# INFORMATION WARFARE IN ASEAN: MALAYSIA AS A CRITICAL NODE IN REGIONAL FIMI DIFFUSION AND DEFENCE

**Amirun Haqqim bin Eldeen HUSAINI[1,2], E Kin Zane Ryan SEOW[3], Karisma Putera bin Abd RAHMAN[3]**
[1] Core Competence Centre for Operations Research, Management-Tenacity-Excellence, Safety & Security ALLIANCE (COMTESSA), University of the Bundeswehr, Neubiberg, Munich
amirun.husaini@unibw.de (**Corresponding author*)
[2] Nottingham University Business School (NUBS), University of Nottingham Malaysia, Semenyih, Malaysia
hpyae1@nottingham.edu.my
[3] Bait Al Amanah, Kuala Lumpur, Malaysia
ekseo1022@gmail.com, karisma@baitalamanah.com

**Abstract:** The paper examines the growing threat of foreign information manipulation and interference (FIMI) in Southeast Asia, focusing on the increasingly important role of Malaysia as a strategically critical node in the regional information environment. It maps Malaysia's emergence as a high-value target for FIMI operations, alongside the structural and technical vulnerabilities that leave it exposed. The paper concludes by proposing future directions, including establishing cooperation and data-sharing frameworks at the ASEAN level, positioning Malaysia as a potential hub for cyberdiplomacy, and developing the informatics capacity needed to improve situational awareness.
**Keywords**: FIMI, resilience, Malaysia, ASEAN, governance.

## INTRODUCTION

### Foreign Information Manipulation and Interference and the Role of the Global South

Foreign information manipulation and interference (FIMI) has become a defining characteristic of the modern security landscape. FIMI refers to a mostly lawful pattern of coordinated, and manipulative behaviour conducted by foreign actors with the intent to shape or influence political or societal developments in a target society (Rakhmat & Purnama, 2026).

Such behaviours encompass a broad range of harmful tactics, techniques and procedures, from cyber intrusions and hacking to the deliberate spread of manipulative or polarising narratives across digital platforms (Wheatley, 2020). These operations are particularly insidious and difficult to address, as they exploit the openness of democratic societies and turn those societies' own levers into threat vectors (Galeotti, 2022).

Documented FIMI operations have taken a variety of forms across different geopolitical contexts, illustrating the breadth of the tactics, actors and impacts involved. Some of the most studied examples involve integrated disinformation ecosystems that combine, for instance, diplomatic networks, state-controlled media, social media, and local proxies (Galán-Cordero & Cremades-Guisado, 2026). Others involve more multifaceted approaches that blend economic coercion, transnational repression, cyber intrusions and narrative manipulation to build influence within the global information space (European Commission, 2019). A common thread across these cases is that FIMI is rarely limited to a single tactic or platform and can

exploit multiple threat vectors simultaneously. As threat actors gain easier access to such vectors, societal resilience will increasingly depend on the ability to identify, understand, and counteract FIMI operations before they achieve their intended effects (Natea, 2022).

The recognition of the information space as a new and consequential frontier of geopolitical conflict, and of FIMI as a strategic threat vector, represents a significant evolution in how the European Union, in particular, has approached foreign-led hybrid attacks (Proto et al., 2025). The EU has responded with a range of dedicated actions aimed at developing analytical frameworks, coordinating responses with partner states, and exposing the underlying infrastructure of FIMI operations (Legucka & Kupiecki, 2022). A landmark step in this effort came in 2023, when the High Representative and Vice-President, Josep Borrell, announced the creation of a FIMI Information Sharing and Analysis Centre (FIMI ISAC) at the European External Action Service (EEAS) Conference on FIMI (Treyger et al., 2022). The FIMI ISAC is designed to facilitate the exchange of information among all relevant stakeholders and establish a shared operational baseline for countering FIMI (Marino-Jiménez et al., 2026). FIMI is not, however, a uniquely European problem. The EEAS has explicitly acknowledged the increasingly sophisticated and transnational nature of FIMI operations. Coordination across the Global North and Global South alike is needed to secure the resilience of the information landscape (EEAS, 2026). Like the information landscape, FIMI is unbounded, and regional occurrences should be understood as multi-layered, transnational threats operating through interconnected nodes that span multiple regions. This networked characteristic of FIMI is what makes it so difficult to counter through siloed responses, and it is why the absence of comparably strong frameworks in regions outside the EU is a structural gap in their security (Barlybaikyzy & Duisen, 2025).

However, useful as the current FIMI frameworks are, they carry a largely European lens. The landscape has changed drastically in recent years, with the geography of information warfare shifting to other regions. For example, substantial investments by major actors in cultivating influence across Southeast Asia, Africa and Latin America have been widely observed (Hamilton, 2025). The Indo-Pacific region, in particular, has emerged as a critical theatre for the deployment of FIMI tactics by major actors, who increasingly perceive the region as a strategically vital arena for building power, shaping public opinion, and consolidating influence. This reflects a broader pattern in which the Global South is an attractive target for FIMI operations, an appeal that extends well beyond its relevance to European security (Nitza-Makowska et al., 2026).

The Indo-Pacific is strategically important for global trade, maritime security and innovation, with rapidly expanding economic interdependencies and an increasingly contested geopolitical environment (Denisov et al., 2021). The region is home to more than half of the world's population and accounts for 60% of global GDP and two-thirds of global economic growth (Scott, 2018). Furthermore, it has been argued that the sub-regions of the Indo-Pacific have distinct material, geographical, ideational and cultural characteristics that render them especially suitable for successful operations (Lee, 2022). The member states of the Association of Southeast Asian Nations (ASEAN), for instance, form an important part of this threat landscape and are uniquely complex for existing FIMI frameworks to address. This article makes two contributions toward addressing FIMI within such underrepresented regions. First, it develops a Malaysia-centred case for why a networked, multi-stakeholder ASEAN response to FIMI is both necessary and feasible. Second, it identifies two concrete technical priorities for future efforts in developing a well-coordinated regional FIMI response architecture.

## The ASEAN Information Environment

ASEAN offers FIMI actors a structural advantage, primarily because its member states are so closely interconnected geographically, culturally and economically. Intra-ASEAN trade, for example, consistently accounted for approximately 22% of the bloc's total trade between 2013 and 2023, a period during which total ASEAN trade nearly doubled in value (ASEAN Stats, 2024). Beyond these deep regional interdependencies, ASEAN sits astride a major maritime corridor connecting the West with the East, which underscores both its centrality to global trade networks and its strategic value as a geographic chokepoint (Chinvanno & Anantasirikia, 2024).

Moreover, the region has recently undergone rapid digitalisation, with an estimated 68% of its population using social media platforms. Although beneficial in many ways, this rapid growth increases the region's vulnerability to the spread of disinformation (Smith & Perry, 2022). Notably, disinformation in the ASEAN information landscape is not only produced by foreign actors but is also consistently linked with state actors and government lawmakers within member states themselves. For example, several ASEAN nations have documented cases of government-affiliated actors deploying coordinated influence networks to spread manipulative narratives (Saraswati, 2020). These dynamics are further compounded by structural vulnerabilities across the region, including low levels of digital literacy, non-democratic governance in several member states, and a highly fragmented media landscape (Martinus, 2023). This normalisation of domestic information manipulation within ASEAN's political cultures, set atop weak institutional safeguards, creates a permissive environment that foreign FIMI actors can readily exploit.

FIMI operations targeting ASEAN member states are already well documented and reveal a consistent pattern of localised, narrative-driven interference that exploits existing social and political fault lines. Across the region, for instance, several foreign-linked actors have deployed coordinated networks of fake accounts to amplify divisive content about regional geopolitics, territorial disputes, and domestic political figures (Meta, 2021; Nimmo et al., 2020; McPherson, 2025). The spread of FIMI operations such as disinformation campaigns within the region has been further compounded by the use of artificial intelligence (AI). For example, in Indonesia, a deepfake video of a figure resembling the late President Soeharto circulated ahead of the country's 2024 election, calling on voters to support candidates from his former party (Fakhruddin, 2023). Similarly, in Singapore, a fabricated video of former Prime Minister Lee Hsien Loong falsely promoting a cryptocurrency scheme spread widely online, prompting him to issue a public clarification (Chiu, 2024). The low financial barrier to using generative AI has also facilitated the production of disinformation at an alarming rate. An investigation by Channel NewsAsia (CNA), for example, found AI-generated "presenters" spreading geopolitical disinformation about Singapore and Malaysia in 500 TikTok videos between October 2025 and June 2026 (Channel NewsAsia, 2026).

