



Disinformation Governance in Indonesia: A Non-Military Security Perspective and Comparative Insights from Singapore, Taiwan, and the European Union

Sintia Clara Aritonang^{1*}, Hikmat Zakky Almubaraq², Herlina Tarigan³
Indonesia Defense University

Corresponding Author: Sintia Clara Aritonang, sintiaclar2311@gmail.com

ARTICLE INFO

Keywords: Disinformation Management; Non-Military Threats; State Security; Digital Governance

Received : 27, July

Revised : 23, August

Accepted: 25, September

©2026 Aritonang, Almubaraq, Tarigan: This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

This study aims to analyze disinformation management as a non-military threat to Indonesia's national security by examining existing response mechanisms and challenges in digital platform governance. Using a descriptive qualitative approach and secondary data, this study examines the relationship between non-military security, disinformation, and digital platform governance. The findings indicate that Indonesia has developed various mechanisms to address disinformation, including content identification and clarification, fact-checking, digital literacy programs, public reporting mechanisms, and collaboration with digital platforms. However, these efforts remain largely focused on content-level responses, while challenges related to algorithmic transparency, recommendation systems, content moderation, and the systemic detection of disinformation require further attention. This study positions disinformation not merely as an information-related issue, but as a non-military threat to national security that requires integrated and systemic governance. The study emphasizes the need to strengthen disinformation management through a preventive, collaborative, and ecosystem-based approach involving the government, digital platforms, media, academics, fact-checkers, and the public to foster public trust and support national stability.

INTRODUCTION

The widespread use of social media has increased the capacity of both political and non-state actors to produce and disseminate manipulated information to the public on a large scale. Social media enables information to be produced and disseminated rapidly, at relatively low cost, and across national borders. However, these characteristics also create opportunities for state and non-state actors to exploit the digital space to systematically produce and disseminate misleading information. This condition demonstrates that state security in the digital era is confronted not only with physical and military threats but also with threats that operate through information and public perceptions. The World Economic Forum (2025) identifies misinformation and disinformation as among the most serious global risks in the short term, particularly because manipulated information can intensify polarization, undermine trust in institutions, and disrupt socio-political stability.

The scale of this threat can be observed through the development of social media manipulation campaigns across countries. Bradshaw et al., (2021) through the Oxford Internet Institute, found that organized social media manipulation campaigns had been identified in 81 countries in 2020, an increase from 70 countries in 2019. More than 76 of the 81 countries examined used disinformation as part of their political communication. These findings indicate that disinformation has evolved from an activity carried out primarily by individuals into a practice that may involve governments, political parties, interest groups, and strategic communication firms. In other words, the digital space has become a competitive arena for systematically influencing public opinion and political behavior (Bradshaw et al., 2021). This phenomenon is also reflected in the following survey data, which demonstrate the extent of public concern regarding this threat across different countries.

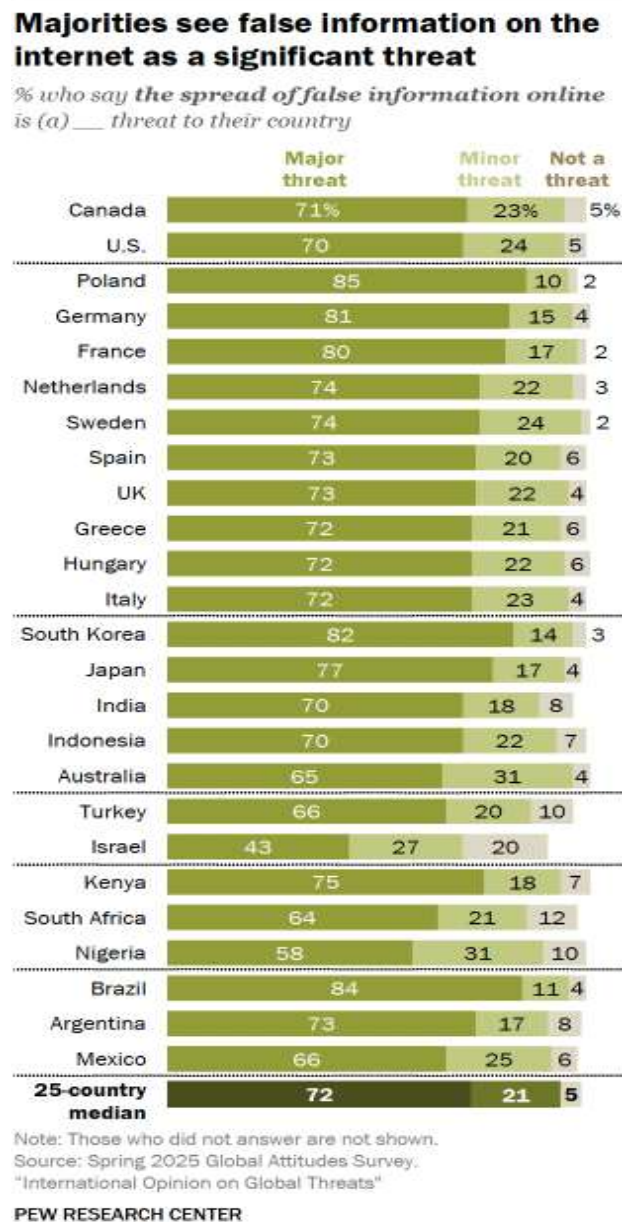


Figure 1. Public Perceptions of Internet-Based Disinformation as a Threat to State Security Across 25 Countries
Source: Pew Research Center (2025)

According to a Pew Research Center survey conducted across 25 countries in 2025, a median of 72% of respondents considered the spread of disinformation on the internet to be a major threat to their countries. This perception reached 85% in Poland, 84% in Brazil, 82% in South Korea, 81% in Germany, and 80% in France. Meanwhile, in Indonesia, 70% of respondents also viewed the spread of disinformation on the internet as a major threat to the country. These findings indicate that concerns about disinformation are not limited to academic research and policy discussions but have also developed into a widely perceived security threat among populations across different regions of the world (Pew Research Center, 2025).

