and communication activities, providing a legal framework to curb covert influence.³⁰

Meanwhile in Southeast Asia, where not all countries are sensitive or concerned about FIMI due to a higher focus on domestic sources of disinformation, media literacy training is mostly the common approach. For example, the ASEAN Foundation, in collaboration with UNESCO and Google launched the ASEAN Digital Literacy Programme (ADLP) as an initiative to further combat misinformation and disinformation in Southeast Asia. Alphabet's Google provided a US\$1.5 million grant for the Foundation between 2022 to 2024 and has equipped more than 1,000 trainers across ASEAN countries with media and information literacy skills that will impact more than 100,000 in their network and community.³¹ Separately, Meta also conducted a fact-checking program by independent third-party fact checkers and

²⁵ Divyanshu Jindal, "An element of doubt? Rare earths targeted in disinfo campaign", *The Interpreter*, 22 July 2022, [online](#) and Jiyeong Go, "Beijing-linked influence campaign takes aim at Western investors", *FDI Intelligence*, 17 August 2022, [online](#).

²⁶ Asia Centre, *State-Sponsored Online Disinformation: Impact On Electoral Integrity In Thailand*, (Bangkok, 2023), [online](#).

²⁷ Thitinan Pongsudhirak and Thanapat Pekan, *A Global Battle of Narratives: China's Media Influence in Thailand*, Friedrich Naumann Stiftung, 6 June 2024, [online](#).

²⁸ Francesca Gentile, "Indonesian News Outlet Promotes Russian Narratives on YouTube", *Centre for Information Resilience article*, 11 December 2023, [online](#).

²⁹ Ben Nimmo, C. Shawn Eib and Léa Ronzaud, "Operation Naval Gazing", *Graphika Report*, 22 September 2022, [online](#).

³⁰ Australian Government Attorney General's Department, *Foreign Influence Transparency Scheme*, Undated, [online](#).

³¹ The ASEAN Foundation, *ASEAN Digital Literacy Programme*, 11 February 2022, [online](#).

published a report of inauthentic activities that took place on its platform.³² However, in January 2025, Meta ended its fact-checking activities to be replaced with a Community Notes approach that relies on the users to add notes to posts. Despite its limitations, as industries are mostly driven by maximising profit for their stakeholders, there are public-private partnerships that help detect foreign influence operations. The challenge with digital literacy programs, however, is that they primarily place the burden of awareness and critical thinking on information recipients, while failing to adequately address opinion leaders and influencers who play a significant role in spreading disinformation.

One solution is using emerging technology to detect, flag and stop manipulative content. The use of computational propaganda or bots in influence campaigns can be countered by automated monitoring that is created by the use of algorithms, machine learning and AI to develop warning systems for patterns indicative of coordinated information operation. An example of this is a research tool developed by Indiana University called Botometer detects the use of bots in social media.³³ Wikiedits also similarly created bots to monitor edits on Wikipedia pages.³⁴ However, using advanced technology to detect, deter and counter foreign influence has significant challenges, such as resource limitations, concerns over censorship by tech companies, and the rapid evolution of disinformation tactics may render the tool obsolete.

A 2024 report by Bateman and Jackson listed down ten interventions to address disinformation. They are (1) supporting local journalism, (2) media-literacy education, (3) fact-checking, (4) labeling social media content, (5) counter-messaging strategy, (6) cybersecurity, (7) statecraft, deterrence and disruption, (8) removing inauthentic networks, (9) reducing data collection and targeted ads, and (10) changing recommendation algorithm. Each of the interventions is then categorised by type whether it is public information, government intervention, or platform action, and subsequently weighted by three questions: How much is known about an intervention? How effective does it seem, given current knowledge? And how easy is it to implement at scale?³⁵ The comparative result is shown in the subsequent table to provide understanding of which intervention is the most significant, most effective and easiest to scale.

³² Meta, *Threat Report: The State of Influence Operations 2017-2020*, May 2021, [online](#).

³³ Onur Varol, *et.al.*, "Feature Engineering for Social Bot Detection", in Guozhu Dong and Huan Liu (eds.), *Feature Engineering for Machine Learning and Data Analytics*, (Boca Raton: CRC Press), 2018, [online](#).

³⁴ Heather Ford, Elizabeth Dubois and Cornelius Puschmann, "Keeping Ottawa Honest—One Tweet at a Time? Politicians, Journalists, Wikipedians, and Their Twitter Bots", *International Journal of Communication*, Vol. 10, 2016, pp.4891-4914, [online](#).

³⁵ Jon Bateman and Dean Jackson, "Countering Disinformation Effectively: An Evidence-Based Policy Guide", *Carnegie Endowment Report*, January 2024, [online](#).

Table 1: Disinformation Intervention Measurement

Type	Intervention	How much is known?	How effective does it seem?	How easily does it scale?
	1. Supporting local journalism	Modest	Significant	Difficult
	2. Media literacy education	Significant	Significant	Difficult
	3. Fact-checking	Significant	Modest	Modest
	4. Labeling social media content	Modest	Modest	Easy
	5. Counter-messaging strategies	Modest	Modest	Difficult
	6. Cybersecurity for elections and campaigns	Modest	Modest	Modest
	7. Statecraft, deterrence, and disruption	Modest	Limited	Modest
	8. Removing inauthentic asset networks	Limited	Modest	Modest
	9. Reducing data collection and targeted ads	Modest	Limited	Difficult
	10. Changing recommendation algorithms	Limited	Significant	Modest



Public information



Government action



Platform action

Source: Jon Bateman and Dean Jackson, "Countering Disinformation Effectively: An Evidence-Based Policy Guide", *Carnegie Endowment Report*, January 2024, [online](#).

Understanding that there are various approaches to countering disinformation – and to an extent FIMI – is the first step to finding the approach that is fit-for-context and enable multi-stakeholder collaboration. Having collaborative frameworks between government, industry and civil society could facilitate information-sharing and joint responses among regional actors. Such initiatives, coupled with sustained investment in education, technology and cross-border cooperation, are critical to mitigating the growing threat of FIMI in Southeast Asia and the broader region of Indo-Pacific.

RESEARCH QUESTION AND OBJECTIVE

This study examines how FIMI impacts democratic processes, social order, and privacy in Southeast Asia countries primarily, as well as in the wider Indo Pacific region with select countries of Australia, Taiwan, Japan, India and South Korea. Additionally, it analyses the strategies that regional and national

stakeholders have implemented to address these interferences, which include legal regulations, detection mechanisms and countermeasures. In essence, the research aims to answer how and when FIMI is applied in Southeast Asia and its neighbours, in what context and how the countries' perceive and respond to FIMI.

As Southeast Asian nations grapple with the dual challenges of democratisation and digital transformation, understanding and mitigating the effects of foreign information manipulation are crucial for safeguarding democratic values and ensuring socio-political stability in the region. This research aims to (1) enable cross-country learning on detecting and analysing the narratives, technological means and tactics of FIMI operations in Southeast Asia and its neighbours, using ASEAN as regional organisation starting point and breaching out to ASEAN's dialogue partners, such as Australia, South Korea, India and Japan, with addition of Taiwan; as well as (2) provide of actionable policy recommendations to respond to state-sponsored disinformation campaigns and information operations conducted by foreign actors through national and regional, sustained multi-stakeholder approach.

To improve regional and national strategies against disinformation in Southeast Asia, the research aims to achieve several key objectives. Firstly, it seeks to identify the technological means and methods that threat actors use in their FIMI operations in the region and beyond, along with their intended effects. This includes comparing the effects and tactics of FIMI operations before and after the development of technologies such as generative AI. Additionally, this research draws on existing lessons learned on FIMI and disinformation campaigns within the broader Indo-Pacific context and compares their effects and tactics in selected Indo-Pacific states and Southeast Asia. Another objective is to analyse the specific impacts of FIMI on Southeast Asia and to identify current practices employed by Southeast Asian governments and civil society organisations to address these incidents. To conclude, the research provides recommendations on the strategies to counter FIMI in Southeast Asia.

METHODOLOGY

The research employs a qualitative methodology to comprehensively explore FIMI in Southeast Asia and several countries in the Indo-Pacific – Australia, Taiwan, Japan, India and South Korea. This approach will encompass several data collection methods, including document analysis, content analysis, interviews, and focus group discussion. Document analysis will involve a systematic review of relevant government regulations, academic papers, and official documents to contextualise existing knowledge and policies related to FIMI. Content analysis will be conducted on media and online platforms to identify prevalent narratives, disinformation patterns, and the means through which these are disseminated. The contents that are analysed are collected mainly from content posted on traditional and digital media, as well as from content reports that have been published by social media platforms.

In-depth interviews with key stakeholders such as government officials, policy experts, journalists, and representatives from civil society organisations, governments and regional organisations from Southeast Asia is done to provide nuanced insights into the strategies and experiences of those directly involved in detecting and countering FIMI. Focus group discussion is organised in Jakarta as the location of the ASEAN Secretariat to facilitate a broader exchange of ideas among stakeholders from the region, as well as the regional organisation, allowing for the identification of common challenges and potential collaborative solutions.

The research scope focuses on 11 countries within Southeast Asia (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Timor-Leste and Vietnam), with comparative insights drawn from Taiwan, Japan, South Korea, India and Australia to highlight practices and lessons learned from relatively mature countries in addressing FIMI, as they have been the target of large disinformation operations compared to other countries in Indo-Pacific. Empirical analysis will be

conducted to identify and compare patterns and trends in information manipulation, with an emphasis on understanding the methods employed by threat actors. This comprehensive qualitative approach aims to provide a detailed understanding of FIMI's impact on Southeast Asia and develop actionable recommendations to enhance regional resilience against such threats.

