International Jurnal Islamic Education, Research and Multiclturalism
(IJIERM)
*Available online https://journal.yaspim.org/index.php/IJIERM/index*

# DIGITAL-ERA LEADERSHIP IN INDONESIA: CHALLENGES AND STRATEGIES FOR NAVIGATING GLOBAL INFORMATION WARFARE

**Dwi Agung[1], Jati Kusumo[2], Djuli Suprijono[3], Aqsa Erlangga[4], Tarsisius Susilo[5]**
[1,2,3,4,5] Indonesian National Armed Forces Command and Staff School (SESKO TNI), Indonesia
[1,2,3,4,5] Email: agunglia02@gmail.com

**Abstract**

Era digital telah memunculkan ancaman perang informasi yang mengganggu stabilitas politik, sosial, dan keamanan nasional. Indonesia menghadapi tantangan serius berupa disinformasi, polarisasi, dan lemahnya regulasi digital, sehingga menuntut kepemimpinan yang adaptif dan visioner. Penelitian ini bertujuan menganalisis tantangan kepemimpinan Indonesia dalam menghadapi perang informasi global serta merumuskan strategi penguatan kepemimpinan digital. Metode penelitian menggunakan pendekatan kualitatif dengan analisis normatif dan studi kepustakaan, dengan kerangka teori kepemimpinan transformasional dan perspektif keamanan non-tradisional. Analisis menunjukkan bahwa kepemimpinan digital di Indonesia masih terbatas akibat rendahnya literasi digital, kapasitas sumber daya manusia yang lemah, dan fragmentasi kebijakan, namun terdapat peluang melalui penguatan regulasi perlindungan data, pembangunan ekosistem literasi digital, dan kolaborasi hexa-helix. Kajian ini menegaskan celah kajian yang masih terbatas dalam mengintegrasikan kepemimpinan digital, kepemimpinan transformasional, dan keamanan non-tradisional dalam konteks resiliensi informasi Indonesia. Penelitian ini menyimpulkan bahwa efektivitas kepemimpinan digital Indonesia terletak pada integrasi visi transformasional, tata kelola inklusif, dan pemanfaatan teknologi modern untuk menjaga kedaulatan informasi serta memperkuat resiliensi nasional.

**Kata Kunci**: kepemimpinan digital, perang informasi, strategi nasional, regulasi, resiliensi

| Corresponding Author | **Dwi Agung** | | |
|---|---|---|---|
| Article History | Submitted: 3 October 2025 | Accepted: 5 February 2026 | Published: 2 March 2026 |

**Abstract**

The digital era has introduced the threat of information warfare that disrupts political, social, and national security stability. Indonesia faces major challenges such as disinformation, polarization, and weak digital regulations, demanding adaptive and visionary leadership. This study analyzes Indonesia's leadership challenges in dealing with global information warfare and formulates strategies for strengthening digital leadership. It employs a qualitative, literature-based normative analysis framed by transformational leadership theory and the perspective of non-traditional security. The analysis indicates that Indonesia's digital leadership remains constrained by low digital literacy, weak human resource capacity, and fragmented policies, yet opportunities exist through strengthening data protection and platform accountability, developing a digital literacy ecosystem, and fostering hexa-helix collaboration. Addressing a gap in integrative scholarship, this article links digital leadership, transformational leadership, and non-traditional security to propose a coherent strategy for national information resilience. The study concludes that effective digital leadership lies in integrating a transformational vision, inclusive governance, and modern technology to safeguard information sovereignty and reinforce national resilience.