This phenomenon has become increasingly evident across countries with different political contexts. For example, in India, Freedom House (2024) reported that information manipulation by political actors became a significant feature of the digital environment during the April June 2024 parliamentary elections. Political actors disseminated false or misleading information, while affiliated and non-affiliated networks amplified political narratives. In Karnataka, investigations identified a network of approximately 150,000 workers used to disseminate pro-government, anti-opposition, and anti-Muslim messages through WhatsApp. This case demonstrates that disinformation can extend beyond political manipulation to threaten social cohesion and public security. A similar threat can be observed in Ukraine and Europe through Foreign Information Manipulation and Interference (FIMI). The European External Action Service (EEAS, 2025) reported that foreign actors, particularly Russia and to some extent China, exploited digital infrastructure to manipulate the information environment in the European Union. The case of Ukraine further shows that disinformation can target public perceptions of government, foreign policy, and state legitimacy, making the information environment a strategic domain that complements military instruments. A similar pattern occurred in the United Kingdom, where the government sanctioned actors linked to Russia's Doppelganger network, which operated at least 120 fake websites resembling legitimate news and government sites.

This phenomenon can also be observed in countries with high levels of digital penetration, such as Indonesia. According to data from the Indonesian Internet Service Providers Association (Asosiasi Penyelenggara Jasa Internet Indonesia APJII), the number of internet users in Indonesia reached 221,563,479, with an internet penetration rate of 79.5%. The large number of people connected to the internet has made the digital space an important part of Indonesia's social and political life. The expansion of Indonesia's digital environment has also been accompanied by a high prevalence of information-related disturbances. The Indonesian Anti-Defamation Society (Mafindo) recorded 2,119 hoax findings in the first half of 2024, compared with 1,185 findings during the same period in 2023. Of these findings, 1,037 cases, or 48.9%, were related to political issues. These data are particularly significant from a state security perspective because manipulated information in a political context has the potential to influence public perceptions of candidates, electoral processes, and government institutions.

Previous studies have examined disinformation from different perspectives. Bradshaw and Howard (2021) focused on the use of social media manipulation in political communication, while Ahmad (2022) examined the role of social media algorithms in shaping disinformation and political polarization in Indonesia. Alamsyah et al. (2024) highlighted challenges in fact-checking practices, whereas Saputra et al. (2024) demonstrated the role of digital literacy and fact-checking skills in improving people's ability to recognize disinformation. However, these studies have not sufficiently addressed disinformation governance as a non-military security issue, particularly in relation to digital platform governance, algorithmic

transparency, recommendation systems, and content moderation. This study addresses this gap by examining disinformation governance in Indonesia from a non-military security perspective, with several countries as comparative references.

Based on this background, a key issue that requires attention is the capacity of states to manage this threat. Various countries have developed mechanisms for fact-checking, digital platform regulation, social media monitoring, digital literacy, and interinstitutional cooperation. However, technological developments have also made disinformation actors increasingly adaptive. Okeke and Omosotomhe (2025) demonstrate that responses to disinformation are still frequently reactive, while the speed of dissemination and the ability of disinformation actors to develop new methods can reduce the effectiveness of government responses. Therefore, the challenge facing states is not merely how to remove false information, but how to build systems capable of continuously preventing, detecting, identifying, responding to, and mitigating information manipulation operations. The novelty of this study lies in integrating content management, digital platform governance, and societal resilience into a single framework for disinformation governance as a non-military security response. This approach extends Indonesia's existing content-focused responses by addressing platform-level challenges, particularly algorithmic transparency, recommendation systems, content moderation, and systemic detection, supported by comparative insights from Singapore, Taiwan, and the European Union.

LITERATURE REVIEW

Previous studies have examined disinformation from political, social, and technological perspectives. Bradshaw and Howard (2021) highlighted the use of social media manipulation in political communication, while Ahmad (2022) examined how social media algorithms can contribute to disinformation and political polarization in Indonesia. Alamsyah et al. (2024) emphasized the role and challenges of fact-checking, whereas Saputra et al. (2024) demonstrated that digital literacy and fact-checking interventions can improve people's ability to recognize disinformation. Other studies have also linked disinformation to national security, social resilience, and political stability (Sarjito, 2024; Njagi, 2025). However, existing literature has paid less attention to disinformation governance as a non-military security issue, particularly regarding algorithmic transparency, recommendation systems, content moderation, and systemic platform governance. This study addresses this gap by examining Indonesia's disinformation management and comparing it with approaches in Singapore, Taiwan, and the European Union.

METHODOLOGY

This study employs a descriptive qualitative approach using secondary data. According to John W. Creswell, qualitative research enables researchers to explore social phenomena in depth, including how information technology facilitates the dissemination of inaccurate information within society. The data used in this study consist of secondary data, including research reports, journal

articles, government data, policy documents, and social media sources related to the dissemination of hoaxes and disinformation. The data were collected by examining national and international scholarly journals, data from the Ministry of Communication and Digital Affairs (Komdigi), and reports from civil society organizations such as the Indonesian Anti-Defamation Society (MAFINDO), as well as relevant government policies and institutional reports. Data were analyzed using content analysis to identify the forms, impacts, and management strategies associated with disinformation as a non-military threat to state security. The secondary data were selected based on their relevance to disinformation management, non-military security, digital platform governance, digital literacy, and societal resilience. The analysis focused on content management, digital platform governance, and societal resilience, while comparative analysis was conducted using Singapore, Taiwan, and the European Union as comparative references.