The research examines the legislation readiness of countries in Southeast Asia, as well as the regional framework maturity to observe FIMI, engaging experts, governments and policy makers. Subsequently, the research engages actors beyond government to provide solutions beyond national legislation and legal approach to disinformation, but also through advocacy, research, fact-checking, and public education. The methodology for this study is done through literature review and stock taking on publicly available information and analysis of FIMI or information operations, as well as expert forum and peer reviews. The qualitative data collected are narratives of foreign information manipulation, as well as regional experts interviews and comments. Additionally, quantitative data measured are the number of accounts that FIMI or information operations take place in Southeast Asia and its adjacent neighbours are revealed to the public through news articles and threats analysis reports. The study runs for two years between 2024 to 2025, with incident data observed for the span of 2019 to 2024. The conceptualisation and data collection for this study took place between March to October 2024. Focus group discussion with academics and experts working on the space of information influence and media is done in November 2024, while gaining feedback for the writing of the report is done in February 2025.

FIMI TRENDS 2019-2024 AND ANALYSIS

Data Collection Guidances

To better understand and counter foreign information manipulation and interference, the FIMI Database employs a structured classification system. It identifies three primary categories of FIMI incidents based on the platforms or methods through which influence is exerted:

1. Traditional Media Influence

This category refers to information manipulation conducted through established, traditional media platforms such as newspapers, television, or radio. Such influence often leverages the credibility and reach of these outlets to shape public opinion. Examples include:

- An influence actor publishing opinion pieces in local media to promote a specific narrative.
- The strategic placement of advertisements in traditional media by foreign actors to subtly introduce influence.

Traditional media remains a significant tool for manipulation, especially in regions where traditional outlets continue to be a trusted source of news and information.

2. Digital Media Influence

The second category encompasses activities conducted on digital or social media platforms, which have become critical battlegrounds for information influence due to their widespread accessibility and rapid dissemination capabilities. Examples of tactics used in this category include:

- The creation of bot networks by influence actors to amplify particular narratives or disinformation campaigns.

- Setting up fake or manipulated social media accounts to share and promote misleading stories, often targeting specific communities or demographics.

This category reflects the adaptability of foreign actors to exploit digital platforms' interconnected nature, making it increasingly difficult to trace the origins and motivations of such campaigns.

3. Offline Influence

The third category captures influence exerted outside of media platforms, focusing instead on actions that directly target economic, social, or political structures. Examples include:

- Economic or investment-based influence, where foreign actors use financial leverage to sway public policies or opinions.
- Manipulation through migrant or diaspora communities, leveraging their networks and cultural ties to influence discourse in their home or host countries.
- Diplomatic efforts aimed at shaping perceptions, often through formal or informal engagement with political or societal leaders.

This category highlights the broader scope of FIMI, which extends beyond digital or traditional media to include direct interventions in societal and political dynamics.

Data collected into the FIMI database through a streamlined process designed to ensure accuracy and consistency. Each incident requires documentation of specific factors to facilitate meaningful analysis and trend identification. The database focuses on incidents occurring between 2019 and 2024, noting the time, actor behind the action, country targeted, content of the information influence and what is the narrative.

The classification begins by identifying the date of the incident within the specified timeframe. Each incident is then categorised under one of three primary categories: Traditional Media Influence, Digital Media Influence, or Offline Influence. To provide greater specificity, subcategories such as Diplomatic Influence, Migrant Influence, Paid Buzzer campaigns, or Media Opinion Pieces are assigned based on the nature of the activity.

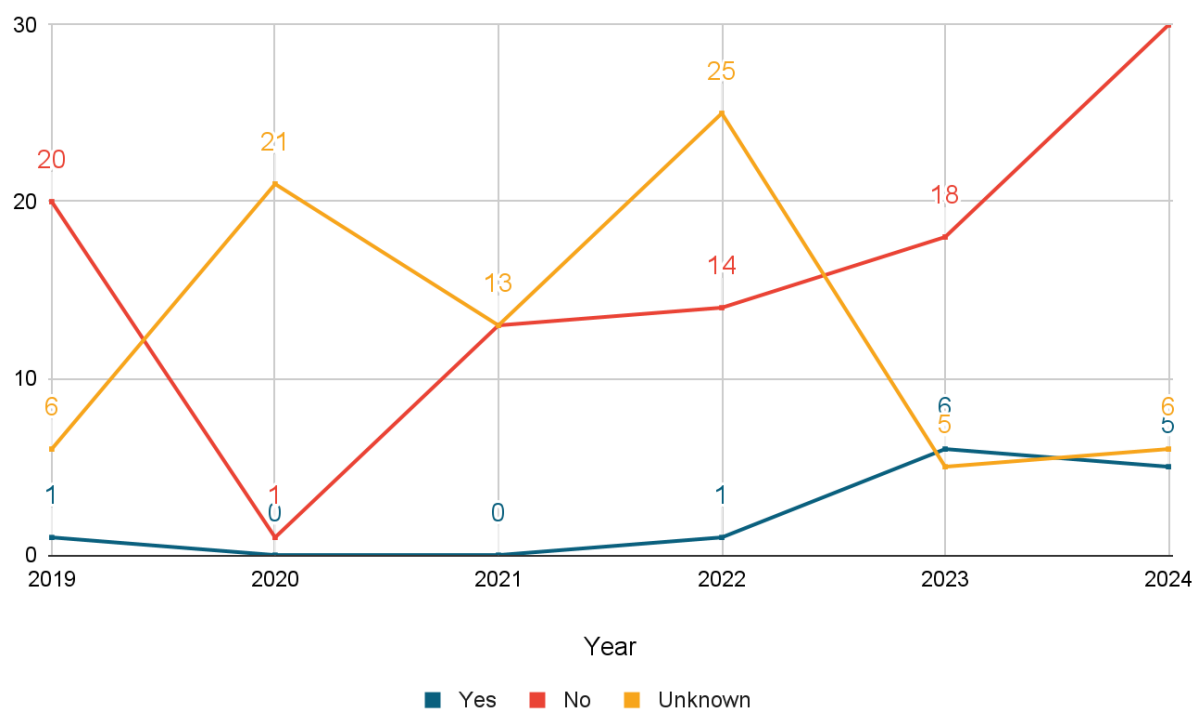
The target country is recorded to map the geographical focus of the influence, while the country of origin of the influence actor is noted whenever possible. This helps contextualise the dynamics of foreign interference. If the origin of the actor remains uncertain, this detail can be left blank, though any supporting evidence should be included to provide context.

A key aspect of classification involves determining whether the incident utilised artificial intelligence, such as bots, deepfakes, or AI-generated content. Identifying AI use is essential for understanding the evolving nature of influence operations. Additionally, the scope of the influence topic—local, national or international—is noted to indicate the intended reach and scale of the operation. Our research findings up to December 2024 have identified cases where AI tools were employed to produce disinformation and influence elections—for example, a voice message purportedly from the late Indonesian President Soeharto directing voters towards a particular party.³⁶ However, our data indicate that the use of AI in foreign influence remains relatively minimal, accounting for under 10% of the cases tracked. Overall, while the dominant perception remains that AI is not widely used in disinformation and foreign influence, the increasing “yes” responses in later years and the persistent

³⁶ Chris Barrett and Karuni Rompies, “Deepfake dictator Suharto takes Indonesia back to the future before election”, *The Sydney Morning Herald*, 12 January 2024, [online](#).

uncertainty indicate an evolving landscape that warrants further investigation and clearer evidence. Moreover, despite the high virality of disinformation material generated with AI, its hype tends to be short-lived.

Figure 2: The use of AI in disinformation and foreign influence in Southeast Asia, Australia and Taiwan



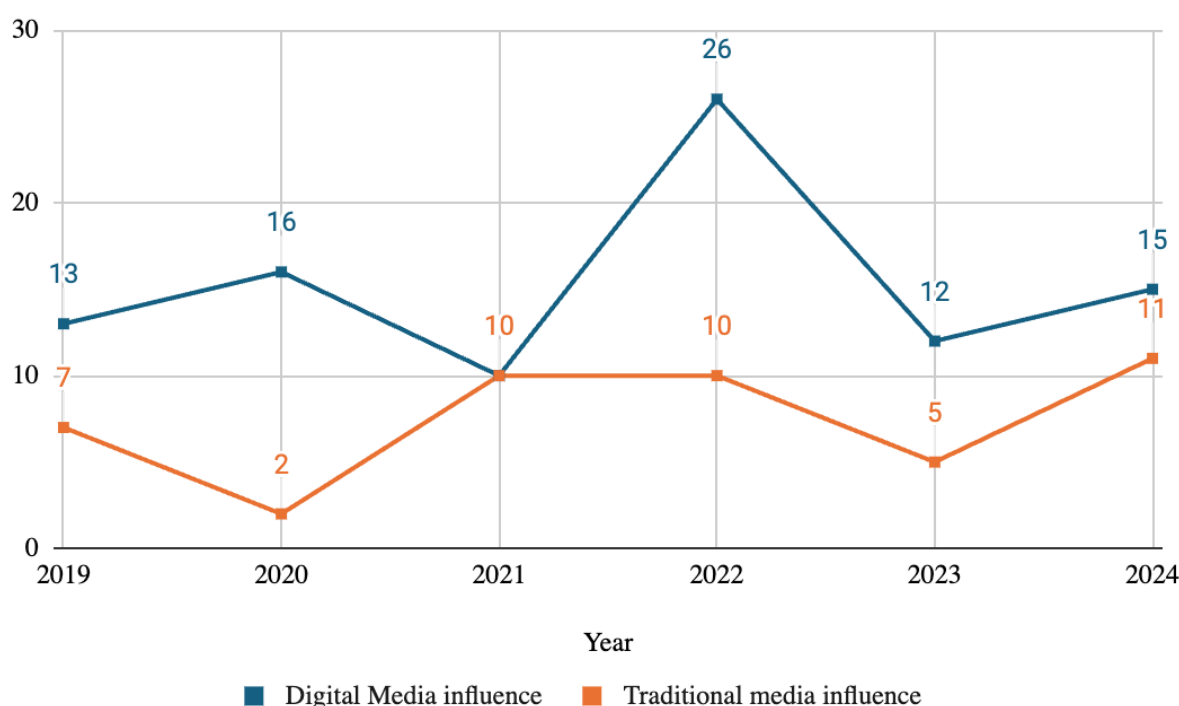
The impact of the incident is another crucial factor, documenting the effects on public opinion, policy, or other areas. If the impact is unreported or unclear, it can be classified as unknown to ensure consistency. The source of information, such as news articles, platform threat reports, or research papers, is also recorded to validate and contextualise the incident. Lastly, a brief description summarises the key details, highlighting the actors involved, methods used, and objectives pursued.