**Keywords:** digital leadership, information warfare, national strategy, regulation, resilience

## INTRODUCTION

Leadership in the digital era represents a new paradigm that requires a combination of transformative vision and the effective use of digital technology in decision-making and public governance (Sawy et al., 2020). This shift not only highlights the importance of leaders in guiding organizations but also necessitates an awareness of the dynamics within the global information ecosystem, which is characterized by rapid data flows, cross-border connectivity, and an increase in non-traditional risks. One of the most significant challenges in this context is the issue of information warfare, which includes the dissemination of disinformation, manipulation of public opinion, and coordinated digital propaganda through the use of algorithms and automation (Bradshaw & Howard, 2019). In Indonesia, a

country with a very large social media audience and high internet adoption, the impact of information warfare is particularly acute (APJII, 2025). Political polarization, a decline in public trust in institutions, and threats to democracy are clear signs of the disinformation crisis affecting Indonesia's digital landscape.

The literature on digital leadership emphasizes that organizational transformation is influenced more by leadership strategies than by technological aspects alone (Kraus et al., 2022). This leadership model requires visionary competencies, digital literacy, and the capacity to adapt in order to effectively manage change within the constantly evolving information ecosystem (Sousa & Rocha, 2019a, p. 362). Global studies indicate that failing to manage information flow can exacerbate crises; this was notably evident during the COVID-19 infodemic, which underscored the crucial role of digital leaders in maintaining the legitimacy of public policy (Herrera-Viedma et al., 2020). Contemporary political research shows a strong link between disinformation on social media and increased political polarization, as well as a decline in public trust in democratic institutions (von Solms & van Niekerk, 2013). This body of literature positions digital leadership as a key instrument for understanding the dynamics of information warfare and for developing strategies aimed at national resilience and the protection of democracy in Indonesia.

The main objective of this study is to identify the challenges facing Indonesia's leadership in the context of the global information war and to formulate a digital leadership strategy that meets national needs. The analysis focuses on three key objectives. First, it aims to map the various threats emerging in Indonesia's digital space, including the spread of political disinformation, weak regulatory governance, and low levels of digital literacy. Second, the study examines the relevance of transformational leadership theory and non-traditional security perspectives as a conceptual framework to assess leaders' capacity to respond to global information dynamics. Third, it seeks to formulate a digital leadership strategy that prioritizes the integration of data protection regulations, the development of a digital literacy ecosystem, and the strengthening of collaboration among the government, society, and the private sector (often referred to as hexa-helix collaboration). This formulation provides a conceptual foundation to enhance national resilience while ensuring the sustainability of democracy in the era of digital connectivity.

The conceptual argument starts with the premise that digital leadership serves as a strategic tool for addressing the increasingly complex

threat of information warfare. Leadership that is oriented towards transformation can effectively guide change by focusing on a long-term vision, inspiring collective action, and empowering key strategic actors at the national level. Adopting a non-traditional security perspective offers an analytical framework that views information threats not merely as technical challenges but also as issues that affect political legitimacy, social cohesion, and state sovereignty. Without an adaptive model of digital leadership, there is a risk of increased polarization and a decline in public trust in institutions. On the other hand, integrating a transformational vision with inclusive information governance and accountability-driven regulation can enhance national resilience. This conceptual hypothesis posits that the effectiveness of digital leadership hinges on its ability to foster cross-sector collaboration and leverage technology to uphold democratic stability and information sovereignty in Indonesia.

## LITERATURE REVIEW

Digital leadership has emerged as a response to technological disruption, necessitating new patterns of leadership in organizational and governmental contexts. Leaders can no longer rely solely on hierarchical authority; instead, they must possess the ability to integrate a transformational vision, technological literacy, and adaptive agility in the face of uncertainty (Soto-Acosta, 2020). Recent studies indicate that digital leadership plays a crucial role in driving innovation, enhancing public legitimacy, and increasing trust through data-driven governance (Zhang et al., 2025). Additionally, leaders must develop cross-sectoral collaborative capacity to build an inclusive digital ecosystem (Kraus et al., 2022). The international literature highlights that digital leadership is not just about adopting technology; it also involves transforming organizational culture and fostering a sustainable strategic orientation. These changes underscore the importance of digital leadership as a foundation for strengthening national competitiveness and resilience amid global dynamics.