Evidently, FIMI is not merely an emerging concern in ASEAN. The region is already vulnerable to foreign exploitation of its regional dynamics and rapid digitalisation, especially given the lack of whole-of-government, whole-of-society (WoGoS) approaches to tackling cross-border FIMI operations within the region. WoGoS approaches are understood here as frameworks and protocols built around "inclusive participation and shared responsibility across sectors" (Nasir et al., 2026).

## ADDRESSING FIMI THE ASEAN WAY

ASEAN governments have adopted a range of legislative measures to respond to the rise of FIMI in the region. In Indonesia, a law obliging foreign internet services to register with the authorities, intended to counter information that undermines public order, has been reinforced. Moreover, a criminal code introduced in 2022 paved the way for criminally charging individuals who spread hatred or misinformation about the government (Luong, 2022). Similarly, in Singapore, under the Protection from Online Falsehoods and Manipulation Act, disseminators of false information can be penalised and prosecuted (Parliament of Singapore, 2019). In Thailand, an "Anti-Fake News Centre" to suppress fake news was launched following the rise of harmful COVID-related news between 2020 and 2022 (Chongkittavorn, 2023). Evidently, individual ASEAN member states have taken vast and divergent measures, ranging from regulations that hold platforms accountable for any disinformation or misinformation they host to the penalisation of individual users. The differences in approach across ASEAN rightly reflect the heterogeneity of the regional threat landscape and the context-specific vulnerabilities of individual member states. However, given the cross-border nature of FIMI operations, it is also crucial to explore how ASEAN responds collectively.

Regionally, there have been several normative efforts to address FIMI. In 2014, ASEAN adopted the Declaration on Socially Responsible Media for a Peaceful and Prosperous Community, followed in 2018 by the Framework to Minimise the Harmful Effects of Fake News (ASEAN, 2014; ASEAN, 2018). That same year, the ASEAN Ministerial Conference on Cybersecurity began foundational discussions for a cross-sectoral cybersecurity mechanism, which led to the establishment of the ASEAN Cybersecurity Coordinating Committee in 2020 (ASEAN, 2022).

In 2019, ASEAN also established a dedicated Task Force on Fake News (ASEAN, 2023b; The Sun Malaysia, 2023). However, the operational record of the Task Force has been limited. ASEAN Digital Ministers have also begun formulating the ASEAN Guide on AI Governance and Ethics, intended to ensure the safe and responsible use of rapidly advancing technologies (ASEAN, 2024).

In 2022, ASEAN, with the support of dialogue partners, conducted a Training of Trainers Program to Address Disinformation and Promote Media Literacy, and a publicly available toolkit was published on the ASEAN Secretariat website. Meanwhile in 2023, the ASEAN Ministers Responsible for Information (AMRI) meeting in Danang City, Vietnam have also seen ASEAN members endorsing Indonesia's proposal outlining principles for managing government information to address disinformation, with recommendations covering key areas including detection and response (ASEAN, 2023b).

More recently, the 4th ASEAN Digital Ministers' Meeting (ADGMIN) in 2024 and 5th ADGMIN in 2025 have seen the publication of an ASEAN Guide on AI Governance and Ethics; the former focusing on promoting trustworthy-AI principles and the latter shines focus on deepfakes to information integrity and electoral interference (ASEAN, 2024; ASEAN, 2025a).

Table 1 provides a consolidated overview of these normative efforts, illustrating both the breadth of ASEAN's commitments and the gaps that remain:

**Table 1.** ASEAN instruments addressing information manipulation, 2014–2025

| Year | Instrument / Body | Forum | Commits Members to | Operational Gap |
|---|---|---|---|---|
| 2014 | Declaration on Social Responsible Media for a Peaceful and Prosperous ASEAN Community | 12th Conference of the ASEAN Ministers Responsible for Information (AMRI), Nay Pyi Taw, 12 June 2014 (ASEAN, 2014) | Aspire to support 'social responsible media'; no substantive norms (ASEAN, 2014) | Lacks clear definitions, monitoring mechanisms, and reporting duty. |
| 2018 | Framework and Joint Declaration to Minimise the Harmful Effects of Fake News | 14th AMRI, Singapore, 10 May 2018 (ASEAN, 2018) | Norms, capacity building, information exchange on fake news (ASEAN, 2018) | Brainstorming in AMRI roundtable limited to measures of cooperation among member states such as best-practice sharing, capacity building, media literacy and public awareness.<br><br>These addresses the content-recipient side but lacks discussion on acting against the creators and senders; i.e. tracking funding to dismantle disinformation industries. |
| 2019 | ASEAN Task Force on Fake News (TFFN) | A regional mechanism on fake news, misinformation, hate speech, extremist views and radicalisation; terms of reference adopted February 2022; Plan of Action supported 2023 (ASEAN, 2023b) | A standing regional mechanism on fake news, misinformation, hate speech, extremist views and radicalisation. | Two meetings on the published record, October 2022 and July 2023; the 17th AMRI (ASEAN, 2025b) acknowledges the Task Force's work without recording any further meeting, date or venue |
| 2020 | ASEAN Cybersecurity Coordinating Committee (ASEAN Cyber-CC) | Agreed on:<br>- 19th Telecommunications and Information Technology Ministers Meeting (TELMIN), 25 October 2019 (ASEAN, 2019); and<br>- 4th ASEAN Ministerial Conference on Cybersecurity (AMCC), 2 October 2019 (Cyber Security Agency of Singapore, 2019)<br><br>ASEAN Cyber-CC inaugural meeting held on 5 Nov 2020 | Cross-sectoral coordination spanning Senior Officials Meeting on Transnational Crime (SOMTC) cybercrime and SOMRI information / media working groups; critical information infrastructure (CII) protection, Computer Emergency Response Teams (CERT) cooperation; United Nations Group of Governmental Experts (UNGGE) norms implementation | Treats disinformation as an 'infodemic' or a by-product of jailbroken generative AI; the 2026–2030 strategy never uses the terms information manipulation, influence, propaganda or information integrity, so no actor-directed threat is in view. |
| 2023 | Guideline on Management of Government Information in Combating Fake News and Disinformation in the Media | 16th AMRI, Da Nang, 23 September 2023 (ASEAN, 2023b) | Norms for government communicators and for platforms, including collaboration | Non-binding and addressed to government information officers; no escalation thresholds, no cross-border trigger, no platform enforcement. |
| 2024 | ASEAN Guide on AI Governance and Ethics | 4th ADGMIN, Singapore, 2 Feb 2024 (Personal Data Protection Commission Singapore, 2024) | Voluntary trustworthy-AI principles (seven guiding principles) for organisations deploying traditional AI; names disinformation and deepfakes among six generative-AI risks (ASEAN, 2024) | The six risks appear only in a forward-looking section addressed to policymakers, which proposes the voluntary adoption of the guide to address Gen-AI governance rather than treating the risks posed by bad-actors. The guide does not cover specialised AI models trained and geared towards disinformation. |
| 2025 | Expanded ASEAN Guide on AI Governance and Ethics – Generative AI | 5th ADGMIN, Bangkok, 17 January 2025 (ASEAN, 2025a) | A resource for ASEAN policymakers; §3.7 treats content provenance, linking deepfakes to information integrity and electoral interference, and discusses watermarking and cryptographic provenance | Offers a single item under 'areas for ASEAN to explore'; confines ASEAN's role to convening power and best-practice sharing; adopts no standard, imposes no labelling obligation, sets no timeline |

*Note: The "operational gap" column is the author's assessment. Instruments are listed by year of adoption or endorsement, not by year of publication.*

Despite the breadth of these normative commitments, significant gaps remain in ASEAN's collective capacity to detect and respond to cross-border FIMI operations. The ASEAN Cybersecurity Coordination Committee, for instance, has focused primarily on the protection of critical infrastructure, and has not yet adequately addressed the growing challenge of computational propaganda and its regional implications. More broadly, while ASEAN has produced a substantial body of declarations and work plans, these instruments cannot be used effectively without enforcement mechanisms, shared technical infrastructure or information-sharing protocols, all of which are currently lacking. Critically, a holistic WoGoS approach to FIMI at the ASEAN level has yet to be operationalised.

