

**RESEARCH PAPER**

# The Multi-Stakeholder Approach towards Addressing Threats of FIMI in Southeast Asia

**PANEL 3**

Regional Responses to Foreign Information Manipulation  
and Interference

## Pieter Pandie

---

Pieter Pandie is a researcher in the International Relations department at CSIS Indonesia. His research interests include Indonesian foreign and defense policy, great power relations, as well as regional security dynamics. He has a BA in Politics and International Studies and MA in International Relations - both of which he obtained from the University of Melbourne.

## Sekar Arum Jannah

---

Sekar Arum Jannah is a Research Assistant at Safer Internet Lab (SAIL) under CSIS Indonesia. Her works explore internet governance and the intersection of geopolitics dynamics and technology, observed from the national security perspective. She holds a bachelor's degree in International Relations from Universitas Diponegoro. She can be contacted at [sekar@saferinternetlab.org](mailto:sekar@saferinternetlab.org)

*This paper is circulated for discussion and feedback. The views expressed are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, CfDS, Faculty of Social and Political Sciences UGM or any other organization. The author(s) welcome comments on this version and invite you to contact them directly with any feedback or questions.*



# The Multi-Stakeholder Approach towards Addressing Threats of FIMI in Southeast Asia

Pieter Pandie, Sekar Arum Jannah

As Southeast Asia is experiencing rapid digitalisation along with its critical position in global geopolitics, the region is ripe with the risk of Foreign Information Manipulation and Interference (FIMI) and disinformation. These operations, often driven by political or financial gain, are strategically carried out in the height of major regional or international political affairs to threaten democratic processes. Given the transnational nature of such threats that transcends beyond borders, this article argues that a multi-stakeholder approach is essential to establish an internet governance model grounded on inclusivity, accountability, collaboration, and transparency in formulating regional efforts to address politically sensitive challenges such as FIMI and disinformation. This analysis will also explore how such an approach can be adapted to Southeast Asia's differing socio-political context.

Keywords: Foreign Information Manipulation and Interference (FIMI), disinformation, multi-stakeholder.



## Introduction

The rapid growth of internet usage and digitalisation in Southeast Asia and the world has coincided with the emergence of challenges such as disinformation and FIMI (Foreign Interference and Information Manipulation) in the digital sphere. The spread of misinformation and disinformation has a range of unfavourable consequences for governments and societies across the globe. These include erosion of public trust towards public or democratic institutions, civil unrest, and decision-making based on inaccurate or unscientific information. Actors who peddle in disinformation vary in motive - they may be seeking certain political gain during electoral periods or in the context of international affairs, or seeking financial gain through the use of financial scams.

In the context of FIMI, threat actors may be seeking to sow discord and drive wedges in the societies they target, often as a broader military strategy against their adversaries. Several cases may be used to illustrate this contention. Russia, for instance, has utilised tools such as social media bot farms, the creation of fake websites mimicking real media outlets and its own media platforms such as RT and Sputnik to manipulate information and interfere in the domestic socio-political affairs of countries such as Ukraine and the United States.<sup>1</sup> In Southeast Asia, the threat landscape is more diverse, but the challenges posed by FIMI are very much present as well. During the COVID-19 Pandemic, the Philippines were targeted by an influence operation conducted by the United States Military, which sought to undermine China's COVID-19 vaccine and accused China of having a deliberate role in the spread of the virus.<sup>2</sup> The operation utilised bot accounts meant to impersonate Filipinos on platforms such as X, which posted anti-China rhetoric in regards to the ongoing pandemic.<sup>3</sup> Similarly, the Philippines again, and to a lesser degree Indonesia, were also subject to a cluster of fake accounts and pages on Facebook which posted on various issues including the South China Sea as well as the George Floyd protests in the United States in a Pro-China perspective.<sup>4</sup> These examples show that not only do such influence operations already occur in the region,

---

<sup>1</sup> Kateryna Odarchenko & Elena Davlikanova (2024), "Russia's evolving information war poses a growing threat to the West," The Atlantic Council, [online](#).

<sup>2</sup> Chris Bing & Joel Schectman (2024), "Pentagon ran secret anti-vax campaign to undermine China during pandemic," Reuters, [online](#).

<sup>3</sup> Ibid.