RESEARCH RESULT AND DISCUSSION

State Security from a Non-Military Perspective

Changes in the nature of threats have led the concept of security to evolve into a multidimensional framework that is directly connected to the well-being of states and societies. The Indonesian Ministry of Defense, through the WIRA magazine in 2015, explained that national security constitutes one of the fundamental pillars of statehood, as the state has an obligation to ensure both the security and welfare of its people. From this perspective, national security is understood as a dynamic condition of the nation and the Unitary State of the Republic of Indonesia that ensures the safety, peace, and welfare of citizens, society, and the nation; protects national sovereignty and territorial integrity; and ensures the continuity of national development against various threats (Bambang Eko S. 2015). This perspective reinforces the argument that national security from a non-military perspective is fundamentally oriented toward the state's capacity to identify and reduce various vulnerabilities that may undermine national stability. Non-military threats differ from military threats because they do not necessarily manifest as direct attacks on a state's territory. Such threats may develop through social, political, economic, cultural, and technological processes that gradually affect societal conditions and the capacity of state institutions. Therefore, safeguarding national security requires an integrated approach and cannot rely solely on military power (Bambang Eko S., 2015).

From a comprehensive security perspective, security is determined not only by military capabilities but also by political stability, economic resilience, social cohesion, and the state's capacity to address various vulnerabilities emerging within society (Acharya, 2011). This perspective indicates that state security is fundamentally concerned with the ability of the state and society to maintain stability, ensure the continuity of government functions, and protect public safety from various forms of disruption, whether physical or non-physical.

In the Indonesian context, this broader security perspective is reflected in the concept of non-military defense. The Indonesian Ministry of Defense (2025)

explains that non-military defense constitutes a strategic component of the national defense system aimed at safeguarding national unity, sovereignty, and the safety of the nation through non-physical instruments. The threats faced by the state in this context are multidimensional, encompassing socio-cultural, political, information technology, economic, and health-related domains. Non-military defense is also not solely the responsibility of the government but requires the involvement of all elements of society through improvements in human resource quality, technological capacity, infrastructure development, strengthening national character, and enhancing digital literacy (Susanti, 2025). Non-military threats do not necessarily seek to directly destroy the state but may exploit internal vulnerabilities within society and state institutions. The Ministry of Defense, for example, identifies horizontal conflicts arising from identity-based provocation, political manipulation through disinformation that can undermine public trust in the government, cybercrime, the spread of hoaxes, and propaganda as forms of threats emerging in the political and information technology domains (Susanti, 2025). Thus, threats to state security can operate through more indirect mechanisms, namely by influencing how people obtain information, shaping public perceptions, determining political attitudes, and assessing the credibility of state institutions.

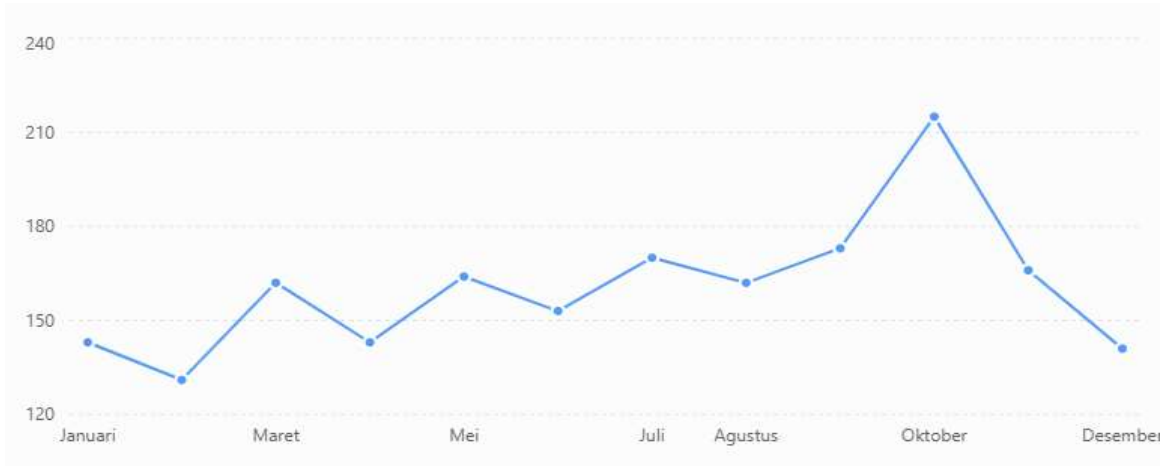
The Indonesian Ministry of Defense also explains that non-military threats may have ideological, political, economic, socio-cultural, technological, public safety, and legislative dimensions, all of which can undermine national defense. Given the increasingly broad nature of these threats, addressing them cannot rely solely on military defense instruments. Instead, government ministries and agencies outside the defense sector serve as the primary actors or leading sectors in addressing non-military threats according to the nature and characteristics of the threats involved (Ministry of Defense of the Republic of Indonesia, 2023). The non-military perspective also places society as an important component of state security. The state is not only responsible for protecting its territory and institutions but also for ensuring that society has a sense of security, well-being, and access to trustworthy information. This demonstrates the close relationship between state security and societal resilience. The stronger society's capacity to withstand social, economic, technological, and information-related pressures, the greater the state's capacity to maintain national stability (Rahayu et al., 2024).