By capturing these elements, the FIMI database provides a comprehensive tool for analysing foreign information manipulation and interference. This structured approach supports efforts to understand the strategies and impacts of influence operations, enabling more effective responses to counter these threats.

Key Trends

From 2019 to 2024, information influence campaigns targeting Southeast Asia showcased distinct shifts in strategies across digital, offline, and traditional media platforms. These changes reflect the evolution of disinformation tactics and the adaptation of influence actors to emerging trends and regional dynamics.

Figure 3: Influence operation based on category of media



- From our data, digital media influence was the dominant method during the earlier years, with 13 and 16 incidents recorded in both 2019 and 2020. This reflects the heavy reliance on social media platforms and digital networks to disseminate propaganda, misinformation, and disinformation narratives. However, activity sharply dropped to 10 incidents in 2021, suggesting either improved regional efforts to counter online campaigns or a temporary shift in focus by influence actors. The trend resurged dramatically in 2022, with 26 recorded incidents, marking the peak for digital campaigns. This spike coincided with global events such as the Russia-Ukraine war, where online platforms were heavily exploited to amplify narratives. By 2023 and 2024, digital influence campaigns range at 12 and 15 each year, indicating a steady but reduced level of activity as actors diversified their methods.
- Traditional media influence, such as through newspapers, television, and radio, was less prevalent overall but showed notable fluctuations. In 2019 and 2020, only 2 incidents were recorded each year, reflecting a relatively low reliance on legacy media. This method gained prominence in 2021 and 2022, with 10 incidents in both years, as influence actors sought to leverage the credibility and reach of traditional media platforms to disseminate narratives. By 2023, the use of traditional media influence declined slightly to 5 incidents, possibly due to the increasing dominance of digital platforms and shifting consumption habits in the region. In 2024, the gap of incidents in both categories narrowed, showing that traditional media might be regaining its relevance.

Meanwhile, based on the influence actors for 2019 to 2024, China remained the most active influence actor throughout the period, consistently engaging in a significant number of activities. Its influence peaked in 2024, with 26 recorded incidents, marking a renewed focus on the region's strategic importance. This steady involvement aligns with China's growing influence in the South China Sea and its economic and political ties across Southeast Asia. Peaks in activity, such as in 2021 (24 incidents) and 2024, suggest targeted campaigns during moments of heightened regional scrutiny.

Russia, while initially dormant, experienced a sharp surge in influence activities in 2022, with 12 recorded incidents. This spike coincided with the global focus on the Russia-Ukraine war, highlighting attempts to shape narratives in Southeast Asia, likely through disinformation and propaganda. However, its activities diminished sharply in subsequent years, reflecting a reduced focus or capability in the region.

The United States maintained a minimal presence in the region's influence campaigns, with sporadic activity observed only in 2019, 2020, and a slight increase in 2024 (3 incidents). This suggests a more targeted and less persistent approach, possibly aimed at countering other actors' narratives during key moments.

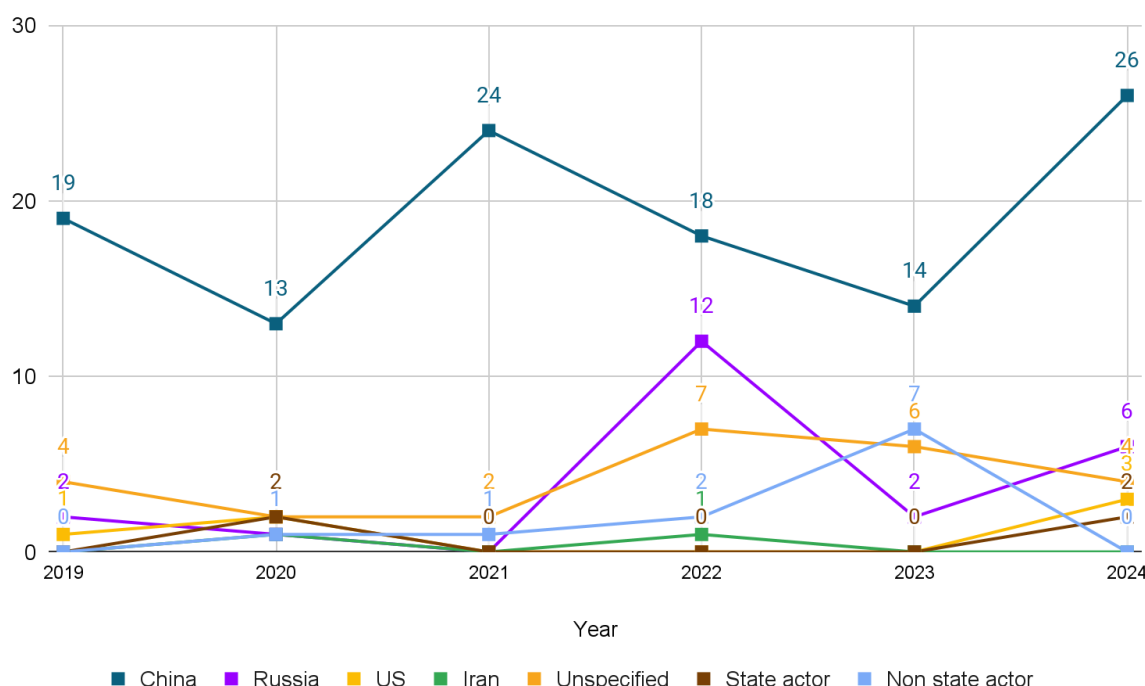
Non-state actors, representing independent or decentralized groups, became increasingly active, peaking in 2023 with 6 recorded incidents. This rise likely reflects the growing influence of non-state entities, such as cyber activist groups or ideological movements, exploiting digital platforms to amplify their messages.

Unspecified actors—those whose origins or affiliations could not be clearly determined—remained a consistent presence throughout the years. Their activities peaked in 2022 (7 incidents) and 2023 (6 incidents), indicating the growing complexity of tracing influence campaigns and the sophistication of these operations.

State-sponsored campaigns, distinct from the activities of specific nations like China or Russia, appeared only in 2024, with 3 incidents. This emergence highlights the increasing involvement of smaller or regional powers attempting to exert influence in Southeast Asia through state-backed operations. Meanwhile, Iran's activity was negligible, with only one recorded incident in 2022, suggesting limited interest or capacity in the region.

The overall trend shows fluctuating activity levels, with an initial rise from 2019 (21 incidents) to 2021 (20 incidents), followed by a significant spike in 2022 (40 incidents). The year 2022 likely served as a turning point, driven by the global impact of the Russia-Ukraine war, heightened regional competition and an increase in digital disinformation campaigns. Activity levels gradually decreased in subsequent years, settling at 29 incidents by 2024. This decline may reflect improved regional resilience against foreign influence or a shift in focus by major actors to other geopolitical hotspots.

Figure 4: Influence operation based on actors



The data underscores how key events, such as conflicts, elections, health crisis and major economic developments, drive the intensity and nature of foreign influence campaigns. China’s persistent focus, Russia’s opportunistic surge, and the growing role of non-state actors illustrate the diverse strategies employed by influence actors to achieve their goals in Southeast Asia. Meanwhile, the presence of unspecified actors and emerging state-sponsored campaigns highlights the region’s complexity as a theatre for influence and disinformation activities.

Major Timelines

Based on the statistics, foreign influence campaigns often coincide with major international, national and local events, leveraging disinformation to exploit tensions, conflicts or socio-political changes. On the international front, the South China Sea has been a recurring focal point, with significant disinformation campaigns observed in 2016, targeting Taiwan amid disputes over territorial claims and international rulings.³⁷ By 2018, The Philippines and Indonesia became key targets, as their positions on the issue gained international attention. Similarly, the Russia-Ukraine War in 2022 fueled widespread narratives globally, polarising opinions and aligning Southeast Asian actors with competing geopolitical blocs. The Israel-Gaza War in late 2023 further exacerbated social divisions within Southeast Asian countries, particularly those having a large Muslim population, where disinformation was used to exploit religious and political sensitivities.