The recommendations emerging from the 2023 AMRI meeting represent a promising step toward addressing this need. The resulting Guideline on the Management of Government Information in Combating Fake News and Disinformation articulates several responsible behaviours appropriate to all member states, including media literacy and critical thinking, responsible sharing of information, transparency and accountability, independence and integrity of the media, and legal and regulatory measures. The Guideline also sets out norms for digital platforms covering transparency, fact-checking, user education, empowerment, accountability and collaboration. The explicit inclusion of collaboration as a pillar for both member states and digital platforms is significant because it acknowledges that FIMI cannot be addressed through siloed tactics. Effective resilience requires coordinated early warning, cross-border information sharing, and joint capacity-building frameworks that treat the ASEAN information environment as a shared, networked space. The following sections examine the potential levers of collaboration available through Malaysia as a key node in the ASEAN information ecosystem.

## MALAYSIA AS AN EMERGING NODE IN THE FIMI ECOSYSTEM

Disinformation is not new to Malaysia, particularly in its domestic politics. A report published by Asia Centre (2022) that analysed Malaysian election campaigns since 1999 has revealed recurring patterns of disinformation involving the creation and dissemination of falsehoods about the sexual orientation, public office and electoral integrity of candidates to discredit political rivals.

Beyond the domestic political sphere, however, one of the earliest reported cases of Malaysian exposure to foreign-sponsored disinformation operations dates back to the 2019-2020 Hong Kong anti-government protests, when online communities in Malaysia were among those caught in the information war between anti-protest and pro-Hong Kong factions in the cyberspace (Malaysiakini, 2021). The embedding of foreign narratives and disinformation into domestic media has also been noted by Freedom House, which in 2022 ranked Malaysia 37$^{th}$ out of 85 indexed countries for susceptibility to media influence efforts by Beijing (Han & Loh, 2022). This coincides with findings published the same year by Watan and the Merdeka Center for Opinion Research on state-sponsored influence operations in Malaysia, which alleged that local media outlets had been sponsored to publish pro-China news in Malay-language media (Watan & Merdeka Center for Opinion Research, 2022). These reported cases of disinformation operations raise the question: why Malaysia, and what makes it a high-value target for FIMI operations?

## What Makes Malaysia a High-Value Target for FIMI Operations

Several factors explain Malaysia's high value for FIMI operations. First, Malaysia sits at the intersection of major geostrategic fault lines through its geography, its demography and its record as a non-aligned middle power amid the superpower contest between China and the United States.

With a gross domestic product (GDP) of US$472.19 billion, Malaysia is a critical upper-middle-income ASEAN economy that borders the Straits of Malacca, a maritime chokepoint facilitating approximately 25-30% of global seaborne trade between the Indian Ocean and the Pacific Ocean. It is also a crucial node in global semiconductor and technology supply chains, recognised as the sixth-largest exporter of semiconductors and commanding 13% of the global market for semiconductor packaging, assembly and testing (Lu & Moorthy, 2026; MIDA, 2024).

Within ASEAN, Malaysia played a central role as the 2025 ASEAN Chair, leading the region's strategic agenda across key domains including conflict mediation, trade and economic integration, digital transformation, and the development of the ASEAN Community Vision 2045 (Lin et al., 2025). Moreover, Malaysia's multi-ethnic, multi-religious composition lends it a distinctive diplomatic profile, enabling it to maintain functional relationships across diverse geopolitical blocs. However, despite its growing importance on the regional and global stages, Malaysia also has several structural and technical vulnerabilities that FIMI operations can exploit.

Primarily, Malaysia's posture of strategic non-alignment, or what has been described as "pragmatic neutrality", has in many ways benefited the nation but may also be a source of vulnerability to FIMI (Kuik, 2024; China-Global South Project, 2025). Malaysia's engagement with major powers has been characterised as an "equidistance" approach, marked by macro-level neutrality combined with selective, issue-based engagement across micro-level domains (Kuik, 2024). In practice, however, this neutrality is actively constructed rather than passively maintained. Malaysia does not maintain equal distance at the micro level and instead pursues differentiated engagement across distinct domains (Lu & Moorthy, 2026). This deliberate and delicate "balancing act" creates the informational conditions that FIMI actors are best positioned to exploit.

Domestically, Malaysia's multi-ethnic, multi-lingual and multi-religious composition, although a source of diplomatic strength in many ways, can also create structural fault lines that are particularly susceptible to exploitation through identity-based influence operations. The EEAS has explicitly identified identity-based disinformation as a core FIMI tactic, describing these as campaigns that deliberately target communities to amplify existing divisions (EEAS, 2024). False narratives and polarising propaganda have been prominent in Malaysia, particularly during politically charged periods. In the aftermath of the 2022 general elections, for instance, trends on TikTok called for "a second May 13", a reference to a dark chapter in Malaysian history marked by violent clashes between ethnic Malays and Malaysian Chinese on 13 May 1969 (Jalli & Jamaluddin, 2024). Malaysia's pluralistic social fabric thus provides FIMI actors with a pre-existing set of fault lines that could be exploited.

Malaysia's digital transformation has also introduced a further layer of structural vulnerability, characterised by near-total reliance on foreign-owned platforms and limited transparency

over content or contact recommendation algorithms. Over 83% of Malaysians are active on social media, with WhatsApp and TikTok dominating the digital landscape (Howe, 2024). The heightened use of social media platforms is particularly concerning given the prominence of disinformation as a political tool within Malaysia. The activity of "cybertroopers", whose objectives are to exert influence over electoral processes and foster political polarisation, has been well observed (Fitriani et al., 2024). Malaysia is thus an increasingly appealing target for FIMI operations, given its acute vulnerabilities and outsized regional significance. Yet these same characteristics may position Malaysia as a key node in a networked ASEAN approach to FIMI.

## The Role of Malaysia in an ASEAN Approach

ASEAN must move beyond normative commitments toward proactive, operationalised mechanisms for countering FIMI. Several concrete directions present themselves. Analogous to the EU's FIMI ISAC, ASEAN member states could benefit from intergovernmental frameworks for sharing incident data, best practices and dynamic threat intelligence using common and interoperable standards. The heterogeneity of legal frameworks and institutional capacities across member states can also be a valuable resource. For instance, Singapore's robust legislative frameworks and enforcement capacity against disinformation propagation have already served as a useful case study for neighbouring states, illustrating the benefits of sharing lessons learned across the region (Fitriani et al., 2024). Crucially, however, governments alone cannot address FIMI effectively. As the Indonesian Ministry of Communication and Informatics has highlighted in the Guideline on the Management of Government Information in Combating Fake News and Disinformation, a multi-sectoral approach is required, combining defence and information ministries with telecommunications, education and youth-policy institutions. Researchers, journalists, civil society organisations and digital platforms must also be formally integrated into the detection and response loop (ASEAN, 2023a; Kingdon, 2024).

Malaysia is well suited in several ways to support such ambitions within ASEAN. Primarily, Malaysia's network of bilateral relationships spanning ASEAN and major external powers across the Global South and Global North positions it as a strategic linchpin within the region for securing the multi-party buy-in that a regional FIMI response framework would require. Critically, its posture of strategic non-alignment is likely to lend any mediatory role to a degree of trusted neutrality and legitimacy. Malaysia's geoeconomic profile adds further weight to this case and may help in coordinating discussions with major infrastructure providers and platforms based outside ASEAN. In this sense, Malaysia's distinctive combination of diplomatic breadth, geoeconomic standing, and trusted neutrality makes it a natural candidate to serve as a key node in a networked ASEAN approach.

However, Malaysia's forward-looking regional role must first be grounded in domestic institutional readiness. The country possesses many of the relevant capabilities across national security, communications regulation, cybersecurity, law enforcement, disaster management, foreign affairs, election administration, and financial scam response. The central challenge is improving coordination among these bodies when an information incident crosses mandates.

Table 2 maps the Malaysian bodies whose mandates would be engaged by a foreign information incident, the basis on which each acts, and where that mandate stops.