<sup>4</sup> Ben Nimmo, C. Shaun Eib & Léa Ronzaud (2020), "Operation Naval Gazing," Graphika, [online](#).

they are also strategically targeted at shaping opinions in regards to major regional or international political affairs.<sup>5</sup>

The various consequences and motives for FIMI and disinformation notwithstanding, actors within both the public and private sector of the digital sphere have sought to address the challenges presented by it through various means. One such approach to internet governance was offered at the World Summit on the Information Society (WSIS) in Tunis in 2005, which called for a multi-stakeholder approach to internet governance, the participation of governments, civil society, the private sector, academia and international organizations is encouraged.<sup>6</sup>

What is the 'multi-stakeholder' approach? How does it apply to internet governance and in addressing challenges such as FIMI? And how does it apply to the context of Southeast Asia? This article will attempt to address these questions and offer strategic and policy-oriented considerations for Southeast Asian states for the implementation of a multi-stakeholder approach in addressing FIMI and disinformation. It is argued here that a multi-stakeholderism is essential to establish a model of internet governance that fosters inclusivity, accountability, collaboration, and transparency, all of which are particularly significant given the global reach of the internet and the cross-border consequences that digital challenges such as FIMI may bring. Involving actors relevant to the information ecosystem (e.g. government authorities, tech platforms, and civil society) help ensure a balanced approach between self-regulation in digital platforms by tech companies, legal measures enforced by government authorities, and public oversight by civil society.<sup>7</sup>

A multistakeholder approach in addressing FIMI and in internet governance more broadly differs in nature. In the context of Southeast Asia, however, differing socio-political contexts may require a multi-stakeholder approach that is tailored to the political and normative contexts of the region. In political terms, the region has diverse regimes and varying priorities in the digital and information landscape, lending itself also to varying policy approaches to governing information. From a social and technical dimension, the region also presents varying degrees of digital capabilities and digital literacy rates in society, creating diverse social and technical contexts across its states. Taken together, these factors are essential in

---

<sup>5</sup> Fitriani, Pieter Pandie & Sekar Arum Jannah (2025), "Tackling Disinformation, Foreign Information Manipulation and Interference in Southeast Asia and Broader Indo Pacific," Safer Internet Lab

<sup>6</sup> International Telecommunication Union (ITU) (2005), *Tunis Agenda for the Information Society*, [online](#).

<sup>7</sup> Beltsazar Krisetya and Ratna Aini Hadi "Defending election integrity from disinformation in Southeast Asia," Westminster Foundation for Democracy (WFD), March 2024, [online](#).

formulating a regional multi-stakeholder approach in addressing politically sensitive challenges such as FIMI and disinformation.

The following sections will attempt to elaborate on these arguments even further. First, the article will define the multi-stakeholder concept, its application in different fields including in internet governance, as well as its prospects and limitations. Second, the article will articulate the domestic and regional political context in Southeast Asia as well as the role of ASEAN as it relates to disinformation and FIMI in the digital sphere. This section will also explore how a multi-stakeholder approach to FIMI and disinformation may be pursued in the region, given the differing socio-political contexts of Southeast Asian states. Taken together, the arguments and ideas presented in this article will offer an argument for a multi-stakeholder approach to addressing FIMI and disinformation in Southeast Asia - one that is tailored to the region's specific political and normative context.

## Understanding the Multi-Stakeholder Model

The multi-stakeholder approach has become an emblematic model in contemporary internet governance, touted as an inclusive, participatory, and flexible response to the transnational challenges of the digital era. Its development was neither automatic nor uncontested. Rather, it reflects a decades-long evolution in global governance, wherein authority over rulemaking in complex, technical domains increasingly shifted away from state-dominated institutions and toward hybrid forums involving public, private, and civil society actors. This section traces the historical trajectory of the concept, examines its institutionalisation in global internet governance, explores its practical application to disinformation and foreign interference, and evaluates its core strengths and weaknesses—particularly in light of the challenges posed by Foreign Interference and Information Manipulation (FIMI).