Humanitarian crises have also been exploited. The Rohingya crisis, a longstanding issue, saw waves of disinformation during key moments, such as 2012 and 2017 in Myanmar, where narratives targeted the

³⁷ Julia Voo, “Chapter 5: Driving Wedges: China’s Disinformation Campaigns in the Asia-Pacific”, IISS Asia-Pacific Regional Security Assessment 2024, May 2024, [online](#).

ethnic minority. This expanded to Malaysia and Thailand in 2020,³⁸ as these countries dealt with refugee influxes, and to Indonesia in February 2024, focusing on migration and human rights.³⁹ Similarly, the Uyghur crisis in 2020 became a region-wide issue, with disinformation targeting audiences in the Philippines, Malaysia, Indonesia, Thailand, and even less affected countries like Laos, Cambodia, Myanmar, Vietnam, and Singapore.⁴⁰ These campaigns often highlighted human rights abuses while intertwining them with geopolitical narratives linked to China's policies.

National events, particularly elections, have consistently been a catalyst for foreign influence campaigns for certain countries. The 2019 Philippine elections marked a significant period of disinformation, targeting political rivalries. In 2020, Myanmar and Singapore experienced similar challenges as foreign actors sought to influence their democratic processes. By 2023, Malaysia, Thailand, and Cambodia became focal points, reflecting the growing importance of these elections in shaping regional geopolitics. The 2024 election year intensified disinformation efforts in Indonesia, Vietnam, Taiwan, Brunei Darussalam, and Australia, where leadership transitions and policy shifts were at stake, although the sources of disinformation differed across countries.

Separatism also remains a critical topic exploited by disinformation campaigns. Between 2018 and 2021, Indonesia's Papua region saw narratives amplifying separatist sentiments,⁴¹ while 2021 saw Aceh emerge as another hotspot.⁴² In 2023, Thailand's Pattani region⁴³ and the Philippines' Mindanao⁴⁴ faced similar disinformation aimed at heightening tensions and questioning national unity. Themes of terrorism and radicalism have further persisted, with campaigns amplifying fears and narratives aligned with global and national security concerns.

Localised issues such as mining, migration, and land rights also feature prominently in disinformation efforts. In resource-rich areas, foreign actors have targeted narratives surrounding mining activities, often linking them to exploitation or environmental degradation. Migration narratives have been used to deepen social divides, particularly around refugee movements and border tensions, as seen in the Rohingya and Uyghur crises. Meanwhile, land rights disputes involving indigenous populations have become another avenue for manipulation, especially where foreign investments or development projects are involved.

This pattern reveals how foreign influence campaigns are not random but rather strategically aligned with significant events. By exploiting international conflicts, national elections, and local socio-economic issues, these campaigns aim to sow division, polarise societies, and influence public opinion to achieve geopolitical or economic objectives.

³⁸ Nadhirah Zainal Rashid and Mohd Irwan Syazli Saidin, “‘#SayNoToRohingya’: a critical study on Malaysians’ amplified resentment towards Rohingya refugees on Twitter during the 2020 COVID-19 crisis”, *The Commonwealth Journal of International Affairs and Policy Studies* Vol. 112, No. 4, 2023, [online](#).

³⁹ United Nations Sustainable Development Group (UNSDG), “Rising Above Hate: Indonesia tackles disinformation against Rohingya refugees”, 29 February 2024, [online](#).

⁴⁰ Uyghur Human Rights Project (UHRP), *The Happiest Muslims in the World’: Disinformation, Propaganda, and the Uyghur Crisis*, July 2020, [online](#).

⁴¹ Dave Mcrae, Maria Del Mar Quiroga, Daniel Russo-Batterham, and Kim Doyle, “A pro-government disinformation campaign on Indonesia Papua”, *Harvard Kennedy School Misinformation*, 2022, [online](#).

⁴² Indonesia's Ministry of Digital Communications, “[Disinformasi] Aceh Kembali Meminta Kemerdekaan”, 15 Januari 2021, [online](#).

⁴³ Robert Lansing Institute, “Insurgency risks increase in Southern Thailand after election”, 14 June 2023, [online](#).

⁴⁴ Rappler, “FACT CHECK: Mindanao remains part of the Philippines”, 9 February 2024, [online](#).

COUNTRIES' APPROACHES TO ADDRESSING FIMI

Brunei Darussalam

FIMI is not as prevalent in Brunei—disinformation is mostly produced by domestic actors compared to foreign actors.⁴⁵ This might stem from the absence of an election cycle for foreign countries to take advantage of. However, mis- and disinformation in Brunei occurred during the height of Covid-19 pandemic where people questioned the efficacy and even leveraged religious aspects on whether or not the Covid-19 vaccine was halal. The misinformation was also circulated through an encrypted private messaging app, Whatsapp. In May 2024, Brunei's first non-profit think tank the the Gaia Alliance conducted a study on misinformation trends in Brunei and released the finding in a report titled *Digital Distortions: Building a Wise Nation to Become Resilient against Misinformation* funded by the Australian embassy that aims to enhance a more whole-of-nation approach and stronger cross-sectoral collaboration. This includes media literacy in education curriculum, improved centralised public service systems, standardisation of journalism ethics, and the provision of media literacy to all levels of society.

Meanwhile, Brunei's Sedition Act and Public Order Act are key laws that, while not specifically designed for FIMI, are often used to regulate disinformation, particularly if it is deemed to threaten the monarchy or national unity.⁴⁶ Brunei has a highly controlled media environment, and any foreign interference or disinformation is swiftly dealt with by the authorities. The country has less exposure to FIMI compared to its neighbours due to its smaller digital landscape and stringent media control.

Cambodia

Cambodia's approach to FIMI primarily involves the use of broad legal frameworks, such as the Telecommunications Law of 2015 and Prakas on Website and Social Media Control.⁴⁷ These laws grant authorities extensive powers to monitor and control online communications, ostensibly to maintain public order and national security. Critics argue that these regulations are used to stifle opposition voices and independent media, with concerns about foreign actors often serving as a pretext for tightening control over the digital space.

Cambodia's Telecommunications Law of 2015 and the Prakas on Website and Social Media Control are the primary legal frameworks used to address FIMI. These laws grant the government extensive powers to monitor and control online communications. The Ministry of Posts and Telecommunications plays a key role in regulating internet activity. Cambodia has been accused of using these laws to suppress opposition voices and independent media, under the guise of preventing foreign influence and disinformation.⁴⁸

The Criminal Code of Cambodia also consists of provisions on false information, such as Article 425 and Article 448. Article 448 stated that the act of supplying false information to a foreign state with an intention to damage the national defense can be subjected to imprisonment from two to five years and a fine from four million to ten million Riels.⁴⁹

⁴⁵ Focus Group Discussion (FGD), November 2024.

⁴⁶ Brunei's Sedition Act (Chapter 24), [online](#); Public Order Act (Chapter 148), [online](#).

⁴⁷ United Nations Human Rights Office of the High Commissioner, *State of Press Freedom in Cambodia*, August 2022, [online](#).

⁴⁸ Human Rights Watch, *Cambodia: Internet Censorship, Control Expanded*, 18 February 2021, [online](#).

⁴⁹ Criminal Code of Cambodia, [online](#).

Indonesia

Indonesia's media landscape, marked by a high level of social media engagement, makes it vulnerable to FIMI, and the government has been especially vigilant during election cycles to combat foreign influence on political discourse.

Indonesia addresses FIMI through its Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law). The ITE Law regulates online activities, imposing criminal sanctions on those found guilty of spreading disinformation, particularly via social media platforms. Amendments made in 2016 and in 2024 strengthened its focus on combating hate speech, false news, and other harmful online content.⁵⁰ The Ministry of Communication and Information Technology oversees its enforcement. The government has also worked with social media companies to control the spread of disinformation, particularly during election periods and in relation to sensitive topics like ethnic relations and political unrest.

In February 2025, the Ministry of Digital Communications will enforce the Ministerial Decree No. 522/2024, as the derivative law of ITE. It imposes administrative fines to digital platforms unable to fulfill the government's request to take down illegal contents. However, the enforcement will prioritize several types of content deemed as illegal, such as pornography, gambling, and illegal loans—while disinformation and fake news are not included.

Aside from the regulation approach, fact-checking and media and information literacy also serve as two "remedies" to debunk and prevent the spread of disinformation. In Indonesia, there is a notable fact-checking organisation called CekFakta that was formed by the media and journalists.

Laos

Laos witnesses strong influence by China state-media through collaboration agreements with local newspapers. China also penetrates the culture and entertainment dimension by utilising Lao-Chinese speaking influencers. Laos has limited specific laws addressing FIMI. However, the Law on Mass Media 2008 and other media regulations provide the government with broad authority to control both traditional and online media.⁵¹ The Laotian government has also worked closely with neighbouring countries, such as Vietnam, to monitor and control cross-border disinformation that may destabilise the regime.

The Lao People's Revolutionary Party has control over the media, with the government owning most of the mainstream outlets, including the national TV and radio networks. There is a law that allows foreign media to set up bureaus with the requirement that they submit their output for review by officials. The government considers natural disasters and major investment projects with countries like Thailand, Vietnam and China as subjects that should not be covered by the media.⁵² Lao is one of the countries that are affected by cybercrime and scams, and thus the government in early 2025 issued a notice to reduce the use of foreign internet connections – however the crackdown was allegedly from the pressure of Thailand that conducting raid towards Chiang Saen district in Thailand's Chiang Rai province which happens to be sharing the border with Golden Triangle Special Economic Zone in the Bokeo province of Laos.⁵³ There is also Southeast Asia regional effort to shape narrative of China's Belt Road

⁵⁰ The Ministry of Digital Communications of Indonesia, *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, [online](#).