**Table 2.** Malaysian Government Agencies, Mandates and Limitations in Countering FIMI

| Function | Lead body | Basis | Relevant powers | Limitations for FIMI response |
|---|---|---|---|---|
| National security coordination | Majlis Keselamatan Negara (MKN), Prime Minister's Department | National Security Council Act 2016 (Parliament of Malaysia, 2016b); executive NSC Directives | Convenes agencies; issues directives; serves as secretariat to national committees | No directive or standing procedure designates a lead agency for an information incident that falls short of a security emergency or declared disaster |
| Cyber security | NACSA (under MKN), with NC4 | Cyber Security Act 2024 (Act 854), in force 26 Aug 2024 (Parliament of Malaysia, 2024b); NSC Directive No. 26 (NACSA, 2026) | NCII designation; mandatory incident notification to NC4; licensing of cyber security service providers | Mandate is limited to the security of computer systems within critical national infrastructure (Parliament of Malaysia, 2024b); influence operations run through legitimate accounts are not necessarily a "cyber security incident" |
| Cybercrime law (pending) | NSC/NACSA; proposed Committee on Combating Cybercrimes | Cybercrimes Bill 2026 (Parliament of Malaysia, 2026), passed by Parliament in July 2026, to repeal the Computer Crimes Act 1997 (Parliament of Malaysia, 2006b; Rahmat Lim & Partners, 2026) | New offences including AI-generated deepfakes and impersonation; extraterritorial reach; inter-agency committee (Rahmat Lim & Partners, 2026) | Offence-based; whether it reaches coordinated but otherwise lawful manipulation is unclear. |
| Content and platform regulation | MCMC (Under the Ministry of Communications) | Communications and Multimedia Act 1998 (CMA) (Parliament of Malaysia, 2006a), as amended, in force 11 Feb 2025 (AmCham Malaysia, 2025); ASP(C) licensing of platforms with ≥8 million users from 1 Jan 2025 (Baker McKenzie, 2024); Online Safety Act 2025 (Act 866), in force 1 Jan 2026 (Parliament of Malaysia, 2025) | Takedowns; licence conditions; platform safety duties; penalties up to RM10m; operates a fact checking website at Sebenarnya.my | Harmful-content categories, including content promoting ill-will or hostility, are judged on substance and are blind to origin and coordination; duties fall on platforms, not users (MCMC, 2026) |
| Criminal investigation of online content | Royal Malaysian Police (PDRM): Bukit Aman CCID; Police Cyber Investigation Response Centre (PCIRC) | Penal Code (Parliament of Malaysia, 2013); CMA 1998 (Parliament of Malaysia, 2006a); Sedition Act 1948 (Parliament of Malaysia, 2006d) | 24-hour monitoring, profiling and investigation; requests takedowns via MCMC (The Vibes, 2025b) | Triggered by an identifiable offence and oriented largely towards fraud; lawful-but-manipulative activity falls outside |
| Intelligence and state security | PDRM Special Branch | Police Act 1967 (Parliament of Malaysia, 2006c); Penal Code Ch. VI, ss. 124B–124N (Parliament of Malaysia, 2013); SOSMA 2012 (Parliament of Malaysia, 2012) | Counter-intelligence; monitoring of foreign agents (The Vibes, 2025a) | Offence threshold requires violent or unconstitutional means, and past use against domestic critics makes it politically costly; intelligence product does not flow into public communication or platform action |
| Financial-harm response | National Scam Response Centre (NSRC), led by PDRM CCID under the Home Ministry, with BNM, MCMC, NFCC, banks and telcos; 997 line | Established 12 Oct 2022 (Bernama, 2026); Penal Code ss. 424A–424D (Parliament of Malaysia, 2024c) and CPC s. 116D (Parliament of Malaysia, 2024a), in force 30 Oct 2024 | Rapid tracing and freezing of funds; mule-account offences (Bank Negara Malaysia, n.d.) | Activated by a victim's complaint and loss; payments to disinformation-for-hire providers produce no complainant |
| Financial intelligence | Bank Negara Malaysia, Financial Intelligence and Enforcement Department (national FIU) | AMLA 2001 (Parliament of Malaysia, 2001) | Receives and analyses suspicious transaction reports; shares intelligence domestically and through the Egmont Group | Analysis is anchored to money laundering and predicate offences |
| Electoral integrity | Suruhanjaya Pilihan Raya (SPR), with election-specific MCMC–SPR arrangements | Elections Act 1958 (Parliament of Malaysia, 2011); Election Offences Act 1954 (Parliament of Malaysia, 2016a) | Regulates campaign conduct; refers material to MCMC for removal | Mandate concentrated in the campaign period; narratives seeded beforehand fall outside; coordination is re-convened for each election |
| Government communication | Ministry of Communications; Jabatan Penerangan; BERNAMA | Executive | Official correction and public messaging; inter-agency task force (PDRM, MCMC, AGC) on unverified news | Correction capacity without dedicated detection or analytic capacity; task force addresses unverified news generally, not foreign-origin operations |
| Crisis management | NADMA | NADMA Directive No. 1 (dated 1 August 2024), which revokes and replaces NSC Directive No. 20 (Agensi Pengurusan Bencana Negara, 2024) | Inter-agency coordination and crisis communication in a declared disaster | Activated only by a declared disaster; an information incident alone does not trigger it |

*Note: The "Limitations for FIMI response" column is the author's assessment.*

Two features stand out. First, most of these mechanisms are activated by a threshold that sits at the level of individual content or individual harm: a prosecutable offence (The Vibes, 2025b), a victim's financial loss (Fintech News Malaysia, 2026), a declared disaster (Agensi Pengurusan Bencana Negara, 2024), an official campaign period (Bernama, 2025b) or a listed category of harmful content (MCMC, 2026). FIMI's defining features, namely coordination, inauthenticity and foreign direction, are not in themselves triggers for any of them (Meta, 2021; Rakhmat & Purnama, 2026). The system can therefore act against an individual post or account, as in the removal of fraudulent content at police request or the freezing of accounts linked to scams, without ever engaging the operation behind it. Second, outside police intelligence work on foreign agents (The Vibes, 2025a), mandates are organised around content or harm rather than around actors and coordinated behaviour (MCMC, 2026). There is no published mandate assigning any body to determine whether an operation is foreign-directed or to attribute it publicly. Act 854, for instance, defines an incident by its effect on computer systems rather than on public discourse (Parliament of Malaysia, 2024b). Malaysia has, however, already built standing inter-agency coordination where harm is financial, in the National Scam Response Centre (Bernama, 2025a). For information incidents, comparable arrangements have so far been convened around particular events, such as the joint police and MCMC cyber task force during the 2022 general election and the committee between MCMC and the Election Commission for the 2025 Sabah state election (Bernama, 2022; Bernama, 2025b).

FIMI-related incidents rarely remain confined to a single policy domain. A manipulated narrative may begin as an online falsehood but rapidly acquire implications for public safety, electoral integrity, financial harm, diplomatic relations or social cohesion. A whole-of-government response therefore requires agreed escalation thresholds, lead and supporting roles, common information-sharing arrangements, authorised spokespersons and routine joint exercises. This is consistent with ASEAN's own guidance, which emphasises coordination and collaboration among government agencies, particularly during crises.

A whole-of-society approach is equally necessary. Official correction alone may be insufficient where trust is uneven, or audiences rely on fragmented digital and community networks. Media organisations, researchers, civil society, educators, platforms, financial institutions and locally trusted community figures each have distinct roles in detecting, contextualising, distributing and reinforcing credible information. Malaysia thus requires a scalable model in which authority, evidence and communication can move coherently across institutions and communities. Developing such a model would give Malaysia practical experience that would allow it to contribute more effectively at the ASEAN level.

Beyond governance structures that would nurture intergovernmental collaboration to deter FIMI, the technical infrastructure also needs to be considered. The following sections highlight two possible directions for the region.

## DETECTION GAPS IN ASEAN'S CYBERTROOPER ECOSYSTEM

An emerging concern across the ASEAN information landscape is the proliferation of "political buzzers", a term that arose in the regional context to describe coordinated networks

of bots, celebrity influencers, cybertroopers and cyber-trolls deployed to generate artificial engagement on social media and to shape public opinion through tactics that include historical revisionism, hate speech, personal abuse, memes and parody accounts (Da San Martino et al., 2020; Tan & McIlvaney, 2025). Although the phenomenon of coordinated inauthentic behaviour has been observed in democracies worldwide, it has become particularly entrenched within several ASEAN member states (Sukmani & Aras, 2024).

In Indonesia, the use of coordinated social media networks in political campaigns can be traced back to the 2012 Jakarta gubernatorial election, in which Joko Widodo (Jokowi) found success in his campaign partly through a social media effort driven by a structured volunteer network designed to shape public support and engage in coordinated counter-messaging against political opponents (Alizen & Fajar, 2021; Fatmala et al., 2020; Suci, 2024). Such tactics became increasingly sophisticated in subsequent election cycles. During Indonesia's 2019 general election, it was reported that both presidential campaigns deployed organised networks of buzzers to spread fake news and undermine opposing candidates (Aspinall, 2019). In the Philippines, former President Rodrigo Duterte's 2016 campaign saw the rise of an online public relations consultancy industry in which organised disinformation was used to ridicule opposition parties. These campaigns involved parties and candidates hiring micro-influencers with loyal followings to insert political content into their non-political posts (Tan & McIlvaney, 2025). Similar anti-opposition messaging also emerged in Malaysia's 2018 general election (Leong & Loh, 2024). Together, these examples illustrate a regional pattern of growing use of fragmented networks of individual social media users to influence political discourse. Although the documented cases primarily involve domestic political actors, the infrastructure of difficult-to-detect influence nodes that has been created may readily be exploited by foreign FIMI actors as well.