Multi-stakeholderism in internet governance emerged in tandem with a broader global trend toward networked governance. The model was shaped not by a coherent ideological commitment to participation, but by institutional contingencies and evolving power dynamics between states and non-state actors in the management of the internet.<sup>8</sup> The term itself emerged in the 1990s in the political context of the UN World Summits and the emergence of management theory in the academic context.<sup>9</sup> For instance, the institutionalisation of new forms of collaboration between government and non-government

---

<sup>8</sup> Jeanette Hofmann (2016), "Multi-stakeholderism in Internet governance: putting a fiction into practice, *Journal of Cyber Policy*, 1:1, 29-49, DOI:10.1080/23738871.2016.1158303

<sup>9</sup> Hofmann, *Multi-stakeholderism in Internet governance*

actors at the 1992 Conference on Environment and Development is an example of the multi-stakeholder approach in practice, as a more 'participatory' model of governance was increasingly promoted.<sup>10</sup>

In the context of internet governance, the 2003 and 2005 World Summits on the Information Society (WSIS) catalysed formal debate over global internet governance. The Tunis Agenda (2005) explicitly called for the participation of all relevant stakeholders—governments, private sector, civil society, and the technical community—in policy development and implementation. This moment institutionalised the multi-stakeholder approach as a normative ideal, even as contestations over its meaning and practice persisted. Western governments and tech companies advocated for decentralised and non-governmental leadership<sup>11</sup> The resulting compromise gave rise to forums like the Internet Governance Forum (IGF), which provides a platform for dialogue without formal decision-making powers, and ICANN, which manages key internet infrastructure through a corporatised but multi-stakeholder governance model.


As such, the multi-stakeholder model was less a principled departure from traditional state-based governance than a pragmatic accommodation to the reality of transnational networks and private-sector dominance in the internet's early development.<sup>12</sup> It was also a response to legitimacy crises facing both states and corporations in their unilateral management of digital spaces. While civil society actors played a crucial role in framing the approach as an inclusive and democratic innovation, their access and influence within governance bodies have often been limited by resource constraints, opaque decision-making structures, and shifting power alliances. The practical application of the multi-stakeholder approach has been most visible in institutions such as ICANN, the IGF, and regional bodies like the Asia Pacific Regional IGF. These platforms allow for the exchange of ideas and coordination among diverse stakeholders, albeit with limited binding authority. More recently, multi-stakeholder coalitions have also been formed in response to emerging threats such as disinformation, cybercrime, and FIMI. These efforts reflect a growing recognition that the complexity of digital threats—

---

<sup>10</sup> Karin Bäckstrand (2006), "Multi-Stakeholder Partnerships for Sustainable Development: Rethinking Legitimacy, Accountability and Effectiveness." *European Environment* 16 (5): 290–306. doi: 10.1002/eet.425.

<sup>11</sup> Laura DeNardis and Mark Raymond (2013), "Thinking Clearly about Multistakeholder Internet Governance," *GigaNet: Global Internet Governance Academic Network, Annual Symposium*, [online](#).

<sup>12</sup> Hofmann, *Multi-stakeholderism in Internet governance*



characterised by transboundary reach, hybrid tactics, and rapid evolution—demands a coordinated, whole-of-society response.<sup>13</sup>

In the context of FIMI, multi-stakeholder responses have involved collaborations between states, technology firms, civil society organisations, fact-checkers, and research institutions. For instance, the European Union’s Code of Practice on Disinformation, while voluntary, brings together platforms, governments, and civil society to establish shared norms and expectations around content moderation and transparency.<sup>14</sup> Similarly, international fact-checking networks have worked across borders to debunk disinformation campaigns, especially during elections and crises such as the COVID-19 pandemic. Unlike traditional state-based security responses, which often focus narrowly on attribution and deterrence, a multi-stakeholder approach to FIMI enables a broader repertoire of responses, from narrative inoculation and public education to collaborative technical interventions. However, implementation remains uneven. While some global tech firms have adopted multi-stakeholder principles—such as through advisory boards, transparency reports, or oversight mechanisms—others continue to exercise unilateral control over content moderation. In addition, conceptual understandings of FIMI are not even across different states in Southeast Asia and beyond, particularly given the differing socio-political contexts and information ecosystems of each state.

The appeal of the multi-stakeholder approach lies in its potential to democratise governance and enhance legitimacy. First, it encourages inclusivity, allowing a broader set of actors—including those traditionally marginalised in international governance—to participate in shaping digital norms and policies. This can lead to more accountable and transparent decision-making, especially in areas like content regulation, algorithmic governance, and cybersecurity.<sup>15</sup> Second, it fosters collaboration across sectors, enabling states to access the technical expertise of private companies, the normative insights of civil society, and the lived experiences of affected communities. This multiplicity of perspectives is particularly valuable in addressing disinformation and FIMI, which operate across multiple domains—legal, technological, societal, and geopolitical. Third, the model can serve as a platform for innovation, where norms and practices are developed iteratively and through experimentation. Finally, it can enhance resilience by building networks of trust and

---

<sup>13</sup> Andrew Gibbons and Andrea Carson (2022), “What is misinformation and disinformation? Understanding multi-stakeholders’ perspectives in the Asia Pacific,” *Australian Journal of Political Science*, 57(3), 231-247, [online](#)

<sup>14</sup> European Union (2025), *Code of Conduct on Disinformation*

<sup>15</sup> Anja Mihr (2014), “Good Cyber Governance, Human Rights and Multi-stakeholder Approach,” *Georgetown Journal of International Affairs*, [online](#).



cooperation that can be mobilised in times of crisis. In addressing FIMI, this means not only detecting and removing harmful content but also strengthening societal immunity through digital literacy, media pluralism, and civic engagement.