⁵¹ Lao PDR Ministry of Information, Culture and Tourism, *Laos' Law on Mass Media 2008*, [online](#).

⁵² "Lao Media Guide", *BBC*, 18 April 2023, [online](#).

⁵³ Phontham Visapra, "Government assures no social media shutdown after panic over foreign internet restrictions", *Laotian Times*, 13 February 2025, [online](#) and "Laos' Golden Triangle SEZ tries to clean up its act, as Thailand gets tough", *The Nation*, 16 February 2025, [online](#).

Initiative in building railway between China-Laos through bringing ASEAN journalist to explore the railway and witnessed the positive impact it brings.⁵⁴

Malaysia

Malaysia does not have a specific legislative or policy framework to address FIMI. Nonetheless, there are ongoing measures to build media and information literacy in the country, including through public service announcements and capacity building programmes. The latter has grown increasingly sophisticated in recent years, with participants of these programmes being more targeted and hyperlocal, such as housewives.

While there remains to be an absence of a specific FIMI legislation, Malaysia's approach towards all digital content centres on the Communications and Multimedia Act (CMA) 1998, which gives the regulator, the Malaysian Communications and Multimedia Commission (MCMC), power to regulate and penalise the improper use of network facilities.⁵⁵ Violations of the CMA 1998 is also frequently cited as a reason for the Malaysian government's takedown requests submitted to social media platforms. Although there is no specific law on FIMI, Malaysia conducted information literacy campaign and training initiated by the government that are mostly conducted through public service announcements with hyperlocal audience, such as the housewives.⁵⁶ Additionally, Malaysia introduced the Anti-Fake News Act in 2018, though this was repealed in 2019 due to concerns about its potential misuse for political purposes.⁵⁷

In Malaysia, the notable case of influence was observed in the 2018 election where there was certain party literature that noted supporting certain candidate would mean more Chinese investment in the country and the Mandarin-language media in regularly highlighted pro-China views while silencing opponents of Beijing.⁵⁸ Unfortunately, as the 2022 observation by Freedom House, Malaysia does not have law to counter the influence directly although the use of Anti-Fake News Act was mentioned as one of the ways to counter misinformation.⁵⁹

Myanmar

The major challenges to the media landscape in Myanmar is the spread of hate speech and disinformation through social media, which has been playing a big part in the escalation of inter-ethnic and inter-religious tensions in the country.⁶⁰ Myanmar also sees an intersection between digital and fintech threats. In the aftermath of Covid-19, many Myanmar population resorts to game centers that are connected to gambling apps from foreign countries such as Macau and Hong Kong.⁶¹

Myanmar's response to FIMI has been largely reactionary, especially following the Rohingya crisis, where social media disinformation played a significant role in fueling violence. The Telecommunications Law 2013 and Electronic Transactions Law 2004 provide the government with some tools to address FIMI. However, these laws have been criticised for being used to target journalists and activists, rather

⁵⁴ "ASEAN journalists and influencers explore China-Laos Railway", *China Daily*, 8 July 2024, [online](#) and [online](#).

⁵⁵ Article19, *Malaysia: The Communications and Multimedia Act 1998 Legal Analysis*, February 2017, [online](#).

⁵⁶ Focus Group Discussion (FGD), November 2024.

⁵⁷ Human Rights Foundation, *Press Release: Malaysia Uses Anti-Fake News Law to Target Political Opponents*, 8 May 2018, [online](#).

⁵⁸ Joshua Kurlantzick, "China's Influence Tactics in Malaysia—Failure Now, Failure Forever?", *Council of Foreign Relations*, 3 March 2023, [online](#).

⁵⁹ Freedom House Report, "Malaysia", *Beijing Global Media Influence*, 2022, [online](#).

⁶⁰ UNESCO, *A Colorful and Diverse Media Landscape in Myanmar*, 20 April 2023, [online](#).

⁶¹ Focus Group Discussion (FGD), November 2024.

than foreign interference specifically.⁶² In January 2025, Myanmar enacted a cybersecurity law that gives legality to block websites and apps at the network level using technology sourced from China and Russia.⁶³ The law enables censorship and media monitoring, as well as limits the use of VPN.

The Philippines

Around the issue of the South China Sea dispute, a pro-Chinese media portrayed the country as an aggressor in the dispute.⁶⁴ Although there are some cases of foreign influence, the dissemination of disinformation in the Philippines is mostly dominated by domestic actors compared to foreign actors.⁶⁵ During the 2024 election campaign, electoral disinformation was also capitalised by both presidential candidates. The narratives include Duterte's assaults on the liberal democratic opposition and Marcos Jr.'s nostalgic narratives that glorified the past dictator and also his father, President Marcos.⁶⁶

The Cybercrime Prevention Act of 2012 is the primary legislation used to address FIMI in the Philippines. This law covers a wide range of online crimes, including the spread of disinformation, hacking and libel.⁶⁷ Although its primary focus is on cybercrime, this law has been invoked in cases related to disinformation. During election periods, the Commission on Elections (COMELEC), in cooperation with the National Telecommunications Commission (NTC), monitors social media for foreign-origin disinformation. The NTC also works alongside other agencies to monitor and regulate online content to mitigate foreign influence on political discourse. Additionally, the Philippines has developed partnerships with tech companies like Facebook to combat disinformation related to political campaigns and COVID-19, though the country still faces challenges due to its highly fragmented media ecosystem.

In 2025, the Senate of the Philippines filed Bill No. 2951 to set stricter penalties for foreign interference in the Philippines, including life imprisonment and fine. The scope of foreign interference covers key areas of the bureaucracy, critical infrastructures and electronic communications. This Bill also proposes the establishment of a Counter Foreign Interference Council (CFIC).⁶⁸

Singapore

The rising geopolitical tensions affect the disinformation landscape in Singapore. The Russian embassy in Singapore used social media and the Telegram messaging app to justify its action on the Russia-Ukraine war. Similarly, the Israel embassy in Singapore also appeared to be citing Qur'an to make a certain political point on the Israel-Gaza war.⁶⁹ Additionally, Chinese media influence in Singapore is quite strong due to the large mandarin-speaking population that justify the market for Chinese-language newspapers. For example, the Singaporean newspaper company Lianhe Zaobao allegedly

⁶² Human Rights Watch, "Dashed Hopes: The Criminalization of Peaceful Expression in Myanmar", 31 January 2019, [online](#).

⁶³ Associated Press, "Myanmar's military rulers enact cybersecurity law with wide-ranging censorship provisions", *APNews*, 4 January 2025, [online](#).

⁶⁴ Bernard Orr, Liz Lee, and Karen Lema,

⁶⁵ Focus Group Discussion (FGD), November 2024.

⁶⁶ Aries A. Arugay and Maria Elize H. Mendoza, "Digital Autocratisation and Electoral Disinformation in the Philippines", *ISEAS Perspective*, No. 53, 2024, [online](#).

⁶⁷ Senate Office of the Secretary of the Philippines, *Cybercrime Prevention Act of 2012*, [online](#).

⁶⁸ Senate of the Philippines, "Sen. TOL bill sets penalties for foreign interference in PH", 27 January 2025, [online](#).

⁶⁹ David Sun, "Israel embassy's post on Palestine 'unacceptable', risks undermining harmony in S'pore: Shanmugam", *The Strait Times*, 26 March 2024, [online](#).

deferred to Beijing's narratives on certain issues in order to maintain its access to China's market.⁷⁰ However, Zaobao denied this allegation and emphasised its commitment to neutrality.

Singapore has a robust legal framework to combat FIMI, with two main laws: the Foreign Interference Countermeasures Act (FICA), passed in 2021, and the Protection from Online Falsehoods and Manipulation Act (POFMA), passed in 2019. This law introduces robust measures to tackle foreign interference in domestic politics, particularly through online channels. It grants authorities the power to block or remove content deemed to be foreign interference, especially in matters relating to political campaigns and public opinion.⁷¹ POFMA, on the other hand, allows the government to issue correction orders for misleading information on social media or other online platforms.⁷² Both laws are enforced by the Ministry of Home Affairs and Ministry of Finance, reflecting the government's prioritisation of national security and public order over free expression in its regulatory approach. The most recent legal measure that the Singapore government put in place in February 2025 is the Maintenance of Racial Harmony Act. As racial issues and communalism could be exploited for foreign interference in multicultural Singapore, this new law includes safeguards to prevent race-based entities such as clan and business associations from being exploited as vectors of political influence by foreign countries.

Thailand

Thailand, along with other countries in Southeast Asia such as Vietnam, Laos, and Singapore also encounter China's penetration through the local media. These local media, both private and local, reproduce contents from Chinese media and translated in the respective countries' local languages.

Thailand's Computer Crime Act (CCA) 2007, which was amended in 2017, addresses FIMI by penalising the dissemination of false information that threatens national security.⁷³ The law grants authorities broad powers to take down content or block access to websites deemed harmful. The Ministry of Digital Economy and Society oversees the enforcement of this act. Critics argue that the law is sometimes used to stifle political opposition, especially during times of political unrest or elections, making it a double-edged sword in combating FIMI. Thailand has also made strides in addressing FIMI, particularly through the Computer Crime Act (CCA) 2007, which was amended in 2017 to broaden its scope in regulating online disinformation. The CCA targets content deemed as a threat to national security, including false information that could incite public disorder.⁷⁴ Thailand's regulatory framework allows authorities to take down or block access to online content that violates these provisions, though critics argue that it has also been used to silence dissent. The Ministry of Digital Economy and Society is primarily responsible for overseeing the implementation of the CCA.