Conventional approaches such as fact-checking initiatives and legislative prohibitions face several structural limitations in the ASEAN context. Such approaches are inherently reactive, often too slow to contain narratives that spread at the speed of social media sharing, and risk being co-opted for partisan ends or used as instruments of democratic repression (Tan & McIlvaney, 2025). Existing predictive analytics frameworks offer a more promising direction. Del Vicario et al. (2019), for instance, demonstrated that polarisation signals on social media can be used to predict future misinformation targets with 77% accuracy, establishing proof of concept for an anticipatory, rather than reactive, approach to disinformation detection. Further development of such predictive frameworks, specifically oriented toward mapping coordinated buzzer networks, may represent a significant avenue for research and development.

## Follow the Money: Financial Technical Infrastructure to Counter FIMI

Government responses to disinformation have largely targeted behavioural outputs *(bots, AI content, deepfakes)*, with policy prescriptions geared towards the end-user *(i.e. social media users)*, for example enhancing media literacy, establishing fake news monitors, and pressing social media corporations to improve content moderation (Mustaffa, 2025). While these suggestions are important, deterrence against disinformation, whether foreign or domestic in origin, must be holistic, and states must pay equal attention to the technical infrastructure that enables an early warning system against FIMI. The technical capabilities of national

security agencies and civil society watchdogs, from open-source intelligence (OSINT) to sophisticated proprietary cybersecurity solutions, must be geared towards the common thread of FIMI operations: funding.

Concerted disinformation operations, regardless of whether they are driven by political or personal conviction, can rarely run *pro bono*. Disinformation-as-a-service (DaaS) is a growing industry in ASEAN, as shown by foreign-led disinformation against Vietnam in the South China Sea (Safer Internet Lab, 2024), cybertrooper services fueling political divides in Malaysia (New Straits Times, 2026), and burgeoning domestic disinformation mills run by freelancers and social media influencers in the Philippines (Safer Internet Lab, 2024). Dismantling these FIMI vectors requires robust frameworks for financial intelligence in ASEAN. The 4th EEAS Annual Report on FIMI Threats has noted that over 65% of global FIMI incidents rely on highly sophisticated, unattributed networks that obscure their financial trails (EEAS, 2026). While many DaaS contractors accept cash and bank transfers in the region, as in the case of Malaysian cybertroopers (New Straits Times, 2026), hard-to-trace alternatives such as cryptocurrencies are poised to obstruct governmental efforts to stem their financing, as seen with disinformation actors targeting the United States and Europe (Olalekan, 2024; TRM Labs, 2024).

At this juncture, Malaysia, Singapore and Indonesia are the only ASEAN economies that are full members of the Financial Action Task Force (FATF), an intergovernmental body established to tackle money laundering and terrorist financing. Other ASEAN economies, such as Brunei, Cambodia, Laos, Myanmar, the Philippines, Thailand, Timor-Leste and Vietnam, have adopted FATF standards by proxy, through their membership of the Asia/Pacific Group on Money Laundering (APG). As David Lam, Visiting Fellow with the Regional Economic Studies Programme at ISEAS, has pointed out, the FATF standards alone are insufficient for cryptocurrency regulation, and certain member states, such as Malaysia and Indonesia, lack crypto exchange regulations such as mule account prevention measures and crypto address blacklists (Lam, 2026). This in turn facilitates the proliferation of mule accounts used to launder cryptocurrency proceeds, a problem compounded by the rise of transnational crime in the form of cyberscam compounds mushrooming across Southeast Asia, which fuels a sophisticated ecosystem of illicit cryptocurrency-laundering networks. Blockchain intelligence is therefore the next logical step, and a focus area, for ASEAN member states seeking to reinforce their financial intelligence infrastructure against shadow economies and underground banking.

## CONCLUSION

The proliferation of FIMI across the global information landscape represents one of the defining security challenges of the modern era. Existing frameworks for deterrence are largely focused on the Global North. Regions within the Global South, such as the ASEAN nations, present uniquely complex and increasingly consequential information landscapes that can be permissive to FIMI operations by foreign actors. The documented cases examined here illustrate that the threat is active, evolving and accelerating within the region. Malaysia's position within this landscape is significant. It is simultaneously a high-value FIMI target within the region and one of the most credible candidates for anchoring a coordinated

ASEAN-level response. Its diplomatic reach and geoeconomic leverage with major powers, infrastructure providers and platforms constitute a distinctive set of levers that could credibly be deployed in a mediatory capacity.

The path forward follows two parallel tracks. At the governance level, ASEAN must translate its normative commitments into operationalised frameworks, drawing on the levers each member state possesses. At the technical level, two possible directions are highlighted: financial intelligence infrastructure capable of tracing the funding flows that sustain coordinated FIMI operations, and predictive, linguistically calibrated computational frameworks capable of detecting coordinated buzzer networks. Together, these imperatives point toward a regional FIMI architecture that is collaborative, technically grounded, and politically anchored. For Malaysia, regional leadership should begin with domestic demonstration: building and exercising a coordinated national model whose lessons can then inform an ASEAN approach to combating FIMI operations that suits the region's diversity.

## REFERENCE LIST


Agensi Pengurusan Bencana Negara. (2024) Arahan NADMA No. 1: Dasar dan mekanisme pengurusan bencana negara [NADMA Directive No. 1: National disaster management policy and mechanism], Putrajaya: Jabatan Perdana Menteri. Available at: https://www.nadma.gov.my/images/2024/RujukanDalaman/Arahan_NADMA_No_1.pdf

Alizen, A. N. & Fajar, M. S. (2021) Election campaigns and cyber troops. Inside Indonesia. 146 (Oct–Dec). https://www.insideindonesia.org/editions/edition-146-oct-dec-2021/election-campaigns-and-cyber-troops

American Malaysian Chamber of Commerce (AmCham Malaysia). (2025) Amendments to the Communications and Multimedia Act 1998 come into force on 11 February 2025 (update). [Online]. Available at: https://amcham.com.my/41059-2/ [Accessed 13th October 2026].

ASEAN. (2014) *Declaration on social responsible media for a peaceful and prosperous ASEAN community*. 12th Conference of ASEAN Ministers Responsible for Information, Nay Pyi Taw, Myanmar, 12th June. https://asean.org/wp-content/uploads/2021/01/Declaration-on-Social-Responsible-Media-for-a-Peaceful-and-Prosperous-ASEAN-Community.pdf

ASEAN. (2018) *Framework and joint declaration to minimise the harmful effects of fake news*. 14th Conference of ASEAN Ministers Responsible for Information, Singapore, 10th May. https://asean.org/wp-content/uploads/2021/01/Framework-and-Joint-Declaration-to-Minimise-the-Harmful-Effects-of-Fake-News.pdf

ASEAN. (2019) Joint media statement: 19th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) and related meetings. Vientiane, Lao PDR, 25th October. [Online]. Available at: https://asean.org/wp-content/uploads/2021/09/ADOPTED-TELMIN-19th-TELMIN-JMS-.pdf [Accessed 14th October 2026].

ASEAN. (2022) ASEAN cybersecurity cooperation strategy (2021–2025). ASEAN Secretariat. [Online]. Available at: https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf [Accessed 14th August 2026].

ASEAN. (2023a) *ASEAN guideline on management of government information in combating fake news and disinformation in the media*. ASEAN Secretariat. https://asean.org/wp-content/uploads/2023/06/ASEAN-Guideline-in-Combating-Fake-News-and-Disinformation-in-the-Media-ISBN.pdf

ASEAN. (2023b) Joint media statement: 16th Conference of the ASEAN Ministers Responsible for Information & 7th Conference of the ASEAN Plus Three Ministers Responsible for Information. Da Nang, Viet Nam, 22–23 September. [Online]. Available at: https://asean.org/wp-content/uploads/2023/09/JMS-16th-AMRI-FINAL.pdf [Accessed 8th October 2026].