However, despite its normative appeal, the approach is not without its limitations. First, the model often reproduces existing power asymmetries. Corporate actors, particularly global technology firms, often possess disproportionate influence within multi-stakeholder forums due to their financial resources, technical expertise, and control over key infrastructure.<sup>16</sup> This can marginalise civil society voices, and lead to governance outcomes that prioritise corporate interests over public welfare. Second, it may lack enforceability. Unlike intergovernmental treaties or national legislation, many multi-stakeholder agreements are non-binding, reliant on soft norms and voluntary commitments. This limits their ability to hold actors accountable or ensure compliance, particularly when dealing with covert or state-sponsored FIMI campaigns. Third, there is the risk of tokenism, where civil society or underrepresented stakeholders are included in name but excluded from meaningful decision-making. Participation without influence can erode trust and legitimacy, particularly when governance outcomes are perceived as opaque or predetermined.<sup>17</sup> Fourth, multi-stakeholderism can be co-opted by authoritarian regimes seeking to legitimise restrictive digital policies. By staging pseudo-consultations or selectively engaging with compliant civil society groups, states can claim participatory legitimacy while silencing dissent. Lastly, it assumes a baseline level of civic space and political freedom that does not exist in all contexts. In restrictive environments, independent civil society actors may be harassed, surveilled, or excluded entirely from governance processes. This limits the applicability of the model in regions where democratic institutions are weak or under threat.

In all, the multi-stakeholder approach represents both a response to the realities of internet governance and an aspirational model for inclusive, democratic participation. In addressing complex challenges like FIMI, it offers pathways for coordination, legitimacy, and resilience that are not easily achieved through state-centric models. However, its effectiveness depends heavily on the design of participation, the balance of power among stakeholders, and the political context in which it is implemented. As the next section will explore, these conditions vary significantly across Southeast Asia, raising critical questions about how multi-stakeholderism can be adapted to regional realities while maintaining its normative and functional promise.

---

<sup>16</sup> Hofmann, *Multi-stakeholderism in Internet governance*

<sup>17</sup> DeNardis & Raymond, *Thinking Clearly about Multistakeholder Internet Governance*

## The Multi-Stakeholder Model and FIMI in Southeast Asia

Southeast Asia presents a complex and uneven information landscape, where the growing prevalence of Foreign Interference and Information Manipulation (FIMI) intersects with diverse governance systems, civil society capacities, and regional institutional norms. The multi-stakeholder model, while attractive as a framework for inclusive and adaptive governance, cannot be transplanted wholesale into the region without adaptation. This section outlines the threat landscape of FIMI in Southeast Asia, surveys the varied responses of individual ASEAN states, and critically analyses how ASEAN's institutional architecture and prevailing political norms enable and constrain the adoption of a regionally appropriate multi-stakeholder approach.

FIMI in Southeast Asia encompasses a wide spectrum of techniques and goals, from coordinated disinformation campaigns and the creation of inauthentic accounts to platform manipulation and information laundering. Threat actors include state-affiliated operations from external powers, domestic political actors, cyber-mercenary groups, and profit-driven disinformation-for-hire networks. Their aims are multifaceted: shaping public opinion, suppressing dissent, undermining elections, sowing mistrust in institutions, and manipulating geopolitical alignments.<sup>18</sup> These threats are enabled by a number of factors, including Southeast Asia's rapid digitalisation, high rates of internet penetration, and low levels of digital literacy in some areas, among others. While social media penetration is high, at times it is not matched by corresponding investments in platform accountability or civic education. Moreover, the proliferation of encrypted messaging apps and private channels makes detection and attribution difficult. In several cases, domestic actors—whether in government or opposition—peddle in disinformation themselves, further complicating efforts at a coordinated response.<sup>19</sup> This is particularly the case during domestic election cycles, where political candidates often choose to disseminate false narratives against their rivals, or to improve upon their own image as well.