Besides the CCA, there have been several efforts to legislate laws to regulate Thai human rights NGOs and the media in the previous administration. This was done as a means to track their financial support from foreign donors, but the legislation was pushed back by the civil society⁷⁵. The current ruling coalition party, the pro-establishment Thai United Party, plans to propose a bill to regulate foreign funding to local NGOs and media⁷⁶. The bill, called the Foreign Interference Prevention Act (FIPA), is modelled after the US's Foreign Agent Registration Act (FARA), which requires the local private sector

⁷⁰ Shibani Mahtani and Amrita Chandradas, "In Singapore, loud echoes of Beijing's positions generate anxiety", *The Wall Street Journal*, 24 July 2024, [online](#).

⁷¹ Ministry of Home Affairs Singapore, "Introduction to Foreign Interference (Countermeasures) Act (FICA)", 4 October 2021, [online](#).

⁷² Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) 2019, [online](#).

⁷³ Thailand's Ministry of Digital Economy and Society, *Thailand's Computer Crime Act of 2007*, [online](#).

⁷⁴ Janjira Sombatpoonsiri, "Labelling Fake News: The Politics of Regulating Disinformation in Thailand", *ISEAS Perspective*, No. 34, 7 April 2022, [online](#).

⁷⁵ Focus Group Discussion (FGD), November 2024.

⁷⁶ Ibid.

to declare their financial support from foreign agents to protect against foreign interference in US politics⁷⁷.

Vietnam

In Vietnam, social media such as Facebook and TikTok pages, plays an important role in amplifying the dissemination of foreign disinformation without rigorous fact-checking. Topics such as China's cooperation and close relation with the region⁷⁸ and Russian disinformation campaigns are apparent on Vietnam's media landscape.⁷⁹

There is a lot of disinformation on social media targeting Vietnamese users, including China's disinformation about the South China Sea, Russian disinformation. However, Vietnam is mostly concerned about interference from the West, which the CPV calls peaceful evolution (efforts by external forces seeking regime change without military use) via promotion of freedom of speech and other human rights. The 2018 Cybersecurity Law was passed to deal with this concern, not Chinese or Russian disinformation. Vietnam also created Task Force 47 and Cyber Command to deal with peaceful evolution.

Vietnam's Cybersecurity Law 2018 is one of the most stringent in Southeast Asia, focusing heavily on controlling foreign influence and domestic dissent. While Vietnam indeed faces disinformation from Chinese and Russian actors, this law was passed due to concerns of interference from the West instead.⁸⁰ The Communist Party refers to interference of the West as "Peaceful Evolution", and has established a military Cyber Command and a special Task Force to deal with the issue⁸¹, in addition to the Cybersecurity Law of 2018. The law requires foreign tech companies to store data locally and comply with government requests to remove content.⁸² This law requires companies operating in Vietnam to store data locally and provides the government with the authority to request content takedowns and data access from social media platforms. The government has been proactive in using this law to combat both domestic dissent and foreign disinformation campaigns, particularly those targeting the ruling party or sensitive geopolitical dynamics.

Timor Leste

Timor Leste, a relatively young democracy, is still in the process of developing comprehensive measures to address FIMI. However, the Criminal Code includes provisions that can be applied to disinformation, especially if it endangers public order or national security.⁸³ While the Criminal Code includes provisions against disinformation, the small digital footprint of Timor-Leste makes it relatively less exposed to large-scale FIMI. However, the government has collaborated with regional partners to enhance its capacity to respond to foreign interference, highlighting an emerging awareness of FIMI threats in developing countries.

The approaches to FIMI across Southeast Asia, Australia, Taiwan, and Timor Leste are varied, reflecting different political priorities and levels of exposure to foreign interference. While some countries, such as Singapore and Australia, have developed sophisticated legal frameworks to combat FIMI, others, like Timor Leste and Laos, are still building their regulatory capacity. Cooperation with social media

⁷⁷ Ibid.

⁷⁸ Ibid.

⁷⁹ Thanh Giang Nguyen, Webinar on "Sputnik News and the Russian Disinformation Campaign in Vietnam", *ISEAS*, 10 October 2024, [online](#).

⁸⁰ Focus Group Discussion (FGD), November 2024

⁸¹ Bich Tran, "Vietnam Strengthens Cyber Capabilities for Political Stability, National Defence, and Socio-economic Development", *ISEAS Perspectives*, 2024, [online](#).

⁸² Vietnam's Cybersecurity Law of 2018, [online](#).

⁸³ Penal Code of the Democratic Republic of Timor Leste, [online](#).

platforms, robust legal measures, and public awareness campaigns are emerging as key strategies in the region's efforts to address this evolving threat.

Australia

In Australia, a network originating from China launched spamouflage activities revealed in 2022 that covers narratives such as CCP critics and dissidents, harassment towards female journalists, stroke outrage around pro-Palestinian protests, and Australian domestic politics (e.g. racial segregation, Jewish plot, establishment of communism and "aborigin tax").⁸⁴ Additionally, around the same year, Dragonbridge influence campaign directed towards US, Canadian and Australian rare earths mining companies spread disinformation in Malaysia.⁸⁵

Australia's approach to FIMI is considered one of the most comprehensive in the Indo-Pacific region. Recognising the growing threats from foreign actors, particularly in relation to Chinese influence, Australia has established robust legal frameworks, strategic international partnerships, and public initiatives to combat FIMI.

- **Foreign Influence Transparency Scheme (FITS)**⁸⁶: Established in 2018, the FITS requires individuals and organisations engaging in activities on behalf of foreign principals to register with the government, ensuring transparency in foreign lobbying and influence efforts. The scheme is particularly focused on identifying and regulating foreign influence in areas like media, academia and political lobbying.
- **Espionage and Foreign Interference Act (2018)**⁸⁷: This act significantly broadens the scope of activities considered espionage and foreign interference, penalising individuals or groups engaged in covert influence operations or disinformation campaigns. The Australian Security Intelligence Organisation (ASIO) plays a key role in identifying and countering FIMI, especially during high-stakes periods like elections and public referendums. ASIO actively monitors foreign countries operations in Australia and works with other government agencies to prevent FIMI-related incidents.⁸⁸
- **International Cooperation**: Australia is a leading member of the Five Eyes Intelligence Alliance (comprising Australia, Canada, New Zealand, the United Kingdom, and the United States), which facilitates intelligence sharing on foreign interference threats. Additionally, Australia's trilateral partnerships with Japan and the United States are also instrumental in fostering a coordinated approach to information security across the Indo-Pacific.⁸⁹
- **Public awareness and media literacy initiatives**: The Australian Communications and Media Authority (ACMA) is actively involved in monitoring of misinformation and disinformation. ACMA also maintain a Register of Foreign Owners of Media Assets, which has information about foreign stakeholders owning more than 2.5% stake of Australian media and their interests in media assets.⁹⁰

⁸⁴ Focus Group Discussion (FGD), November 2024.

⁸⁵ Divyanshy Jindal, "An element of doubt? Rare earths targeted in disinfo campaign", *Lowy Institute*, 25 July 2022, [online](#).

⁸⁶ Attorney-General's Department of Australian Government. *Foreign Influence Transparency Scheme*, n/d, [online](#).

⁸⁷ Australian Federal Police, *Espionage and foreign interference*, [online](#).

⁸⁸ Chris Taylor and Linus Cohen, "The 2025 Annual Threat Assessment: ASIO makes the case for 'national' security", *Australian Strategic Policy Institute*, 20 February 2025, [online](#).

⁸⁹ U.S. Department of Defense, "Australia-Japan-United States Trilateral Defense Ministers' Meeting November 2024 Joint Statement

⁹⁰ Australia Communications and Media Authority, *Guidance notes for notification by a foreign stakeholder of interests in an Australian media company*, September 2020, [online](#).

- **Collaboration with digital platforms:** Recognising the role of digital platforms in distributing disinformation, Australia has formed partnerships with companies – Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok, Twitch and Legitimate – to flag and manage disinformation. These collaborations have been especially active during elections, with platforms required to maintain transparency around political advertisements and remove accounts identified as inauthentic behaviours trying to shape information narratives.⁹¹

India

India's approach to FIMI combines domestic regulatory measures and international cooperation. India is particularly concerned about misinformation emanating from regional rivals and addresses these concerns through legal frameworks and strategic alliances.

- **Information Technology Act (2000):** This foundational law, along with subsequent amendments, empowers the government to monitor and intercept digital communications that may threaten national security. India amended its IT rules in 2021 to further regulate social media companies and control the spread of misinformation.⁹²
- **India-Japan 2+2 Foreign and Defence Ministerial Meeting:** India collaborates with Japan on regional security issues through initiatives like the 2+2 dialogues, which enhance cooperation in cybersecurity, intelligence sharing, and countering disinformation. This partnership is pivotal for addressing FIMI in the Indo-Pacific region, as both countries share concerns about Chinese influence.⁹³
- **Public media literacy initiatives:** India has also invested in public media literacy programmes to educate citizens on identifying and managing false information. Global initiatives like the Media and Information Literacy Week that is adopted nationally are designed to bolster public awareness and resilience.⁹⁴

Japan

The Japanese government included measures against foreign influence operations in its National Security Strategy in 2022. Given its proximity to China and North Korea, both of which are often identified as sources of disinformation and influence operations, Japan has attempted to address these threats through an approach that includes robust cybersecurity strategies and alliances with global partners.