ASEAN. (2024) *ASEAN guide on AI governance and ethics*. https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf

ASEAN. (2025a) Expanded ASEAN guide on AI governance and ethics – generative AI. ASEAN Secretariat. [Online]. Available at: https://asean.org/wp-content/uploads/2025/01/Expanded-ASEAN-Guide-on-AI-Governance-and-Ethics-Generative-AI.pdf [Accessed 8th October 2026].

ASEAN. (2025b) Joint media statement: 17th Conference of the ASEAN Ministers Responsible for Information (AMRI) and 8th Conference of the AMRI Plus Three. Bandar Seri Begawan, Brunei Darussalam, 7th May. [Online]. Available at: https://asean.org/wp-content/uploads/2025/05/Adopted-JMS_17th_AMRIAnnex.pdf [Accessed 14th October 2026].

ASEAN Stats. (2024) *Exploring intra-ASEAN merchandise trade*. https://www.aseanstats.org/wp-content/uploads/2024/05/ASB-202405-03.pdf

Asia Centre. (2022) *Youth and Disinformation in Malaysia: Strengthening Electoral Integrity*. https://asiacentre.org/wp-content/uploads/Youth-and-Disinformation-in-Malaysia-Strengthening-Electoral-Integrity-1.pdf

Aspinall, E. (2019) *The polarisation paradox in Indonesia's 2019 elections*. New Mandala. https://www.newmandala.org/the-polarisation-paradox-in-indonesias-2019-elections/

Baker McKenzie. (2024) Malaysia: Licensing of social media and internet messaging service providers — from 1 January 2025 onwards. [Online]. Available at: https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/malaysia-licensing-of-social-media-and-internet-messaging-service-providers-from-1-january-2025-onwards [Accessed 13th October 2026].

Bank Negara Malaysia. (n.d.) Mule account. [Online]. Available at: https://www.bnm.gov.my/muleaccount [Accessed 13th October 2026].

Barlybaikyzy, Z. & Duisen, A. (2025) The EU approach to counter foreign digital interference. In: Qoraboyev, I. & Bekshora, Z. (eds.) CEGREG yearbook: Central Asia in global and regional governance. Maqsut Narikbayev University. pp. 59–90.

Bernama. (2022) Fake news, online provocations dropped after GE15 campaign period. Bernama, 24th November. [Online]. Available at: https://www.bernama.com/en/news.php?id=2141842 [Accessed 14th October 2026].

Bernama. (2025a) PDRM takes the lead at NSRC to strengthen online financial fraud crackdown. Bernama, 16th July. [Online]. Available at: https://www.bernama.com/en/general/news.php?id=2445804 [Accessed 13th October 2026].

Bernama. (2025b) Sabah polls: MCMC to collaborate with EC, police to monitor online campaign materials – Fahmi. Bernama, 16th October. [Online]. Available at: https://bernama.com/en/news.php?id=2479686 [Accessed 14th October 2026].

Bernama. (2026) PM Anwar launches 24-hour NSRC at MCMC Tower 2. Bernama, 3rd March. [Online]. Available at: https://bernama.com/en/news.php?id=2529896 [Accessed 14th October 2026].

Channel NewsAsia. (2026) AI-generated women on TikTok spread false or misleading information about Singapore and Malaysia. *Channel NewsAsia*, 13th July. https://www.channelnewsasia.com/singapore/tiktok-ai-women-disinformation-deepfake-presenters-6250271

China-Global South Project. (2025) China and U.S. put Malaysia's ASEAN-first neutrality to the test. [Online]. Available at: https://chinaglobalsouth.com/2025/09/21/china-us-malaysia-asean-first-neutrality-2024-trade-october-test/ [Accessed 8th August 2026].

Chinvanno, A. & Anantasirikia, S. (2024) Maritime security: Emerging challenges and their implications for ASEAN. International Studies Centre. 5, 1–5.

Chiu, C. (2024) PM Lee warns against responding to deepfake videos of him promoting investment scams. *The Straits Times*. https://www.straitstimes.com/singapore/pm-lee-warns-against-responding-to-deepfake-videos-of-him-promoting-investment-scams

Chongkittavorn, K. (2023) Combatting fake news the ASEAN way. Economic Research Institute for ASEAN and East Asia (ERIA). [Online]. Available at: https://www.eria.org/news-and-views/combatting-fake-news-the-asean-way [Accessed 12th August 2026].

Cyber Security Agency of Singapore (CSA). (2019) ASEAN member states agree to move forward on a formal cybersecurity coordination mechanism. 2nd October. [Online]. Available at: https://www.csa.gov.sg/news-events/press-releases/amcc-release-2019/ [Accessed 8th October 2026].

Da San Martino, G., Cresci, S., Barrón-Cedeño, A., Yu, S., Di Pietro, R. & Nakov, P. (2020) A survey on computational propaganda detection. Proceedings of the 29th International Joint Conference on Artificial Intelligence (IJCAI 2020). pp. 4826–4832. https://doi.org/10.24963/ijcai.2020/672

Del Vicario, M., Quattrociocchi, W., Scala, A. & Zollo, F. (2019) Polarization and fake news: Early warning of potential misinformation targets. *ACM Transactions on the Web*. 13 (2), 1–22.

Denisov, I., Paramonov, O., Arapova, E. & Safranchuk, I. (2021) Russia, China, and the concept of Indo-Pacific. *Journal of Eurasian Studies*. 12 (1), 72–85.

European Commission. (2019) *EU–China strategic outlook: Commission and HR/VP contribution to the European Council*. 21st March.

European External Action Service (EEAS). (2024) *Safeguarding democracy: Building resilience against identity-based disinformation*. https://www.eeas.europa.eu/eeas/safeguarding-democracy-building-resilience-against-identity-based-disinformation_en

European External Action Service (EEAS). (2026) Information integrity and countering foreign information manipulation & interference (FIMI). [Online]. Available at: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en [Accessed 12th August 2026].

Fakhruddin, F. (2023) Artificial intelligence, disinformation, and the 2024 Indonesian elections. *The Diplomat*, 16th November. https://thediplomat.com/2023/11/artificial-intelligence-disinformation-and-the-2024-indonesian-elections/

Fatmala, D. R., Amelia, A. & Trianingsih, F. A. (2020) Penggunaan akun bot media sosial untuk mempengaruhi opini publik: Sebuah tinjauan hukum di Indonesia. Ajudikasi: Jurnal Ilmu Hukum. 4 (1), 55–68. https://doi.org/10.30656/ajudikasi.v4i1.2210

Fintech News Malaysia. (2026) National Scam Response Centre moves to full 24-hour operations in Malaysia. Fintech News Malaysia, March. [Online]. Available at: https://fintechnews.my/56987/security/malaysia-scam-centre/ [Accessed 14th October 2026].

Fitriani, Kusumawati, N. P., Pandie, P. & Krisetya, B. (2024) *Regional and cross-border responses towards disinformation in Southeast Asia* [Policy brief]. Safer Internet Lab. https://saferinternetlab.org/wp-content/uploads/2024/04/Policy-Brief-Regional-and-Cross-Border-Responses-Towards-Disinformation-in-Southeast-Asia-.pdf

Galán-Cordero, C. & Cremades-Guisado, Á. (2026) From disinformation to foreign information manipulation and interference: Policy and legal challenges for European security. Frontiers in Political Science. 8, 1893048.

Galeotti, M. (2022) The weaponisation of everything: A field guide to the new way of war. New Haven, CT: Yale University Press.

Hamilton, R. E. (2025) Setting the stage: An overview of Chinese and Russian interests and influence in the Indo-Pacific. Foreign Policy Research Institute. 28th January. https://www.fpri.org/article/2025/01/setting-the-stage-an-overview-of-chinese-and-russian-interests-and-influence-in-the-indo-pacific/

Han, B. C. & Loh, B. (2022) *Malaysia: Beijing's global media influence 2022 country report*. Freedom House. https://freedomhouse.org/country/malaysia/beijings-global-media-influence/2022

Howe, S. (2024) Social media statistics for Malaysia [Updated 2024]. Meltwater. [Online]. Available at: https://www.meltwater.com/en/blog/social-media-statistics-malaysia [Accessed 12th August 2026].

Jalli, N. & Jamaluddin, K. (2024) Fortifying the ballot: Addressing disinformation and electoral integrity in Malaysia. ISEAS Perspective, 2024/72. [Online]. Available at: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-72-fortifying-the-ballot-addressing-disinformation-and-electoral-integrity-in-malaysia-by-nuurrianti-jalli-and-khairy-jamaluddin/ [Accessed 14th August 2026].