A research report by Safer Internet Lab in 2025 revealed FIMI and disinformation campaigns that are related to the rising geopolitical issues. This includes border tensions in the South China Sea involving the Philippines as one of the claimants, where China state media highlights derogatory portrayals of the Philippines. This campaign was deployed through

---

<sup>18</sup> Fitriani, Pieter Pandie & Sekar Arum Jannah, *Tackling Disinformation*

<sup>19</sup> Ibid.

multifaceted operations such as cross-posting, engaging with influencers, and involving “experts” from within and outside China to shape public opinion.<sup>20</sup> This illustrates how such operations are often an extension of physical conflict. Domestically, AI has also been utilized to generate deepfakes for political purposes such as during the 2024 Indonesian election where a manipulated video ‘resurrecting’ the former president Suharto urging the public to vote for Golkar party went viral.<sup>21</sup> In 2024, digital threats were further demonstrated through cyber threats by Brain Cipher ransomware group that targeted data center operations of local government agencies in Indonesia, along with South Africa, Philippines, Portugal, and Thailand.<sup>22</sup>

Against this backdrop, states in Southeast Asia have adopted a variety of measures to address disinformation and FIMI, reflecting their differing political systems, regulatory capacities, and normative commitments. Indonesia has taken a multipronged approach on combating misinformation and disinformation, although it has not specifically focused on FIMI. On one hand, it has pursued legal and regulatory measures through the Ministry of Communication and Information (Kominfo), invoking the Information and Electronic Transactions (ITE) Law to clamp down on false information. Additionally, civil society actors like MAFINDO have developed independent fact-checking platforms and public education initiatives. During elections, temporary collaborations between government, election committee, civil society, and tech platforms have emerged to counter coordinated disinformation, including from foreign sources. However, concerns remain about the misuse of anti-hoax laws to target dissent or alternative narratives.<sup>23</sup>

The Philippines, with its vibrant yet polarised online ecosystem, has become a focal point for the spread of online disinformation and influence operations. Election periods are events that see high rates of online disinformation in the Philippines, with political candidates often employing campaign consultants, social media influencers, parody meme accounts, and fake accounts to disseminate narratives for themselves or against their opponents.<sup>24</sup> Legal approaches to disinformation and FIMI include the Cybercrime Prevention Act of 2012, which

---

<sup>20</sup> Internews. *Nexus of Manipulation: Anatomy of Influence Operations in the Philippines*, 2024.

<sup>21</sup> Gemma Ware, “Deepfakes and disinformation swirl ahead of Indonesian election – podcast,” *The Conversation*, 12 February 2024, [online](#).

<sup>22</sup> Muhammad Faizal Abdul Rahman, “How ASEAN’s Cybersecurity Push Could Protect People and Economies,” *The Diplomat*, 18 November 2024, [online](#).

<sup>23</sup> Joshua Kurlantzick, “Southeast Asian Governments Squeeze Freedom of the Press”, *Asia Unbound - Council on Foreign Relations*, 27 January 2020 and Andrea Carson and Andrew Gibbons, “The Big Chill? How Journalists and Sources Perceive and Respond to Fake News Laws in Indonesia and Singapore”, *Journalism Studies*, 2023, Vol. 24, No. 14, pp. 1819-1838, DOI: 10.1080/1461670X.2023.2192299

<sup>24</sup> Jonathan Corpus Ong and Ross Tapsell, “Mitigating Disinformation in Southeast Asian Elections”, *NATO Strategic Communications*, 2020, [online](#).

covers a wide range of crimes including the spread of disinformation.<sup>25</sup> Singapore, on the other hand, has adopted perhaps the most institutionalised response through its Protection from Online Falsehoods and Manipulation Act (POFMA) and the Foreign Interference Countermeasures Act (FICA). FICA introduces safeguards and countermeasures to prevent, detect and disrupt foreign interference,<sup>26</sup> while POFMA allows the government to order corrections or takedowns of content deemed false.<sup>27</sup> Although, it is important to note that the legislation has been criticised by some for potentially undermining public confidence and shielding the government from criticism.<sup>28</sup> Malaysia similarly employs legislation in its Penal Code and the Communications and Multimedia Act of 1998 against disinformation.<sup>29</sup>