Digital leadership is defined by the ability to combine a strategic vision with the effective use of digital technology to establish adaptive governance. Key competencies required for successful digital leadership include digital literacy, agile decision-making, and the ability to foster cross-sector collaboration in a dynamic environment (Zeike et al., 2019). Recent research highlights that innovative digital leaders can enhance organizational capabilities and improve competitiveness by exploring new technologies (Lee & Trimi, 2021). A crucial aspect of this leadership is the ability to cultivate a work culture that emphasizes continuous learning and digital experimentation, which is essential for organizations to thrive amid

disruption. International literature underscores that the success of digital transformation relies more on leadership competencies than on technology adoption alone. Leaders with strong digital capabilities play a pivotal role in maintaining organizational stability while expanding opportunities for innovation.

Information warfare is defined as a systematic effort to manipulate the information ecosystem by spreading disinformation, misinformation, and coordinated propaganda. The goal is to influence public opinion and undermine the legitimacy of institutions (Wardle & Derakhshan, 2017). The tactics employed include social media algorithms, automated accounts, and structured communication networks, which enable political messages to spread widely beyond national borders. Recent studies indicate that global disinformation campaigns have significantly contributed to social polarization, decreased public trust, and increased political instability (Bennett & Livingston, 2018). This issue is particularly evident in elections in the United States and the European Union, where digital manipulation has been shown to impact political behavior and public perception (Gerhardt, 2018). The international literature characterizes information warfare as a multidimensional threat that affects democracy, national security, and international relations in our digitally connected era.

Disinformation in contemporary literature is regarded as one of the most significant threats to the quality of modern democracy. Comparative research indicates that the flow of disinformation on social media directly influences voter behavior and diminishes public trust in democratic institutions (Farkas & Schou, 2023). Recent analyses have shown that exposure to manipulative content intensifies political polarization, weakens social cohesion, and increases the fragmentation of public spaces (Humprecht et al., 2020). Other studies confirm that the impact of disinformation extends beyond elections to influence public policy discussions, leading to biases in public opinion (Spohr, 2017). Additionally, big data-driven research demonstrates that digital platform algorithms accelerate the spread of misleading content, creating echo chambers that suppress the diversity of political perspectives (Cinelli et al., 2021). These findings illustrate that democracy faces structural challenges due to digital disinformation, particularly regarding political legitimacy and the quality of citizen participation.

The issue of disinformation, which poses a threat to the quality of global democracy, is also evident in Indonesia. The high penetration of social media makes Indonesia one of the largest digital markets in the world, creating an environment that is vulnerable to the spread of

manipulative content. Recent research shows that political hoaxes during election periods have intensified identity polarization and diminished public trust in democratic institutions (Tomsa, 2020). Analytics-based survey experiments indicate that exposure to false information impacts voter perceptions and undermines the legitimacy of election results (Lim, 2025). Another study highlights that disinformation in Indonesia is often produced systematically through political buzzer networks, mirroring the phenomenon of computational propaganda observed in other countries. These empirical findings position Indonesia as a significant case study in the global discourse on information warfare, emphasizing the urgent need for strong digital leadership to uphold social cohesion and the resilience of democracy.

The study of disinformation in Indonesia highlights the urgent need for a theoretical framework that can explain how leadership dynamics operate in the context of information warfare. Research on transformational leadership indicates that visionary, inspirational, and change-oriented leaders are better equipped to guide organizations through periods of digital disruption (Buil et al., 2019). Additionally, studies suggest that combining digital leadership with transformational principles can enhance organizational innovation and strengthen public legitimacy (Sousa & Rocha, 2019b). From a non-traditional security perspective, disinformation is viewed as a threat that extends beyond technical issues, impacting social, political, and sovereign aspects of the state (Andrade et al., 2020). Recent literature has started to connect this issue to the necessity for resilient information governance; however, discussions that specifically link digital leadership, transformational theory, and non-traditional security remain scarce. Addressing this gap contributes to the development of a more contextual academic analysis of information warfare in Indonesia.