- Japan has Cybersecurity Strategic Headquarters that coordinates national cybersecurity efforts, including strategies to address disinformation and safeguard critical information infrastructure.⁹⁵ This agency has implemented various cyber initiatives to monitor and defend against FIMI. The 2021 Cybersecurity Strategic explicitly highlights the importance of countering information warfare and stresses collaboration with allies.
- International alliances: Japan works closely with the United States and South Korea under the American–Japanese–Korean trilateral pact to combat FIMI through information sharing and

⁹¹ Meta, "Submission on draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023", August 2023, [online](#).

⁹² Ministry of Law, Justice, and Company Affairs, The Information Technology Act No. 1 of 2000, [online](#).

⁹³ Ministry of Foreign Affairs of Japan, "Joint Statement Third Japan-India 2+2 Foreign and Defence Ministerial Meeting", 20 August 2024, [online](#).

⁹⁴ UNESCO, *Global Media and Information Literacy Week 2024 - Celebrations around the world*, 13 November 2024, [online](#).

⁹⁵ The Government of Japan, "Cybersecurity Strategy", 28 September 2021, [online](#).

joint security operations. This trilateral cooperation is particularly critical given the shared regional threats posed by North Korea and China.

- **Public Awareness Campaigns:** Japan has also focused on public education to increase resilience to disinformation, ensuring citizens are aware of disinformation tactics and how to identify misleading content.

South Korea

South Korea's response to FIMI is rooted in both legal measures and international cooperation. With ongoing tensions on the Korean Peninsula, South Korea views FIMI as a national security issue, particularly concerning North Korean influence operations.

- **National Security Act:** South Korea's National Security Act criminalises activities deemed supportive of foreign entities, including the dissemination of false information that could destabilise the country. The law is used to monitor and counter disinformation campaigns, especially those linked to North Korea.⁹⁶
- **United States–Japanese–Korean Trilateral Pact:** Through its alliance with Japan and the United States, South Korea participates in joint military exercises and intelligence-sharing initiatives that address cybersecurity and disinformation threats. This partnership is crucial in bolstering South Korea's resilience against regional FIMI threats.⁹⁷
- **Domestic monitoring and media education:** South Korea actively monitors social media for foreign disinformation and has invested in digital literacy, especially targeting young people, to raise awareness of misinformation and disinformation tactics. This activity is mostly done by the Ministry of Science and ICT (MSIT), South Korea.⁹⁸ Media literacy education has also been incorporated into school curriculums where the guidelines and core competencies are set by the Ministry of Education.⁹⁹

Taiwan

Threat actors also appear to be exploiting and escalating domestic controversies to employ information operations. In Taiwan, the landscape of information operations revolve around several topics such as criticism of the Democratic Progressive Party, national defense and Taiwan Strait war, controversial events involving political figures, issues related to democratic process, ineffective governance, cross-strait and diplomatic relations, inevitable reunification across the strait, and US skepticism.¹⁰⁰

Taiwan faces significant FIMI threats, particularly from China, which conducts influence operations aimed at shaping Taiwan's public opinion, influencing elections, and undermining Taiwan's democratic governance. Taiwan's response to these threats is multifaceted, involving legislative action, media literacy campaigns, and international cooperation.

- **Anti-Infiltration Act (2020):** Taiwan enacted the Anti-Infiltration Act to combat foreign interference, primarily targeting Chinese influence operations. This law penalises activities such

⁹⁶ Christopher Green and Steven Denney, "Why do democratic societies tolerate undemocratic laws? Sorting public support for the National Security Act in South Korea", *Democratization*, 31(1), 113-131, 21 December 2022, [online](#).

⁹⁷ U.S. Mission Korea, *Joint Statement of Japan, the Republic of Korea, and the United States*, 15 November 2024, [online](#).

⁹⁸ Ministry of Science and ICT, "Korea to nurture one million talent to lead the digital era", *Press Release*, August 2022, [online](#).

⁹⁹ Jiwon Yoon, Hyeon-seon Jeong, and Amie Kim, "Media Literacy in South Korea", *The International Encyclopedia of Media Literacy*, 09 May 2019, [online](#).

¹⁰⁰ Focus Group Discussion (FGD), November 2024.

as accepting foreign funds, spreading disinformation on behalf of foreign governments, and participating in political campaigns funded by foreign actors. It is a direct response to rising concerns over Chinese infiltration in Taiwan's media and political landscape. The Ministry of Justice Investigation Bureau (MJIB) oversees enforcement, working closely with intelligence agencies to identify and respond to foreign influence.¹⁰¹

- **Collaborations with technology companies:** Taiwan collaborates with major social media platforms like Facebook, LINE, and Google to detect and remove disinformation, especially during election cycles. These partnerships include fact-checking initiatives and direct channels for reporting disinformation to platform administrators. For example, Facebook has partnered with Taiwan Fact-check Center since 2019 to enhance public access to accurate information and counter the spread of falsehoods.¹⁰²
- **Media Literacy and Public Awareness Campaigns:** Taiwan's government has heavily invested in media literacy education to build societal resilience against disinformation and misinformation. The Ministry of Education, in collaboration with civil society, runs programmes in schools to teach students critical thinking skills, helping them recognise and critically evaluate disinformation. Campaigns targeting the general public also aim to increase awareness about the risks associated with disinformation and misinformation.
- **International partnerships:** Taiwan collaborates closely with democratic allies, including the United States and Japan, on countering FIMI and cybersecurity.¹⁰³ Through these partnerships, Taiwan shares intelligence, engages in joint cyber exercises, and receives support for capacity building in information security. Taiwan's Digital Diplomacy Program also fosters international awareness of Taiwan's vulnerabilities and enhances collaborative efforts to counter influence operations.

The approaches to addressing foreign influence vary significantly across countries, reflecting differences in legal frameworks, regulatory priorities, and national contexts. Southeast Asian nations and their regional counterparts have adopted a mix of legislative measures, regulatory mechanisms, and collaborative efforts to counter disinformation and safeguard information integrity. These strategies often balance the need for effective intervention with considerations of free speech, national security, and public order. While some countries rely on broad legal authority to monitor and control information flows, others focus on fostering partnerships with technology companies or enhancing media literacy to build public resilience. The following table provides an overview of key legislative frameworks, approaches, and regulatory authorities responsible for addressing FIMI in various countries.

Table 2: Countries approaches to addressing FIMI

Country	Legislation/ Framework	Approach	Regulatory Authority
Brunei	Sedition Act, Public Order Act	Regulates disinformation that threatens monarchy or unity	Government of Brunei Darussalam

¹⁰¹ Ministry of Justice Investigation Bureau (MJIB), *Investigation of National Affairs*, 12 September 2022, [online](#).

¹⁰² Taiwan Fact-check Center, "How does Taiwan Fact-checking Center cooperate with Meta? Frequently asked questions answered", *Announcements and Press Releases*, 20 January 2025, [online](#).

¹⁰³ Global Taiwan Institute, "US-Taiwan Cooperation to Counter PRC Interference and Disinformation", *Global Taiwan Brief*, 12 December 2018, [online](#); Taiwan Academic Cybersecurity Center (TACC), *Deepening Taiwan-Japan Cooperation: TACC Introduces Taiwan's Cybersecurity Research Initiatives in Tokyo*, 5 August 2024, [online](#).

Cambodia	Telecommunications Law of 2015, Prakas on Website and Social Media Control	Monitors and controls online communications, citing public order concerns	Ministry of Posts and Telecommunications
	Criminal Code of Cambodia Article 425 and Article 448	Imposes imprisonment and fine	Government of Cambodia
Indonesia	Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law)	Imposes criminal sanctions on disinformation; collaborates with social media platforms	Ministry of Communication and Information Technology
Laos	Law on Mass Media 2008	Broad authority over traditional and online media; cross-border collaboration	Government of Laos
Malaysia	Communications and Multimedia Act (CMA) 1998, Anti-Fake News Act (repealed in 2019)	Regulates and penalises disinformation; empowers communications ministry	Malaysian Communications and Multimedia Commission
Myanmar	Telecommunications Law 2013, Electronic Transactions Law 2004	Reactionary response, especially post-Rohingya crisis; targeted at journalists and activists	Government of Myanmar
Philippines	Cybercrime Prevention Act of 2012	Covers online crimes, including disinformation and libel; partnerships with tech firms	Commission on Elections (COMELEC), National Telecommunications Commission (NTC)
Singapore	Foreign Interference Countermeasures Act (FICA), Protection from Online Falsehoods and Manipulation Act (POFMA)	Allows blocking or removal of foreign-influenced content; enforces correction orders	Ministry of Home Affairs, Ministry of Finance
Thailand	Computer Crime Act (CCA) 2007 (amended in 2017)	Broad powers to take down content; monitors online disinformation	Ministry of Digital Economy and Society
Vietnam	Cybersecurity Law 2018	Requires local data storage; frequent use for state security and dissent control	Government of Vietnam
Timor-Leste	Criminal Code	Basic provisions on disinformation; collaborates regionally for capacity building	Timor-Leste Ministry of Justice

Australia	Foreign Influence Transparency Scheme (FITS), Espionage and Foreign Interference Act (2018)	Transparency requirements for foreign influence; penalises covert operations	Australian Security Intelligence Organisation (ASIO), Attorney-General's Department
India	Information Technology Act (2000)	Empowers government to monitor communications; media literacy initiatives	Ministry of Electronics and Information Technology
Japan	Cybersecurity Strategy Headquarters	Coordinates national cybersecurity, counters disinformation with allies	Cybersecurity Strategy Headquarters
South Korea	National Security Act	Criminalises foreign-supportive activities; monitors social media for disinformation	Government of South Korea
Taiwan	Anti-Infiltration Act (2020)	Targets Chinese influence; penalises foreign-funded disinformation	Ministry of Justice Investigation Bureau (MJIB)

Source: Compiled by authors.