In many Southeast Asian countries, the risk of regulatory overreach remains high. Cambodia, Vietnam, and Brunei approach disinformation through a similar centralised lens. Government responses are primarily driven by national security concerns, with sweeping controls on online speech and extensive surveillance infrastructures.<sup>30</sup> Nonetheless, their citizens are not immune to the effects of foreign disinformation, such as from influential geopolitical actors such as China and Russia. For instance, China-linked criminal groups have been relocating their online gambling and scamming operations to Cambodia along with the Philippines, Laos, and Myanmar.<sup>31</sup> In Vietnam, a Russian-based news service made a content sharing agreement with Vietnam News Agency where it revolves on anti-Kyiv and anti-Nato propaganda.<sup>32</sup>

At the regional level, ASEAN's ability to respond to FIMI is shaped by its institutional design. While ASEAN has acknowledged disinformation and fake news as a cross-border issue in the digital sphere, it is also important to note that conceptual understandings of FIMI are not uniformly adopted across Southeast Asian states, much less at the ASEAN level. This is evident in the fact that while ASEAN has released its own guidelines on managing government information in combating fake news and disinformation in the media, it does not adopt FIMI as its own concept. The ASEAN Guideline on Management of Government

---

<sup>25</sup> Senate Office of the Secretary of the Philippines, Cybercrime Prevention Act of 2012, [online](#).

<sup>26</sup> Ministry of Home Affairs Singapore, "Introduction to Foreign Interference (Countermeasures) Act (FICA)", 4 October 2021, [online](#).

<sup>27</sup> Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) 2019, [online](#).

<sup>28</sup> Howard Lee, "Singapore's 'fake news' fixer risks undermining public confidence," East Asia Forum, 2023, [online](#).

<sup>29</sup> Fitriani, Nandita Putri Kusumawati, Pieter Pandie & Beltsazar Krisetya, "Regional and Cross-Border Responses Towards Disinformation in Southeast Asia," Safer Internet Lab, 2024, [online](#).

<sup>30</sup> Fitriani, Pieter Pandie & Sekar Arum Jannah, *Tackling Disinformation*

<sup>31</sup> U.S.-China Economic and Security Review. "China's Exploitation of Scam Centers in Southeast Asia," 18 July 2025, [https://www.uscc.gov/sites/default/files/2025-07/Chinas\\_Exploitation\\_of\\_Scam\\_Centers\\_in\\_Southeast\\_Asia.pdf](https://www.uscc.gov/sites/default/files/2025-07/Chinas_Exploitation_of_Scam_Centers_in_Southeast_Asia.pdf)

<sup>32</sup> Thanh Giang Nguyen, "Assessing the Role of Sputnik News in Propagating Anti-Ukrainian and Anti-Western Narratives in Vietnam," ISEAS Perspective No. 62, 16 August 2024, [https://www.iseas.edu.sg/wp-content/uploads/2024/07/ISEAS\\_Perspective\\_2024\\_62.pdf](https://www.iseas.edu.sg/wp-content/uploads/2024/07/ISEAS_Perspective_2024_62.pdf)

Information in Combatting Fake News and Disinformation in the Media was released for the objective of providing a framework for ASEAN governments to respond to disinformation and fake news, to ensure transparency and accountability in policy responses against disinformation, improve coordination between government agencies, and to encourage engagement with non-government entities such as civil society organisations, media outlets, and technology companies.<sup>33</sup> The Guideline also defines what is meant by disinformation in the ASEAN context, as well as safeguards, countermeasures, and what policy approaches should be prioritised in addressing disinformation and fake news. Importantly, the guidelines underline the importance of cross-sector collaboration between government, civil society, fact-checking organisations, media, and tech companies, as well as the importance of promoting media literacy, access to information, and transparency, among others.

However, core to ASEAN's identity are the principles of non-interference in domestic affairs and consensus-based decision-making.<sup>34</sup> These principles have historically enabled stability and diplomatic cohesion among its member states, particularly as ASEAN member states have diverse political systems and local contexts in their own right. Yet, these same principles also present significant limitations when confronting transnational challenges such as FIMI. First, non-interference limits ASEAN's ability to coordinate robust, binding action on issues that are considered politically sensitive. FIMI often intersects with domestic politics—such as electoral processes, sovereignty, or elite interests—rendering collective intervention diplomatically fraught. Second, ASEAN's consensus model tends to produce lowest-common-denominator outcomes, which limits the ambition and enforceability of regional initiatives. Even when states agree on the threat posed by disinformation, they differ on causes, appropriate responses, and the role of civil society. Third, ASEAN operates through informal mechanisms and weak secretariats. It lacks the supranational authority to enforce standards or ensure compliance. Given these conditions, the feasibility of a conventional multi-stakeholder approach in Southeast Asia is constrained. The unevenness of civil society development across countries, differences in approaches towards internet governance and responses to disinformation, and ASEAN's institutional architecture all limit the scope for replicating models found in other regions.