## RESEARCH METHODS

This research employs a qualitative approach to analyze the dynamics of digital leadership within the context of global information warfare. The focus is on Indonesia, a country characterized by high social media penetration and significant vulnerability to disinformation. The digital space serves as the primary unit of study, as it represents an arena where political actors, regulators, media organizations, and civil society interact. The involvement of these diverse actors leads to complex communication configurations, which impact social cohesion and democratic stability. The study emphasizes the role of digital leadership in effectively managing a dynamic and uncertain information ecosystem. This choice of analysis aligns with qualitative research traditions, which

prioritize understanding social processes by exploring empirical contexts (Hennink et al., 2020).

The methodological framework is bolstered by the literature on political communication, highlighting the necessity of in-depth studies of information practices in the digital age (Dijck et al., 2018). The research design combines a qualitative approach with a normative framework to evaluate digital leadership in information warfare. The normative perspective outlines the legal rules and policies governing information governance. According to Marzuki, normative legal research emphasizes the analysis of legal documents and literature as essential sources for building arguments (Marzuki, 2017). This view is supported by Soekanto and Mamudji, who suggest that normative legal research involves studying primary, secondary, and tertiary legal materials (Soekanto & Mamudji, 2015). A qualitative approach was further utilized to examine secondary data, such as academic reports, international publications, and case studies relevant to the Indonesian context. Banakar and Travers describe the socio-legal tradition as a bridge connecting legal analysis with social and political practices (Banakar & Travers, 2005). This combination of methodologies provides a framework for understanding the capacity of digital leadership, considering both regulatory dimensions and the empirical realities within Indonesia's information ecosystem.

## RESULTS AND DISCUSSION

### 1. Global and Regional Dynamics of Information Warfare

Information warfare has become a global issue that influences political direction and governance in democracies around the world. The 2016 and 2020 United States elections serve as prime examples of how cyber operations and algorithmic manipulation can deepen societal polarization. This phenomenon is often driven by transnational actors who exploit digital platforms (Benkler et al., 2018). In Europe, the spread of misleading narratives regarding migration and regional integration has been shown to strengthen populist movements and create policy instability at the regional level (Humprecht et al., 2020). This aligns with comparative research findings that indicate disinformation has shaped a cross-border political landscape and eroded trust in democratic institutions (Grabe & Bucy, 2022). The Covid-19 pandemic further intensified this issue through an "infodemic," where an overwhelming amount of misinformation disrupted public health coordination and undermined the legitimacy of global policy responses (Pulido et al., 2020). These developments suggest that information warfare is increasingly central to discussions in non-traditional security studies.

Southeast Asia exhibits a distinct pattern of digital disinformation closely linked to domestic political dynamics. In the Philippines, troll farms and the involvement of political consultants create an organized communication ecosystem that produces and distributes manipulative content for electoral advantage (Ong & Cabañes, 2018). In Myanmar, social media is used as a channel for spreading ethnic propaganda, which the military leverages to bolster its political legitimacy (Schissler, 2025). Thailand demonstrates disinformation practices related to monarchy issues, illustrating how the digital space is utilized in political contests between pro-democracy groups and the government (Sinpeng, 2019). This comparative study positions the phenomenon as part of a regional trend, where political actors and the state systematically use digital spaces to manage public perception (Wu-Ouyang & Hu, 2025).

Table 1. Comparison of Global and Regional Information War Phenomena

| Country/ Region | Main Cases | Dominant Actor | Main Impact |
|---|---|---|---|
| **United States** | The 2016 & 2020 elections, Russia's digital intervention | State actors, digital platforms | Political polarization, declining public trust |
| **European Union** | Misinformation on migration and Brexit issues | Populist political groups, online bots | Strengthening populism, policy instability |
| **Philippines** | Buzzer politik & troll farms | Konsultan politik, buzzer | Manipulation of public opinion, normalization of digital politics |
| **Myanmar** | Propaganda anti-Rohingya via Facebook | Military, ethnic groups | Military legitimacy, ethnic conflict |
| **Thailand** | Disinformation related to the monarchy | Government, pro-monarchy groups | Opposition repression, erosion of democracy |