Disinformation as a Threat to State Security

Disinformation refers to the intentional dissemination of false or misleading information aimed at influencing public perceptions and creating confusion. These characteristics make disinformation a form of non-military threat, as its effects can undermine political, social, and economic stability, as well as public trust in state institutions (Sarjito, 2024; Njagi, 2025).

Evidence of the significant role of social media in the dissemination of disinformation is provided by Sarjito (2024), who found that approximately 70% of hoaxes were disseminated through Facebook and WhatsApp. This finding is further supported by Vosoughi et al. (2018), who demonstrated that

false news spreads faster and reaches a wider audience than true information on social media. In the Indonesian context, this issue is particularly relevant given the high intensity of digital space usage in people's daily lives. The Ministry of Communication and Digital Affairs recorded 1,923 hoax contents that were identified and clarified throughout 2024. The details of these contents



are presented below.

Figure 2. Distribution of Disinformation Content by Category in 2024
Source: Komdigi (2025), processed by the authors

The distribution of these disinformation contents across categories is presented below



Figure 3. Distribution of Disinformation Findings by Category
Source: Komdigi, 2025

These data are particularly significant from a state security perspective because the political and government-related categories are directly associated with public perceptions of political processes and public institutions. This indicates that the dissemination of misleading information in the digital space can extend beyond individual misunderstanding and potentially affect the

relationship between society and the state. When false information concerning government, public policies, or political processes is disseminated on a large scale, people may form judgments based on inaccurate information. Over the long term, such conditions can erode public trust and intensify social polarization.

The significance of this threat is also reflected in the Global Risks Report 2025 published by the World Economic Forum (WEF). Based on the Global Risks Perception Survey, *misinformation and disinformation* were once again ranked as the number one global risk over the next two years, through 2027, marking the second consecutive year in which they have occupied the top position. This vulnerability is also evident at the individual level. The Reuters Institute Digital News Report 2025, based on nearly 100,000 interviews with online news consumers across 48 markets, found that 58% of respondents globally were concerned about their ability to distinguish between accurate and inaccurate information online. This level of concern reached 73% in Africa and the United States, while it stood at 46% in Western Europe. The report also found that *online influencers/personality figures* and national politicians were each identified by 47% of respondents as major sources of false or misleading information. These findings demonstrate that disinformation is not merely a matter of the existence of false content but also concerns people's ability to evaluate the information they encounter within the digital environment.

The position of disinformation as a non-military threat becomes even clearer when its effects are examined as a gradual process. Disinformation can begin with the manipulation of information, which subsequently influences public perceptions, erodes trust in institutions, intensifies social polarization, and, under certain conditions, disrupts national stability and resilience.



Figure 4. The Pathway of Disinformation's Impact on State Security
Source: processed by the author, 2026.

Managing Disinformation Across Countries

Disinformation management across countries reflects a broader shift from reactive responses toward more systematic and multidimensional approaches. From a non-military security perspective, this shift demonstrates that threats to the state can emerge from the information environment and do not necessarily take the form of direct attacks. Kashuri (2024) identifies cybersecurity, societal resilience, strategic communication, and government cooperation with non-state actors as important components of non-military defense.

Singapore has adopted a relatively robust approach that combines regulatory measures, information clarification, and efforts to strengthen public media literacy. One of its key instruments is the Protection from Online Falsehoods and Manipulation Act (POFMA), which enables the government to issue correction directions for information deemed to contain falsehoods (Protection from Online Falsehoods and Manipulation Act, 2019). Rather than relying solely on the removal of misleading content, this approach also provides the public with corrective information to counter false narratives. It is complemented by initiatives aimed at strengthening people's ability to evaluate information, including the S.U.R.E. (Source, Understand, Research, Evaluate) media literacy programme. Singapore's approach therefore combines government-led regulatory intervention with efforts to strengthen the public's capacity to identify and critically evaluate inaccurate information.

The European Union takes a more collaborative approach to disinformation management, involving governments, digital platforms, fact-checkers, researchers, and civil society. The Code of Practice on Disinformation, strengthened in 2022, includes measures to demonetize disinformation actors, improve transparency in political advertising, empower users, strengthen fact-checking, and provide researchers with access to relevant data (European Commission, 2022). In February 2025, the European Commission and the European Board for Digital Services formally incorporated the Code of Practice on Disinformation into the Digital Services Act (DSA) framework as the Code of Conduct on Disinformation. The code now serves as a reference for assessing and mitigating disinformation-related risks on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) (European Commission, 2025).

Taiwan takes a somewhat different approach by placing greater emphasis on building societal resilience against disinformation. Its approach brings together government agencies, media organizations, fact-checkers, civil society groups, and civic-tech communities (Ministry of Digital Affairs Taiwan, 2023; Huang & Chou, 2025). The government not only works to correct misleading information but also seeks to provide accurate information quickly and transparently, allowing the public to access trusted sources when misleading narratives emerge (Executive Yuan, 2017; Ministry of Digital Affairs Taiwan, 2023). This approach reflects the broader idea of societal resilience, which emphasizes the ability of communities to adapt to and recover from disruptions as an important part of non-military security (OECD, 2024).

Similarly, Kashuri (2024) identifies societal resilience as an important element in addressing non-military threats.