---

<sup>33</sup> ASEAN Guideline in Combatting Disinformation and Fake News in the Media, 2024.

<sup>34</sup> Taku Yukawa, "The ASEAN Way as a symbol: an analysis of discourses on the ASEAN Norms," *The Pacific Review*, 2018, 31:3, 298-314, DOI: 10.1080/09512748.2017.1371211

Yet, this does not render multi-stakeholderism irrelevant. Rather, it calls for a contextualised model. A Southeast Asian multi-stakeholder approach must be designed around these core considerations:

1. **Acknowledging Different Political Realities While Expanding Inclusion:**

Multi-stakeholder mechanisms in Southeast Asia must operate within the boundaries of state sovereignty and political acceptability. In practice, this could mean building semi-formal collaborations where civil society and academia are involved in technical working groups, capacity-building, or advisory roles—without threatening state control. In Indonesia, for example, Kominfo has intermittently collaborated with civil society organisations during crises. Such models, though limited, can be expanded into more consistent and structured partnerships.

2. **Strengthening Track 2 and Cross-Border Civil Society Networks:**

ASEAN's formal institutions may be limited, but Track 2 mechanisms—such as university networks, think tanks, and NGOs—provide viable spaces for dialogue, norm diffusion, and cross-border collaboration. Regional initiatives like the proposed Asia-Pacific Fact-Checking Coalition can serve as entry points for broader cooperation.<sup>35</sup> These networks can build regional capacity and serve as informal nodes for monitoring, education, and counter-narrative campaigns.

3. **Platform Accountability and Regional Norm Diffusion:**

While Southeast Asia lacks a binding regional regulatory authority over tech firms, regional coordination can still pressure platforms to localise their policies and engage stakeholders more meaningfully. ASEAN states can collectively push for improved transparency, greater investment in content moderation, and more engagement with regional fact-checkers. Norm diffusion—even through soft mechanisms—can set expectations and create peer pressure for corporate behaviour.

4. **Investing in Institutional Infrastructure:**

A regional body or secretariat specifically focused on information integrity—possibly within ASEAN or through an associated mechanism—could coordinate regional responses, pool resources, and support national-level actors. While such an initiative

---

<sup>35</sup> Ratna Aini Hadi & Nuril Hidayah, "Charting the Path for an Asia Pacific Regional Fact Checking Coalition," Safer Internet Lab, 2024.

may be politically sensitive, it could start as a voluntary coordination platform with rotating leadership and broad stakeholder inclusion.

The diversity and dynamism of Southeast Asia's political and information ecosystems demand a tailored and incremental approach to multi-stakeholderism. While the region's current political norms and institutional architectures pose real constraints, there are windows of opportunity for adaptation, experimentation, and norm-building. By starting with informal coalitions, governance forums, and soft mechanisms of collaboration, Southeast Asia can move toward a model of internet governance that recognises the multifaceted nature of FIMI and leverages the collective capacity of state and non-state actors. The path forward is not straightforward—but it is both necessary and possible.

## Conclusion and Recommendations

This article argues that the implementation of a multi-stakeholder model to address FIMI can be promising, yet challenging. This model offers an inclusive and flexible mechanism that allows diverse actors to engage in collective responses to enhance security resilience. Respective actors, ranging from government agencies, civil society, and local communities, have different capabilities that can be leveraged for a broader collaboration to support response and technical interventions that goes beyond traditional and state-centric approaches. Despite the appeal, the implementation of this model remains hindered by structural limitations like resource disparities (both financial and technical expertise), lack of enforceability, and risk of tokenism for underrepresented stakeholders.

Taken to the specific context of Southeast Asia, national measures to FIMI and disinformation vary. Countries such as Indonesia, Philippines, and Malaysia, have fostered collaboration between the government and NGOs, while Cambodia, Vietnam, and Brunei have a more centralised approach. While national measures are important, this should be complemented by broader regional efforts by recognizing FIMI as a security concern within ASEAN's agenda. However, ASEAN, which is deeply entrenched in its non-interference and consensus-based decision-making principles, can potentially hinder its adaptability to form a collective response to address politically sensitive issues such as FIMI. Therefore, the adoption of multi-stakeholder approach and to what extent in which such approach is accepted, very much depend on both the domestic openness of the member states and regional norms.