Kingdon, A. (2024) Socio-technical and multi-stakeholder approaches to countering online propaganda. In: The world white web: Uncovering the hidden meanings of online far-right propaganda. Cham: Springer Nature Switzerland, pp. 209–251.

Kuik, C.-C. (2024) Explaining hedging: The case of Malaysian equidistance. Contemporary Southeast Asia: A Journal of International and Strategic Affairs. 46 (1), 43–76.

Lam, D. (2026) Redirecting crypto exchanges to fight — rather than facilitate — crypto scams in Southeast Asia. ISEAS Perspective, 2026/43. ISEAS–Yusof Ishak Institute. [Online]. Available at: https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2026-43-redirecting-crypto-exchanges-to-fight-rather-than-facilitate-crypto-scams-in-southeast-asia-by-david-lam/ [Accessed 14th August 2026].

Lee, J. (2022) Chinese information and influence warfare in Asia and the Pacific. Hudson Institute. 14th September. https://www.hudson.org/national-security-defense/chinese-information-and-influence-warfare-in-asia-and-the-pacific

Legucka, A. & Kupiecki, R. (eds.) (2022) Disinformation, narratives and memory politics in Russia and Belarus. London: Routledge. https://doi.org/10.4324/9781003281597

Leong, P. P. Y. & Loh, B. Y. H. (2024) State-sponsored disinformation through digital media in Malaysia. In: *State-sponsored disinformation around the globe*. Routledge, pp. 287–301.

Lin, J., Fong, K. & Martinus, M. (2025) Malaysia chairs ASEAN at a strategic crossroads: Priorities, opportunities and challenges. Trends in Southeast Asia, 2025/12. ISEAS–Yusof Ishak Institute. [Online]. Available at: https://www.iseas.edu.sg/articles-commentaries/trends-in-southeast-asia/malaysia-chairs-asean-at-a-strategic-crossroads-priorities-opportunities-and-challenges/ [Accessed 14th August 2026].

Lu, Q. & Moorthy, R. (2026) Strategic responses and regional pressures: Malaysia in the US–China semiconductor competition. *The Pacific Review*. 39 (1), 177–207.

Luong, D. (2022) Internet blocks won't solve Southeast Asia's fake news problem. *Nikkei Asia*, 6th August. https://asia.nikkei.com/opinion/internet-blocks-won-t-solve-southeast-asia-s-fake-news-problem

Malaysiakini. (2021) *The Hong Kong infowar in Malaysia*. 11th August. https://pages.malaysiakini.com/hk-misinfo/en/

Malaysian Communications and Multimedia Commission (MCMC). (2026) Online Safety Act 2025: Risk Mitigation Code FAQ. [Online]. Available at: https://www.malaysianwireless.com/wp-content/uploads/2026/05/MCMC-FAQ-Risk-Mitigation-Code-RMC-22-May-2026-Online-Safety-Act-2025.pdf

Malaysian Investment Development Authority (MIDA). (2024) *Securing Malaysia's position in the global semiconductor supply chain*. https://www.mida.gov.my/mida-news/securing-malaysias-position-in-the-global-semiconductor-supply-chain/

Marino-Jiménez, M., Rodrich-Portugal, R., Aliaga-Lodtmann, C. & Ramos-Rugel, R. (2026) The endogenous threat: Adapting the FIMI framework to analyze state-directed information manipulation in fragile democracies. *Frontiers in Communication*. 11, 1739581.

Martinus, M. (2023) Can ASEAN mitigate fake news in Southeast Asia? Fulcrum, ISEAS–Yusof Ishak Institute. [Online]. Available at: https://fulcrum.sg/aseanfocus/af-can-asean-mitigate-fake-news-in-southeast-asia/ [Accessed 8th August 2026].x

McPherson, P. (2025) Exclusive: Fake accounts drove praise of Duterte and now target Philippine election. Reuters, 11th April. [Online]. Available at: https://www.reuters.com/world/asia-pacific/fake-accounts-drove-praise-duterte-now-target-philippine-election-2025-04-11/ [Accessed 14th August 2026].

Meta. (2021) December 2020 coordinated inauthentic behavior report. Meta Newsroom, 12th January. [Online]. Available at: https://about.fb.com/news/2021/01/december-2020-coordinated-inauthentic-behavior-report/ [Accessed 14th August 2026].

Mustaffa, S. (2025) Merdeka and misinformation: Did we skip a step? KRI Views 33/25. Khazanah Research Institute. [Online]. Available at: https://cdn.prod.website-files.com/684b55df28cddcbe52b406f2/68b94a428348ea52da840814_Views%20Merdeka_Did%20We%20Just%20Skip%20a%20Step.pdf [Accessed 8th August 2026].

Nasir, S. F. S., Fuad, A. F. A. & Johari, F. (2026) Civil-military coordination in CBRN response: A WOGOS approach for ASEAN resilience. International Journal of Research and Innovation in Social Science. 10 (6), 2248–2257.

Natea, M. D. (2022) Information and disinformation in the Ukrainian war. In: Natea, M. D. (ed.) Disinformation crossing borders: The multilayered disinformation concerning the war in Ukraine. Editions L'Harmattan.

National Cyber Security Agency (NACSA). (2026) National Security Council's Directive No. 26: National cyber security management. [Online]. Available at: https://www.nacsa.gov.my/directive26.php [Accessed 13th October 2026].

New Straits Times. (2026) Cybertroopers earn up to RM10,000 manipulating online narratives. New Straits Times, 24th May. [Online]. Available at: https://www.nst.com.my/news/nation/2026/05/1447073/cybertroopers-earn-rm10000-manipulating-online-narratives [Accessed 12th August 2026].

Nimmo, B., Eib, C. S. & Ronzaud, L. (2020) Operation Naval Gazing. Graphika. 22nd September. [Online]. Available at: https://www.graphika.com/reports/operation-naval-gazing [Accessed 14th August 2026].

Nitza-Makowska, A., Bhutia, K. D., Riether, D., Sinitsyna, A. & Süld, E. (2026) Is China losing its soft power in the Ukraine war? Evidence from the Indo-Pacific. *Asia Europe Journal*. 24 (1), 245–264.

Olalekan, O. A. (2024) Cryptocurrency and political campaign finance: Opportunities and risks. British Journal of Mass Communication and Media Research. 4 (4), 1–12. https://doi.org/10.52589/BJMCMR-7KRVPRV0

Parliament of Malaysia. (2001) Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613). [Online]. Available at: https://www.labuanfsa.gov.my/clients/asset_120A5FB8-61B6-45E8-93F0-3F79F86455C8/contentms/img/documents/Legislation_and_Guidelines/Legislation/Subsidiary_Legislation/Anti-Money-Laundering-Act-2001-Act-613.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2006a) Communications and Multimedia Act 1998 (Act 588). Reprint incorporating all amendments up to 1 January 2006. Commissioner of Law Revision, Malaysia. [Online]. Available at: https://www.importlicensing.wto.org/sites/default/files/members/91/Act%20No.588%20-%20Communications%20Multimedia%201998_01.01.2006.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2006b) Computer Crimes Act 1997 (Act 563). Reprint incorporating all amendments up to 1 January 2006. Commissioner of Law Revision, Malaysia. [Online]. Available at: https://database.cyberpolicyportal.org/api/files/16642786938881kdod8llv95.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2006c) Police Act 1967 (Act 344). Reprint incorporating all amendments up to 1 January 2006. Commissioner of Law Revision, Malaysia. [Online]. Available at: https://policehumanrightsresources.org/content/uploads/2016/03/Police-Act-Malaysia-1967.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2006d) Sedition Act 1948 (Act 15). Reprint incorporating all amendments up to 1 January 2006. Commissioner of Law Revision, Malaysia. [Online]. Available at: https://www.icnl.org/wp-content/uploads/Malaysia_SeditionMalay.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2011) Elections Act 1958 (Act 19). Online version of updated text of reprint, as at 1 December 2011. [Online]. Available at: https://aceproject.org/ero-en/regions/asia/MY/malaysia-elections-act-up-to-december-2011/at_download/file [Accessed 14th October 2026].