Source: Data processed by the author, 2025

The pattern of disinformation in Southeast Asia is highly relevant to Indonesia, given the similarities in digital space usage across the region. Indonesia has one of the highest internet and social media penetration rates in the world, with over 200 million active users. As a result, digital

platforms have become a primary source of daily information. This heavy reliance on social media creates significant opportunities for the spread of hoaxes and digital propaganda, particularly during electoral periods. Previous research has shown that disinformation in Indonesia often intertwines political issues with religious sentiments, which exacerbates the potential for societal polarization. Similar findings indicate that the digital space serves not only as a means of communication but also as a complex battleground for political contestation (Nugroho et al., 2025). This situation underscores the urgent need for analyzing digital leadership in Indonesia to effectively address the challenges of information warfare.

## 2. Disinformation Ecosystem in Indonesia: Social Media, Polarization, and Regulatory Challenges

Social media has emerged as the primary platform for information exchange in Indonesia, taking over many functions traditionally held by conventional media in shaping public opinion. According to a report from the Indonesian Internet Service Providers Association (APJII, 2025), there are over 200 million active internet users in the country, with WhatsApp, Facebook, Instagram, and TikTok leading in popularity. The widespread use of these digital platforms positions social media as a crucial channel for sharing political, economic, and social information. Recent studies indicate that Indonesia's digital landscape is evolving into a space for citizen engagement in public discourse. However, this development is not matched by a sufficient level of digital literacy among users (Andajani et al., 2024). Consequently, there is a heightened risk of the spread of hoaxes and misinformation, particularly concerning sensitive issues related to political and religious identities. Therefore, social media in Indonesia serves not only as a means of communication but also as a battleground that influences the trajectory of political and social dynamics.

Political hoaxes are a significant phenomenon in Indonesia's digital landscape, particularly during election periods. The 2019 election highlighted the intensity of misinformation related to religious issues and identity politics, a pattern that is re-emerging as we approach the 2024 election. Key players, such as political buzzers, influencers, and communications consultants, are instrumental in creating and disseminating digital narratives aimed at shaping public opinion. Previous studies have shown that political polarization on social media is exacerbated by the use of religious issues as a tool for mass mobilization (Soderborg & Muhtadi, 2023). Additionally, algorithmic bias on digital platforms contributes to the formation of echo chambers, restricting people's exposure to diverse viewpoints and deepening social

fragmentation (Biddlestone et al., 2022). This situation has led to a decline in public trust in both the media and political institutions, underscoring the need for an adaptive digital leadership strategy to address the challenges of polarization.

Table 2. Typology of Disinformation in Indonesia Based on Dominant Issues and Actors

| Main Issue Categories | Content Characteristics | Dominant Actor | Socio-Political Impact |
|---|---|---|---|
| **Electoral Politics** | Hoaxes related to candidates, election results | Buzzer, political consultant | Polarisasi politik, trust deficit |
| **Religion & Identity** | Sectarian narratives, group delegitimization | Identity groups, buzzers | Social fragmentation, political exclusion |
| **Health & Crisis** | Infodemic (Covid-19, vaksinase) | Influencers, alternative media | Crisis of trust in public authority |
| **Economy Digital** | Investment fraud, market manipulation | Private actors, online brokers | Financial losses, declining public literacy |

Source: Data processed by the author, 2025

The typology of disinformation presented in the table highlights the intricate relationship between political, religious, health, and economic issues in shaping the digital ecosystem in Indonesia. Various dominant actors, including political buzzers, religious groups, and social media influencers, play a strategic role in creating and disseminating narratives that serve specific interests. The socio-political impact of this phenomenon is marked by a decline in public trust in formal institutions, an increase in social fragmentation, and the rampant practice of exclusion within digital public spaces. This situation illustrates that the information war in Indonesia extends beyond mere communication—it has become a strategic tool for political and economic competition.