Singapore, Taiwan, and the European Union were selected as comparative references because they represent distinct approaches to disinformation governance that are relevant to Indonesia's challenges. Singapore places greater emphasis on government regulation and intervention, making it relevant for examining government capacity in content management, while Taiwan focuses on societal resilience, public participation, digital literacy, and collaboration with non-state actors. The European Union, in contrast, emphasizes collaborative and systemic governance involving digital platforms, particularly through platform accountability, transparency, and systemic risk management, which is relevant to Indonesia's challenges in algorithmic transparency, recommendation systems, content moderation, and systemic detection. The comparison highlights that, despite these different priorities, all three approaches recognize the importance of early detection, information verification, public communication, digital literacy, and cross-sector coordination. This broader pattern supports Kashuri's (2024) argument that effective non-military defense requires the integration of cybersecurity, societal resilience, public-private partnerships, and strategic communication, while providing relevant insights for strengthening Indonesia's integrated approach to disinformation governance.

Managing Disinformation in Indonesia

Indonesia has implemented several measures to address disinformation, but these efforts remain relatively fragmented. Ahmad (2022) argues that the growth of social media and algorithmic mechanisms in Indonesia can create a "disinformation order" and "algorithmic trap," which may intensify political polarization and undermine national narratives and democratic norms. Against this backdrop, disinformation management in Indonesia can be examined through several key dimensions.

Early Detection and Clarification of Disinformation

One of the most visible aspects of Indonesia's response to disinformation is the government's effort to identify and clarify hoax-related content. This mechanism is supported by the activities of the Ministry of Communication and Digital Affairs through its AIS Team under the Content Control Sub-Directorate, which monitors online content and investigates information suspected of being hoaxes, misinformation, or disinformation (Komdigi, 2025).

As noted earlier, a total of 1,923 hoax-related contents were identified and clarified throughout 2024. This monitoring process continues through the AIS Team, with clarification results disseminated through government communication channels to help the public distinguish content classified as hoaxes or disinformation (Komdigi, 2026). Data from the Public Information and Documentation Management Office (PPID) of the Central Java Provincial Office of Communication, Informatics, and Digital Affairs, based on AIS Team records, show that 1,017 issues were identified between January and August 2026, with the following distribution:



Figure 5. Trends in Hoaxes and Disinformation in 2026

Source: AIS Team, Ministry of Communication and Digital Affairs (Komdigi), 2026; data processed by the author.

The data indicate that disinformation detection is an ongoing process, as dozens to more than a hundred new issues are identified each month and require verification and clarification to the public (AIS Team, Komdigi, 2026). The mechanism also shows that the government's disinformation management efforts extend beyond political issues to other sectors that may influence public perceptions. For example, in June 2026, the clarification records included claims concerning a global power outage, the Free Nutritious Meals Program, government officials, and WhatsApp accounts impersonating prosecutors' office officials (AIS Team, Komdigi, 2026). Thus, identification and clarification serve as an initial government response to contain the spread of false information before it develops into a broader societal issue (Alamsyah et al., 2024).

Disinformation detection and clarification also involve fact-checking organizations and the media, indicating that responses to disinformation do not rely solely on government efforts. Alamsyah et al. (2024) highlight the important role of fact-checking organizations in investigating and assessing the accuracy of information circulating on digital platforms. Their study found that fact-checking practices in Indonesia have not kept pace with the rapid production and dissemination of disinformation, indicating the need for greater coordination and resources among government institutions, fact-checking organizations, the media, and civil society to address disinformation effectively (Alamsyah et al., 2024).

In addition, public reporting mechanisms form part of the identification system, as the government provides reporting channels through AduanKonten for people who encounter information of questionable accuracy, including email, social media accounts, and instant messaging applications (Komdigi, 2025). This means that the identification process is not entirely top-down, as it also provides opportunities for the public to serve as an early source of information about potentially misleading content. This mechanism is important because it demonstrates that identification and clarification are necessary initial

responses, but they are not sufficient to address the broader disinformation ecosystem.

Digital Literacy as a Strategy for Preventing Disinformation

The Indonesian government has positioned digital literacy as a preventive strategy for addressing disinformation by strengthening the public's ability to access, understand, and critically evaluate digital information. Through the Ministry of Communication and Digital Affairs (Komdigi), the government implements the National Digital Literacy Movement (GNLD) under the *Indonesia Makin Cakap Digital* initiative, which is built around four key pillars: digital skills, digital ethics, digital safety, and digital culture (Komdigi, 2023). This approach has been further developed through the *Cakap Digital, Aman Digital, Budaya Digital, dan Etika Digital* (CABE) framework, which serves as a national framework for digital literacy. The program is designed not only to improve people's ability to use digital technologies but also to promote safe, responsible, and ethical engagement with the digital environment amid the growing risks of disinformation and other online threats (BPSDM Komdigi, 2025).

Beyond public education, the Indonesian government uses the Indonesia Digital Society Index (IMDI) to assess the development of digital capabilities across the country. In 2024, the national IMDI score reached 43.34, while the digital skills sub-index increased to 58.25 from 56.59 in 2023, with the assessment covering 514 districts and municipalities nationwide (BPSDM Komdigi, 2024). These figures indicate an improvement in the digital capabilities of Indonesian society, although the national score suggests that further efforts are still needed to strengthen digital capacity and resilience. In the context of disinformation management, these programs are important because the government is not only seeking to remove false information after it has circulated but also to strengthen the public's ability to identify reliable sources, think critically, verify information, and refrain from sharing unverified content. The effectiveness of this preventive approach is supported by Saputra et al. (2024), who conducted a cluster-randomized controlled trial involving 325 students from nine classes across three areas in Central Java. Their findings demonstrate that digital literacy and fact-checking interventions can strengthen individuals' ability to recognize and respond to disinformation.