Based on these findings, the following recommendations outline how a multi-stakeholder approach can be built to address FIMI and disinformation in Southeast Asia through ASEAN.

**First**, facilitate FIMI dialogues through the existing mechanisms in ASEAN. For instance, the ASEAN Digital Ministers' Meeting (ADGMIN) or ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN) can serve as an avenue to incorporate emerging digital threats, such as FIMI, to its regional agenda. Beginning strategic dialogues and setting norms and standards in regards to FIMI and disinformation that are catered to the regional context of ASEAN should be the priority at this stage, particularly as the regulatory approaches and social contexts vary from each ASEAN member state. These platforms allow ASEAN to promote a shared understanding and awareness of the FIMI landscape in the region, and work towards identifying common interests for cooperation. Aligning priorities and norms can also enhance more effective and coordinated efforts to jointly respond to FIMI by bridging varying capacity of the member states through exchanging best practices and lessons learned, knowledge sharing, technological assistance, and joint research between within ASEAN or between ASEAN and dialogue partners.

**Second**, strengthening the existing frameworks for government-civil partnership. Rather than creating new institutions, the existing cross-border informal channels like Asia Pacific Regional Internet Governance Forum (APrIGF), ASEAN Digital Rights Forum (ADRF), RightsCon can be an entry point for a sustainable and continuous collaboration, foster trust between stakeholders, intensify knowledge-sharing and develop non-binding recommendations across the region. ASEAN Secretariat can be convening power that acts as a facilitator for coordination and collaboration, while also empowered by ASEAN Ministerial bodies like ADGMIN. This can assist relevant stakeholders to secure fundings, accumulate human capital and expertise, and broaden access to advanced tools. Incorporating civil society perspectives in the process of drafting and revising regulations enhance credibility and legitimacy in digital governance. However, this arrangement may challenge the foundational principles of ASEAN such as non-interference and consensus-based decision-making.

**Third**, support capacity-building programs for civil society. ASEAN member states should invest in strengthening the existing efforts such as fact-checking and digital literacy, especially in countries with limited civic participation. Such efforts can be conducted by facilitating workshops, training, and mentorship programs for civil society organisations, journalists, and media organisations, to advance bottom-up approaches in addressing FIMI and disinformation campaigns. This includes strengthening digital skills (such as verifying

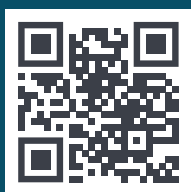




information, personal data protection, and financial literacy), enhancing technical capacity to detect patterns of information operations, and investing in advanced tools to counter the spread of FIMI. All of which leverage the positionality of civil society that complement government-led initiatives in internet governance.

**Fourth**, engage in international partnerships and leverage regional perspectives. ASEAN member states should actively participate in global multi-stakeholder forums, such as IGF and ICANN. These platforms can be an avenue that provides opportunities for Southeast Asian countries to amplify their perspectives, as well as advocating for a more inclusive governance that includes the participation of other developing states. Through this engagement, ASEAN can play an active role in contributing to global norms-setting and policy development on internet governance. In the long run, strategic partnerships that involve various stakeholders will also open up the opportunities for broader cross-regional collaboration.

In sum, this article offers reflections of the multi-stakeholder approach in strengthening information resilience in the Southeast Asian context, while attempting to provide strategic and policy-oriented recommendations in that regard. As highlighted above, the multi-stakeholder approach allows for inclusive decision-making processes, accountability, and transparency, while also encouraging cross-sector collaboration between different actors, which is important for addressing issues such as FIMI in the digital sphere. However, given the various socio-political contexts of states in Southeast Asia, there is a need for a multi-stakeholder approach that caters to the region's specific context and norms, while still being effective enough in addressing the challenges of FIMI and disinformation.



INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

## Generative AI and Information Resilience in the Asia-Pacific: Actions and Adaptations

↳ Faculty of Social and Political Sciences  
Universitas Gadjah Mada

↳ 21 August 2025

 [saferinternetlab.org/iris](https://saferinternetlab.org/iris)

 [@saferinetlab](https://www.instagram.com/saferinetlab)

 [@cfds\\_ugm](https://twitter.com/cfds_ugm)

 [iris@saferinternetlab.org](mailto:iris@saferinternetlab.org)