Furthermore, the rise of disinformation reveals that the digital space has transformed into a complex arena of political and social contestation. The typology of hoaxes surrounding political, religious, health, and economic issues demonstrates how various actors systematically produce manipulative narratives to shape public perception. These dynamics present significant challenges to the sustainability of democracy as they deepen polarization, erode social cohesion, and undermine the legitimacy

of formal institutions. The fragmentation of digital public spaces complicates efforts to achieve a healthy social consensus, particularly during critical moments such as elections. This complexity highlights that the issue of disinformation is not solely a matter of digital literacy; it is also closely tied to regulatory governance and leadership capacity in guiding the information ecosystem. This scenario paves the way for further analysis of how national regulatory strategies and digital leadership approaches can be effectively designed to respond to the challenges posed by information warfare.

### 3. Digital Regulatory and Leadership Strategy for National Information Resilience

Indonesia's national regulations governing the digital space are anchored in the Information and Electronic Transactions Law (UU ITE) and implementing regulations issued by the Ministry of Communication and Informatics. This legal framework provides a basis for enforcement against hoaxes, hate speech, and other abuses of information technology, while also enabling the state to develop institutional capacities for cyber governance. However, the effectiveness of the ITE Law remains contested due to the multi-interpretability of several provisions, which can produce legal uncertainty. In addition, platform accountability is not comprehensively regulated, leaving a gap between national rules and evolving global governance practices. Scholarly reviews therefore highlight the need to refine legal instruments so they are more precise, transparent, and aligned with human rights principles (Lindsey & Butt, 2018). A more targeted approach to regulatory reform can provide a stronger foundation for digital leadership strategies in responding to information warfare

The national regulations governing the digital space in Indonesia are based on the Information and Electronic Transactions Law and implementing regulations issued by the Ministry of Communication and Informatics. This legal framework establishes a foundation for law enforcement against hoaxes, hate speech, and other forms of information technology abuse, while also strengthening the government's authority to establish cyber surveillance agencies. However, the effectiveness of the ITE Law faces challenges due to some articles being open to multiple interpretations, which can lead to legal uncertainty. Additionally, the accountability of digital platforms is not comprehensively regulated, creating a gap between national regulations and global governance practices. The latest review highlights the need to update legal instruments through mechanisms that are more precise, transparent, and aligned with human rights principles. A more focused reformulation of regulations

could serve as a basis for digital leadership strategies in addressing the dynamics of information warfare.

Digital leadership capacity is a crucial factor in determining the effectiveness of regulations governing cyberspace. Leadership encompasses not only the technocratic skills required to oversee information flow but also the ability to foster public trust through inclusive and transparent governance. The adaptive leadership model highlights the importance of flexibility in response to rapid changes driven by the advancement of digital technologies, including the dynamic nature of disinformation (Heifetz, 2009). Research on digital governance shows that successful management strategies for digital spaces typically involve coordination among multiple stakeholders, including countries, platform providers, civil society, and the private sector (Przeybilovicz & Cunha, 2024). In the Indonesian context, effective digital leadership should focus on enhancing digital literacy among the population, increasing the accountability of platforms, and promoting collaboration across sectors. This approach lays the groundwork for developing a more integrated and sustainable regulatory strategy to address the challenges posed by information warfare.

A strategic response to information warfare requires an integrated approach that combines legal regulation, digital leadership, and community capacity building. Normative regulations provide a foundation for legal certainty and establish an accountability framework for digital platforms. Adaptive digital leadership is essential for fostering coordination among multiple stakeholders, including governments, the private sector, and civil society, to promote more transparent and collaborative information governance. Additionally, enhancing public digital literacy is a crucial tool for strengthening individuals' resistance to hoaxes and disinformation. This integrative model aligns with the concept of algorithmic governance, which emphasizes the need for a balance between regulatory intervention and community participation (Kalpokas, 2019). It also reflects the ideas of digital diplomacy, which views cyberspace as a strategic arena for building political legitimacy and public trust (Tomsa, 2020). This approach allows for the development of a more responsive and sustainable national information security framework.