Thus, the government's role in promoting digital literacy can be understood as a preventive layer within Indonesia's broader disinformation management system. The government has established various initiatives, including mass education programs, training, the development of digital literacy facilitators, digital competency assessments, and the integration of information verification skills. However, the growing number of programs and participants does not necessarily indicate that all segments of society have developed equal capacity to respond to disinformation. Digital literacy therefore needs to move beyond basic technological proficiency toward critical abilities to verify and assess information, particularly as disinformation

increasingly spreads through social media, deepfakes, and AI-generated content (Komdigi, 2025).

These findings indicate that digital literacy functions not only as an educational program but also as a societal resilience mechanism within disinformation governance. A resilient society is better positioned to verify information, recognize misleading narratives, and avoid contributing to their further dissemination. However, the existence of digital literacy programs does not eliminate the need for stronger institutional and platform-level responses. Societal resilience therefore needs to operate together with content management and digital platform governance rather than being treated as a separate preventive measure.

Digital Platform Governance: Challenges in Indonesia's Disinformation Management

A more fundamental challenge concerns the governance of digital platforms. Law No. 1 of 2024, which amends the Electronic Information and Transactions Law (ITE Law) for the second time, requires Electronic System Providers (Penyelenggara Sistem Elektronik – PSE) to fulfill several obligations, including moderating illegal content and making necessary adjustments to their electronic systems (Republic of Indonesia, 2024). However, the *Policy Paper: Roadmap for Disinformation Management in Indonesia 2026* points out that the current regulatory framework remains broad and does not yet provide clear standards for transparency in recommendation systems, the formation of echo chambers, or the mechanisms through which sensational content can gain greater visibility (Tobing et al., 2026). This regulatory gap is particularly relevant given the changing ways in which disinformation circulates online. Wulandari et al. (2025), for example, found that during the 2024 Indonesian elections, disinformation increasingly spread through video-based platforms such as TikTok, with video content becoming more prominent than in the 2019 election. Government data further illustrate the scale and cross-platform nature of the problem, recording 1,325 disinformation contents on Facebook, 947 on X, 342 on TikTok, 198 on Instagram, 36 on SnackVideo, and 34 on YouTube during the 2024 election period (Ministry of Communication and Informatics, 2024). The distribution of disinformation across multiple platforms suggests that addressing the problem requires more than detecting and removing individual pieces of content; it also requires stronger attention to how digital platforms shape the visibility, recommendation, and spread of information.

The Indonesian government has also worked with digital platforms to curb the spread of disinformation. One example is the partnership between the General Elections Supervisory Agency (Bawaslu) and TikTok ahead of the 2024 elections to provide accurate electoral information and address content that violated the platform's policies (Freedom House, 2024). However, such partnerships have not fully addressed challenges at the systemic level. Transparency surrounding algorithms, content recommendation systems, and moderation practices remains a significant issue in digital platform governance (Komdigi, 2026). Research on trolls and disinformation during the 2024 elections similarly found that existing regulations were not yet sufficient to

mitigate the negative effects of disinformation, highlighting the need for greater transparency in political advertising and stronger early-detection mechanisms (Nurdin, 2024). The challenge in Indonesia, therefore, is not simply a lack of regulation, but a persistent gap between regulatory requirements and the capacity to oversee how digital platforms operate internally.

The government has begun to recognize these limitations and is gradually shifting its approach from content control toward system-level governance. In 2026, the Ministry of Communication and Digital Affairs (Komdigi) emphasized that effective platform governance should encompass transparency, accountability, a stronger legal framework, systemic risk assessment, and meaningful engagement among government institutions, digital platforms, academics, the media, and civil society (Komdigi, 2026). This shift is important because regulations focused primarily on removing individual pieces of content do not fully address how disinformation is produced, amplified, and systematically distributed across the digital ecosystem (Komdigi, 2026).

Overall, the main weakness in Indonesia's approach to disinformation management lies in platform-level governance, particularly in relation to algorithmic transparency, content recommendation systems, content moderation, and the capacity to detect disinformation at a systemic level. Evidence of widespread disinformation across multiple platforms suggests that government efforts need to move beyond a "detect and remove" approach toward one that addresses systemic risks within the broader digital ecosystem (Wulandari et al., 2025; Nurdin, 2024). This shift is particularly important from a non-military security perspective, as disinformation circulating through digital platforms can undermine public trust, deepen social polarization, and weaken the legitimacy of democratic processes (Nurdin, 2024).

Comparative Analysis of Disinformation Management

To assess Indonesia's position in disinformation management, the following comparative analysis examines differences in approaches, management mechanisms, as well as the strengths and limitations of Indonesia's framework in comparison with those of Singapore, Taiwan, and the European Union. The comparison is presented in Table 1 and serves as a basis for identifying practices that may inform efforts to strengthen Indonesia's disinformation management system.