Parliament of Malaysia. (2012) Security Offences (Special Measures) Act 2012 (Act 747). [Online]. Available at: https://icj.org/wp-content/uploads/2012/12/Malaysia-Security-Offences-Special-Measures-Act-2012-eng.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2013) Penal Code (Act 574). Online version of updated text of reprint, as at 1 February 2013. [Online]. Available at: https://sherloc.unodc.org/cld/uploads/res/document/penal-code_2014_html/2014_Act_574_-_Penal_Code.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2016a) Election Offences Act 1954 (Act 5). Reprint, as at 1 December 2016. Commissioner of Law Revision, Malaysia. [Online]. Available at: https://www.globalbersih.org/wp-content/uploads/2020/04/Election-Offences-Act-1954-Act-5.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2016b) National Security Council Act 2016 (Act 776). Majlis Keselamatan Negara. [Online]. Available at: https://www.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/Akta-MKN-2016-BI.pdf [Accessed 13th October 2026].

Parliament of Malaysia. (2017) Criminal Procedure Code (Act 593). Online version of updated text of reprint, as at 1 September 2017. [Online]. Available at: https://www.forestry.gov.my/images/stories/pdf/Akta/Kanun%20Tatacara%20Jenayah%20CPC-%20BI.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2024a) Criminal Procedure Code (Amendment) Act 2024 (Act A1722). [Online]. Available at: https://lom.agc.gov.my/ilims/upload/portal/akta/outputaktap/2368175_BI/Act%20A1722.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2024b) Cyber Security Act 2024 (Act 854). [Online]. Available at: https://nacsa.gov.my/act854.php [Accessed 14th October 2026].

Parliament of Malaysia. (2024c) Penal Code (Amendment) Act 2024 (Act A1721). [Online]. Available at: https://lom.agc.gov.my/ilims/upload/portal/akta/outputaktap/2368163_BI/Act%20A1721.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2025) Online Safety Act 2025 (Act 866). [Online]. Available at: https://www.wccpenang.org/wp-content/uploads/2025/07/Online-Safety-Act-2025.pdf [Accessed 14th October 2026].

Parliament of Malaysia. (2026) Cybercrimes Bill 2026 [D.R.8/2026]. Dewan Rakyat. [Online]. Available at: https://www.parlimen.gov.my/files/billindex/pdf/2026/DR/Cybercrimes%20Bill%202026.pdf [Accessed 14th October 2026].

Parliament of Singapore. (2019) *Protection from Online Falsehoods and Manipulation Act 2019 (Act 18 of 2019)*. https://sso.agc.gov.sg/Act/POFMA2019

Personal Data Protection Commission Singapore (PDPC). (2024) Two guides unveiled at ADGMIN 2024. 2nd February. [Online]. Available at: https://www.pdpc.gov.sg/media-events/two-guides-unveiled-at-adgmin-2024 [Accessed 8th October 2026].

Proto, L., Lamoso-González, P. & Bouza García, L. (2025) The EU's FIMI turn: How the European Union External Action Service reframed the disinformation fight. Media and Communication. 13. https://doi.org/10.17645/mac.9474

Rahmat Lim & Partners. (2026) Cybercrimes Bill 2026: Closing the gaps in Malaysia's cybercrime legal framework. [Online]. Available at: https://www.rahmatlim.com/perspectives/articles/33326/mykh-cybercrimes-bill-2026-closing-the-gaps-in-malaysia-s-cybercrime-legal-framework [Accessed 13th October 2026].

Rakhmat, M. Z. & Purnama, Y. (2026) *The Global South needs its own definition of FIMI*. Global Policy Journal. https://www.globalpolicyjournal.com/blog/15/07/2026/global-south-needs-its-own-definition-fimi

Safer Internet Lab. (2024) Tackling rising cases of FIMI in Southeast Asia: Insights from IGF 2024. [Online]. Available at: https://saferinternetlab.org/tackling-rising-cases-of-fimi-in-southeast-asia-insights-from-igf-2024/ [Accessed 8th August 2026].

Saraswati, M. S. (2020) The political campaign industry and the rise of disinformation in Indonesia. In: Sinpeng, A. & Tapsell, R. (eds.) From grassroots activism to disinformation: Social media in Southeast Asia. Singapore: ISEAS–Yusof Ishak Institute. pp. 43–62.

Scott, D. (2018) The Indo-Pacific in US strategy: Responding to power shifts. *Rising Powers Quarterly*. 3 (2), 19–43.

Smith, R. & Perry, M. (2022) Fake news and the pandemic in Southeast Asia. *Australian Journal of Asian Law*. 22, 131.

Suci, P. (2024) Penanganan ujaran kebencian terhadap Presiden Jokowi di media sosial. *CoverAge: Journal of Strategic Communication*. 14 (2), 146–165.

Sukmani, K. N. A. & Aras, T. S. (2024) Cybertroops: Contestation and polarization in the perspective of critical discourse analysis. Legal Brief. 13 (2), 588–594. https://legal.isha.or.id/index.php/legal/article/view/964/677

Tan, N. & McIlvaney, A. (2025) Bots, buzzers and AI-driven campaigning distort democracy. East Asia Forum. [Online]. Available at: https://eastasiaforum.org/2025/07/25/bots-buzzers-and-ai-driven-campaigning-distort-democracy/ [Accessed 14th August 2026].

The Sun Malaysia. (2023) 16th AMRI endorses fake news and disinformation guidelines. The Sun Malaysia, 23rd September. [Online]. Available at: https://thesun.my/news/world-news/16th-amri-endorses-fake-news-and-disinformation-guidelines-nh11529136/ [Accessed 8th October 2026].

The Vibes. (2025a) Malaysia will not compromise on national security amid foreign agent activity, Fahmi says. The Vibes, 24th August. [Online]. Available at: https://www.thevibes.com/articles/news/111953/malaysia-will-not-compromise-on-national-security-amid-foreign-agent-activity-fahmi-says [Accessed 14th October 2026].

The Vibes. (2025b) Over 6,000 fraudulent online posts removed since 2023, says police. The Vibes, 30th October. [Online]. Available at: https://www.thevibes.com/articles/news/114806/over-6000-fraudulent-online-posts-removed-since-2023-says-police [Accessed 14th October 2026].

Treyger, E., Cheravitch, J. & Cohen, R. S. (2022) Russian disinformation efforts on social media. RAND Corporation. Report No. RR-4373/2-AF. https://doi.org/10.7249/RR4373.2

TRM Labs. (2024) *The crypto election: Crypto, disinformation, and presidential politics*. https://www.trmlabs.com/resources/blog/the-crypto-election-crypto-disinformation-and-presidential-politics

Watan & Merdeka Center for Opinion Research. (2022) *State sponsored influence operations in Malaysia*.

Wheatley, S. (2020) Foreign interference in elections under the non-intervention principle: We need to talk about "coercion". Duke Journal of Comparative & International Law. 31 (1), 161. https://scholarship.law.duke.edu/djcil/vol31/iss1/3



**Amirun Haqqim bin Eldeen HUSAINI** is a PhD researcher dually affiliated with the University of Nottingham Malaysia and the COMTESSA Competence Center (Core Competence Center for Operations Research, Management-Tenacity-Excellence, Safety & Security Alliance) at the University of the Bundeswehr Munich. His research sits at the intersection of computational social science and information warfare, with a particular focus on the detection, mapping, and modelling of disinformation campaigns and politically manipulative narratives across social media networks. His work contributes to broader efforts to understand how coordinated influence operations diffuse across digital information environments and the implications of such operations for democratic discourse and regional security.



**E Kin Zane Ryan SEOW** is a Fellow at Bait Al Amanah and an alumnus of Universiti Malaya, where he earned a Master of Public Policy. As a policy researcher whose work focuses extensively on Southeast Asian geopolitics, his background spans Track II initiatives concerning peacebuilding in Myanmar as well as maritime security dynamics in the South China Sea, with a specific emphasis on the vulnerabilities of critical subsea cable infrastructure. His current research on regional security sits at the intersection of critical infrastructure protection and cognitive security, focusing on the detection, mapping, and strategic implications of disinformation and misinformation within the ASEAN region



**Karisma Putera bin Abd RAHMAN** is Executive Director at Bait Al Amanah working at the intersection of foreign affairs, public policy, and political analysis. He is interested in how geopolitical developments shape the decisions faced by governments, businesses, and communities. Alongside research and analysis, Karisma contributes to partnership development and stakeholder engagement. He builds relationships across policy, business, academic and civil-society circles, bringing people and perspectives together to deepen understanding, identify shared interests and create opportunities for meaningful collaboration. Karisma holds a Master's degree in Public Policy from Universiti Malaya and a Bachelor's degree in International Political Economy from City St. George's, University of London



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.