Not only legislation, there are also other initiatives to counter foreign influence including fact-checking and media literacy within the aforementioned countries. However, there are concerns of impartiality of the fact-checkers, as well as the question of scalability that is too small and too slow, lack of funding, and sustainable business model since most of these initiatives are donor-driven (e.g. Google and Meta).¹⁰⁴ The later challenges can potentially lead to the question of impartiality and criticism towards fact-checking organisations being labelled as pro-Western organisations. In the discussion, a participant raised an importance on engaging religious groups in digital literacy programs since they are equally susceptible to disinformation from their religious leaders, if not from social media. It is also worth paying more attention to explore more psychological approaches on how people accept mis- and disinformation and fact-checking results. Ideally, grouping countries together in a regional organisation may become an avenue to address these challenges.

REGIONAL ORGANISATIONS' APPROACH ON FIMI

The high penetration of internet users, coupled with the increasing usage of social media as a source of information have provided a fertile ground for FIMI. The forms of influence vary, ranging from information operations, hybrid threats, and offline influence. This section further discussed the overview of regional organisation approaches on FIMI in Southeast Asia and in the Pacific, as well as how geopolitical and domestic context shape the landscape of FIMI in the region.

¹⁰⁴ Focus Group Discussion (FGD), November 2024.

ASEAN

In Southeast Asian countries, the absence of a conceptual framework and varying understanding of FIMI can potentially threaten free speech by the government. Therefore, in response to FIMI, upholding a mix of government, bottom-up approach, and cooperation with social media companies to build information resilience at the national and regional level.

ASEAN's response to FIMI is shaped by its principles of non-interference and consensus-based decision-making, which can limit the organisation's ability to take direct action against FIMI. However, ASEAN recognises the importance of addressing information security and has taken initial steps to foster regional cooperation.

- **Cybersecurity cooperation:** ASEAN has formed the ASEAN Cybersecurity Cooperation Strategy to guide member states in tackling cyber threats and enhancing information security. This strategy involves capacity-building initiatives, joint exercises, and dialogues with ASEAN partners, including the US and Japan.¹⁰⁵
- **Public awareness and capacity building:** ASEAN's initiatives focus on capacity building and information-sharing to enhance the region's collective resilience to disinformation, rather than imposing binding regulations on member states.
- **Defence sectoral cooperation in information:** The ASEAN Defence Ministers' Meeting (ADMM) in 2021 approved the establishment of the ADMM Cybersecurity and Information Centre of Excellence (ACICE) that Singapore proposed. In its term of reference, ACICE aims to enhance multilateral cooperation against information threats such as disinformation.¹⁰⁶

At the regional level, Southeast Asian government has developed a key policy instrument known as ASEAN Guidelines on the Management of Government Information in Combating Fake News and Disinformation in 2024. The guideline underlines a whole community approach and cross-sector collaboration between the government, media, fact-checking organisations, and CSOs to combat fake news and disinformation. ASEAN's measures focus on the promotion of media literacy, promotion of information access, educational youth programs to fight against disinformation, media capacity building for journalists and media broadcasters through media exchange programs within ASEAN member states and dialogue partners such as India, Pakistan, and Turkey.¹⁰⁷

Way forward, the ASEAN Secretariat is also interested in developing policy frameworks that strengthen digital literacy and cyber-wellness. ASEAN is also working on a strategic plan and framework to minimise the effect of generative AI misuse on disinformation and misinformation.¹⁰⁸ It is also important to have more inter-agency coordination between governments in ASEAN because of the potential political and economic ramifications stemming from fake news and disinformation. In 2025, ASEAN is also planning on a symposium on disinformation and synthetic media, inviting media representatives, CSOs, think-tanks, academicians, and the government.

¹⁰⁵ Mahirah Mahusin and Hilmy Prilliadi, "Strengthening ASEAN's Cybersecurity: Collaborative Strategies for Enhanced Resilience and Regional Cooperation," ERIA Policy Brief, 2024, [online](#).

¹⁰⁶ ASEAN Secretariat, *Terms of Reference of the ADMM Cybersecurity and Information Centre of Excellence*, 2022, [online](#).

¹⁰⁷ Ministry of Communications and Informatics Republic of Indonesia, *ASEAN Guideline on Management of Government Information in Combating Fake News and Disinformation in the Media*, March 2024, [online](#).

¹⁰⁸ Focus Group Discussion (FGD), 2024.

Pacific Islands Forum (PIF)

The PIF, which includes 18 member countries and territories in the Pacific, recognises the risks associated with FIMI, particularly as external powers show increasing interest in the region. Although PIF lacks specific legislation on FIMI, its member states have started to focus on information security as a component of regional security.

- **Pacific Islands Cybersecurity and Information Security Strategy:** Recognising the vulnerability of its member states, the PIF has worked on developing a regional information security strategy. This initiative includes cybersecurity training, policy development, and public awareness campaigns to combat FIMI.
- **Regional Collaboration and Capacity Building:** The PIF emphasises collaboration among member states to enhance information resilience, with support from partners like Australia and New Zealand. Initiatives focus on building digital infrastructure, improving media literacy, and developing regulatory capacity to address foreign disinformation threats.
- **Partnerships with External Allies:** Given the strategic interest of larger nations in the Pacific, PIF has engaged with the US, Australia, and New Zealand to receive support in strengthening cyber capabilities, a critical measure given the region's limited resources for combatting FIMI.

CONCLUSION AND RECOMMENDATION

Overall, countries in Southeast Asia and in the wider region of the Indo-Pacific have differing approaches to addressing FIMI and disinformation. Their threat perceptions towards FIMI also differ - some countries in Southeast Asia such as Singapore have made deliberate policy efforts to address FIMI, while others have focused more on domestic sources of disinformation and have made little mention of FIMI. Capabilities to detect and tackle FIMI also differ across the region, as does political will to address it. In this regard, efforts to improve information resilience in Southeast Asia should be proactive rather than reactive.

First and foremost, a conceptual definition and interpretation of FIMI at both the national and regional level must be reached prior to any major policy response. As it stands, while disinformation, fake news and hoaxes have been discussed at the regional level such as in ASEAN, the concept of FIMI has received little attention and discussion. Again, this is likely due to the differing political contexts and capabilities of Southeast Asian states, leading to differing perceptions and interpretations of FIMI. The process of defining FIMI must also be inclusive of all key societal actors to ensure that any legislative approach does not devolve into censorship or lead to restrictions of democratic freedoms and freedoms of speech. A multistakeholder approach involving academia, civil society, government, and tech platforms is ideal.

Second, in the region of Southeast Asia, countries should explore new avenues of cooperation to address FIMI at the regional level through ASEAN and strengthen its existing mechanisms for dialogue and cooperation. ASEAN has several existing initiatives to improve the region's cybersecurity capabilities through capacity building and information sharing frameworks, focusing on a wide range of threats including cybercrime, cyberattacks and disinformation. These include initiatives such as the ASEAN Regional Computer Emergency Response Team (CERT), the ASEAN Cybersecurity Coordinating Committee (Cyber-CC), the ASEAN-Japan Cybersecurity Capacity Building Centre, and the ASEAN Cybercrime Operations Desk. ASEAN also released the ASEAN Guideline on Management of Government

Information in Combating Fake News and Disinformation in the Media, and established the ASEAN Task Force on Fake News.

Southeast Asian states should explore new cooperation avenues to complement these existing initiatives. To do so, ASEAN should work towards building its capacity to detect disinformation through the establishment of an early warning system for disinformation. Understanding the motives and tactics of threat actors operating in the region is also essential for being able to detect deliberate disinformation campaigns. Expanding the scope of ASEAN's cyber and digital capacity building initiatives to include training on addressing and detecting disinformation could also be a way forward. Ensuring agility and adaptability in implementing these initiatives is essential, particularly due to the rapid development of technologies such as AI, which has significant implications on how threat actors operate in the information landscape. In addition, cooperation with social media companies is crucial to bridge gaps in implementing their community standards for moderating online content, especially since these companies possess technologies, such as AI tools, that can save time and money in content moderation.

Depending on the level of trust and historical relationships, some countries might be reluctant to share information with others due to sensitivities and differences in threat perceptions. Furthermore, certain countries, because of their political and economic dependencies, may be hesitant to openly identify or attribute influence campaigns to a particular source. As such, building trust and capabilities in cyberspace amongst ASEAN member states and partners is essential in the region, so that cooperation can be done in a more transparent and efficient manner.

Overall, it would be beneficial for countries and regional organisations to adopt a strategic agenda for addressing disinformation, starting with low-hanging fruit where international cooperation is most feasible—such as combating financial scams, which are less politicised and less sensitive to domestic political dynamics—thereby paving the way for collaboration on broader disinformation issues. Our findings indicate that while each ASEAN country has its own threat perceptions regarding what constitutes interference, other Indo-Pacific countries that have been the target of information campaigns due to their border tensions are more aware and ready to address the issue because these operations are often conducted on the sidelines of diplomatic tensions and escalating geopolitical rivalries. As such, it is recommended that ASEAN countries enhance information exchange with the Indo-Pacific nations mentioned in this report to share lessons learned in addressing FIMI. This exchange could focus on identifying best practices that can be adapted to local contexts, taking into account each country's unique historical and societal conditions.



Safer Internet Lab

 saferinternetlab.org

 Jl. Tanah Abang III no 23-27
Gambir, Jakarta Pusat. 10160

Find Us On



CSIS Indonesia | Safer Internet Lab