Table 1. Comparative Strategies for Disinformation Management

Aspect	Indonesia	Singapore	European Union	Taiwan
Main approach	Combination of approaches	Regulatory	Collaborative	<i>Societal resilience</i>
Key instruments	Clarification, fact-checking,	POFMA and Correction Directions	DSA and Code of Practice	Government agencies, fact-checkers,

	digital literacy, and regulation			civic-tech communities, and the public
Primary focus	Content management and digital literacy	Government-led information correction	Systemic platform risks	Societal resilience
Strengths	Multiple instruments and response mechanisms	Strong regulatory response	More systematic platform accountability	Strong engagement of society and non-state actors
Key limitations	Digital platform governance remains a major challenge	Potential for excessive government control	Complex implementation across actors and member states	Relies heavily on public participation

Source: processed by the author, 2026

The comparative analysis indicates that Indonesia has established several important components of disinformation governance, particularly content identification and clarification, fact-checking, digital literacy, public reporting, and cooperation with digital platforms. However, these mechanisms remain more strongly oriented toward responding to individual pieces of problematic content than toward managing the broader digital environment in which disinformation is produced, amplified, and circulated. This distinction is important because the effectiveness of disinformation governance depends not only on the ability to identify false information, but also on the capacity to address the structural conditions that facilitate its dissemination.

Compared with the three comparative cases, Indonesia's main area for improvement lies in strengthening the integration between content-level responses, societal resilience, and platform governance. The Singapore experience highlights the importance of clear regulatory and corrective mechanisms; Taiwan demonstrates the role of public participation, media engagement, and societal resilience; while the European Union illustrates the importance of platform accountability, transparency, and systemic risk management. These approaches provide complementary lessons for Indonesia rather than models that can be adopted directly, given differences in institutional structures, regulatory environments, and societal contexts.

For Indonesia, the most significant implication is the need to strengthen platform-level governance as a complement to existing identification, clarification, fact-checking, and literacy measures. Greater attention is required to how recommendation systems, content moderation, platform transparency, and other digital mechanisms can contribute to the amplification of

disinformation. Strengthening these aspects would enable Indonesia to move beyond a predominantly reactive approach toward a more preventive and integrated governance framework. Such an approach would connect government regulation, platform accountability, fact-checking institutions, and societal resilience as complementary elements of non-military security governance.

CONCLUSIONS AND RECOMMENDATIONS

This study demonstrates that disinformation is not merely a matter of false information circulating online but constitutes a non-military security risk that can shape public perceptions, undermine trust in institutions, and affect national stability. Disinformation management is therefore an important component of state security beyond conventional military approaches. Indonesia has developed a range of mechanisms to address disinformation, including content identification and clarification, fact-checking, digital literacy initiatives, public reporting mechanisms, and cooperation with digital platforms. However, these efforts have not yet been fully integrated, particularly in areas such as platform governance, algorithmic transparency, content moderation, and the early detection of disinformation patterns.

The comparative analysis of Singapore, the European Union, and Taiwan shows that effective disinformation management requires the integration of regulatory measures, platform accountability, fact-checking, public communication, and societal resilience. Indonesia therefore needs to move beyond a predominantly content-focused response toward a broader approach to managing risks across the digital ecosystem. This requires stronger collaboration among government institutions, digital platforms, the media, academics, fact-checking organizations, and the public. Such an approach can help reduce vulnerabilities within the information environment before disinformation develops into a broader threat to public trust and national stability.

ADVANCED RESEARCH

This study is limited by its reliance on secondary data and a descriptive qualitative approach, which restricts direct evaluation of the effectiveness of disinformation management in Indonesia. The study also relies on selected comparative cases from Singapore, Taiwan, and the European Union, whose regulatory and institutional contexts differ from Indonesia. In addition, the analysis of platform governance is based on available public information and does not directly examine internal platform systems or algorithms. Future research could incorporate primary data and empirical assessments to evaluate the effectiveness of disinformation governance and platform-level interventions.

REFERENCES

- Acharya, A. (2011). Norm subsidiarity and regional orders: Sovereignty, regionalism, and rule-making in the Third World. *International Studies Quarterly*, 55(1), 95–123. <https://doi.org/10.1111/j.1468-2478.2010.00637.x>
- Ahmad, N. (2022). Disinformation order and social media algorithmic trap: New challenges for sustainability of the Indonesia's united nation-state narrative and liberal democratic norms. *Politik Indonesia: Indonesian Political Science Review*, 7(2), 134–149. <https://doi.org/10.15294/ipsr.v7i2.37261>
- Alamsyah, P., Hakim, L. N., Wijaya, G., & Wicaksono, A. (2024). Debunking disinformation on YouTube: A fact check on the 2024 Indonesian election. *Jurnal Studi Komunikasi*, 8(3), 547–560. <https://doi.org/10.25139/jsk.v8i3.8348>
- Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). APJII jumlah pengguna internet Indonesia tembus 221 juta orang. <https://web.apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>
- Badan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Digital. (2024). Indeks Masyarakat Digital Indonesia 2024. Kementerian Komunikasi dan Digital Republik Indonesia.
- Badan Pengembangan Sumber Daya Manusia Kementerian Komunikasi dan Digital. (2025). Program literasi digital nasional. Kementerian Komunikasi dan Digital Republik Indonesia.
- Bambang Eko S. (2015). Urgensi UU Kamnas dalam sistem ketatanegaraan Indonesia. WIRA: Media Informasi Kementerian Pertahanan, Edisi Khusus 2015. Kementerian Pertahanan Republik Indonesia.
- Bradshaw, S., Bailey, H., & Howard, P. N. (2021). Industrialized disinformation: 2020 global inventory of organized social media manipulation. Oxford Internet Institute, University of Oxford. <https://demtech.oii.ox.ac.uk/wpcontent/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf>
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.
- European External Action Service. (2025). 2025 report on EEAS activities to counter foreign information manipulation and interference (FIMI). European Union.
- Freedom House. (2024). Freedom on the Net 2024: India. <https://freedomhouse.org/country/india/freedom-net/2024>
- Huang, K.-S., & Chou, M. (2025). Resilience in truth: Public-private collaboration in Taiwan's response to disinformation. Research Institute for Democracy, Society and Emerging Technology. <https://dset.tw/en/research/resilience-in-truth-public-privatecollaboration-in-taiwans-response-to-disinformation/>
- Kashuri, M. (2024). Benchmark kebijakan pertahanan non militer dari berbagai negara: Sebuah review. JISIP UNJA: Jurnal Ilmu Sosial dan Ilmu Politik

- Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Status literasi digital di Indonesia 2023. Kementerian Komunikasi dan Informatika Republik Indonesia.
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2024). Data konten disinformasi selama Pemilu 2024. Kementerian Komunikasi dan Informatika Republik Indonesia.
- Kementerian Pertahanan Republik Indonesia. (2023). Ancaman nonmiliter dan penanganannya dalam sistem pertahanan negara. Kementerian Pertahanan Republik Indonesia.
- Kementerian Pertahanan Republik Indonesia. (2025). Kebijakan publik dalam kerangka pertahanan nirmiliter guna menghadapi ancaman non-militer. Direktorat Jenderal Potensi Pertahanan. <https://www.kemhan.go.id/pothan/2025/09/17/kebijakan-publik-dalam-kerangka-pertahanan-nirmiliter-guna-menghadapi-ancaman-non-militer>
- Kementerian Komunikasi dan Digital Republik Indonesia. (2025). Data dan penanganan konten hoaks/disinformasi tahun 2024. Kementerian Komunikasi dan Digital Republik Indonesia.
- Kementerian Komunikasi dan Digital Republik Indonesia. (2026). Menuju tata kelola platform yang lebih transparan dan akuntabel. <https://www.komdigi.go.id/berita/siaran-pers/detail/menuju-tata-kelola-platform-yang-lebih-transparan-dan-akuntabel>
- Masyarakat Anti Fitnah Indonesia. (2024). Lanskap hoaks 2024: Semester 1. Mafindo.
- Matanji, F., Tully, M., Mudavadi, K. C., Diop, L., & Madrid-Morales, D. (2024). Media literacy and fact-checking as proactive and reactive responses to misinformation in Kenya and Senegal. *Journal of Media Literacy Education*, 16(3), 1-18. <https://doi.org/10.1080/23743670.2024.2401782>
- Ministry of Digital Affairs Taiwan. (2023). Digital affairs and information security initiatives. Ministry of Digital Affairs, Taiwan.
- Njagi, S. M. (2025). Disinformation as a threat to Kenya's national security in the contemporary information environment. *National Security: A Journal of the National Defence University-Kenya*, 3(2), 34-44. <https://doi.org/10.64403/4efzpe03>
- Nurdin, R. (2024). Trolls, disinformasi, dan strategi kampanye: Tantangan demokrasi digital dalam Pemilu 2024. *Electoral Governance: Jurnal Tata Kelola Pemilu Indonesia*, 6(1), 1-26.
- OECD. (2024). Facts not fakes: Tackling disinformation, strengthening information integrity. OECD Publishing. <https://doi.org/10.1787/d909ff7a-en>
- Okeke, O. R., & Omosotomhe, S. I. (2025). Examining the Impact of Misinformation, Disinformation and Propaganda on National Security: A Comparative Study of Select Countries. *TSU Journal of Communication and Media Studies*, 5(1), 174-184.

- Pew Research Center. (2025). False information online as a threat. Pew Research Center.
- Rahayu, L., Sihombing, D. N., & Santoso, P. (2024). Indonesia's non-military threats dynamics: A philosophical perspective. *Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity*, 10(1), 39–53. <https://doi.org/10.33172/jp.v10i1.19459>
- Republik Indonesia. (2024). Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Rød, B., Pursiainen, C., & Eklund, N. (2025). Combatting disinformation – How do we create resilient societies? Literature review and analytical framework. *European Journal for Security Research*, 10, 73–114. <https://doi.org/10.1007/s41125-025-00105-4>
- Sarjito, A. (2024). Hoaks, disinformasi, dan ketahanan nasional: Ancaman teknologi informasi dalam masyarakat digital Indonesia. *Journal of Governance and Local Politics*, 6(2), 175–186. <https://doi.org/10.47650/jglp.v6i2.1547>
- Saputra, A. D., Wulansari, K., & Tomozane, K. (2024). Combatting misinformation in a high-context society: A cluster-randomized controlled trial of digital literacy intervention in Indonesian language education. *Literate: International Journal of Social Science and Humanities*, 3(1). <https://doi.org/10.52005/literate.v3i1.26>
- Susanti, C. (2025). Kebijakan publik dalam kerangka pertahanan nirmiliter guna menghadapi ancaman non-militer. Direktorat Jenderal Potensi Pertahanan, Kementerian Pertahanan Republik Indonesia.
- Tim AIS Kementerian Komunikasi dan Digital. (2026). Data isu hoaks/disinformasi Januari–Agustus 2026. Kementerian Komunikasi dan Digital Republik Indonesia.
- Tobing, N. R., Wendratama, E., & Sumono, N. (2026). Policy paper: Peta jalan penanganan disinformasi di Indonesia. Masyarakat Telematika Indonesia (MASTEL).
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Wulandari, C. D., Muqsith, M. A., Tayibnapis, R. G., & Muzykant, V. L. (2025). Disinformation on TikTok: Analyzing hoaxes surrounding the 2024 Indonesian election. *Ekspresi dan Persepsi: Jurnal Ilmu Komunikasi*, 8(2), 209–222. <https://doi.org/10.33822/jep.v8i2.10163>