The hexa-helix approach presents an effective collaborative framework for developing strategies to address information warfare in Indonesia. This model highlights the synergy among six key stakeholders: the government, academia, businesses, civil society, the media, and the international community. The government is responsible for establishing clear and accountable regulations, while academia contributes through

evidence-based research to inform policy formulation. Businesses, particularly digital platform providers, have a duty to ensure algorithmic transparency and implement accountability mechanisms. Civil society acts as both a supervisor and a promoter of digital literacy, and the media plays a crucial role in safeguarding the integrity of public information. Lastly, the international community enhances this framework by facilitating the exchange of best practices and fostering transnational cooperation. By integrating these six actors, we can create a more adaptive and layered approach to information governance, ultimately strengthening the capacity of national digital leadership to effectively respond to the challenges of information warfare in a sustainable manner.

Table 3. The Role of Actors in the Hexa-Helix Model for Information Governance in Indonesia

| Actor | Main Role | Strategic Objectives |
|---|---|---|
| **Government** | Formulate precision regulations, ensure law enforcement, establish cyber surveillance agencies | Ensure legal certainty, platform accountability, and information sovereignty protection |
| **Academy** | Producing evidence-based research, providing policy input, developing digital literacy | Provide a scientific basis for regulation and strengthen the literacy capacity of the community |
| **Business World** | Provide algorithmic transparency, build digital platform accountability mechanisms | Maintaining the integrity of the digital ecosystem and increasing public trust |
| **Civil Society** | Become an independent supervisor, initiate digital literacy programs, and advocate for inclusive policies | Strengthening public participation and protecting citizens' rights in the digital space |
| **Media** | Providing accurate information, countering disinformation, | Improving the quality of public information and |

| | | |
|---|---|---|
| | maintaining the integrity of digital journalism | strengthening deliberative democracy |
| **International Community** | Forming transnational cooperation, sharing best practices, supporting regulatory capacity | Strengthening global collaboration to confront cross-border threats in information warfare |

Source: Data processed by the author, 2025

The collaborative approach outlined in the table highlights the importance of clearly defining and complementing the roles of governments, academia, businesses, civil society, the media, and the international community. This synergy among these actors is essential for establishing adaptive, inclusive, and multi-layered information governance, especially in the context of escalating information warfare. The effectiveness of this strategy relies not only on robust regulations but also on the quality of public participation and the accountability of digital platforms operating in Indonesia. By integrating these six pillars, national digital leadership can gain greater legitimacy to coordinate among multiple stakeholders and enhance information resilience as part of the overall national resilience in the digital era.

Synthesis of these findings suggests that information warfare in Indonesia should be approached as a governance challenge with security implications, rather than as a purely technical or communication issue. Three conceptually grounded implications follow: (1) regulatory reform must move beyond content takedown toward clearer due process and platform accountability; (2) national resilience requires sustained investment in digital literacy and civic media competence to reduce vulnerability to polarization; and (3) effective digital leadership depends on an institutionalized hexa-helix coordination mechanism that aligns incentives and responsibilities across sectors.

## CONCLUSION

Digital leadership in Indonesia is strategically positioned to strengthen national information resilience amid an escalating global information war. Challenges associated with the scale of social media use, uneven digital literacy, and inconsistencies in regulatory governance underscore the need for leaders who can articulate a transformational vision and navigate disinformation dynamics adaptively. Leadership that is responsive to the digital landscape is crucial for maintaining social cohesion and limiting polarization that can undermine democratic stability.

The analysis yields three interrelated insights. First, global and regional developments show that digital manipulation has become a central instrument in political and security contests, including across Southeast Asia. Second, Indonesia's disinformation ecosystem displays a multifaceted typology across political, religious, health, and economic issues, involving actors ranging from influencers to organized identity groups. Third, strengthening digital leadership requires an integrated strategy that combines refined legal instruments, sustained literacy-building, and cross-sector collaboration through a hexa-helix governance approach.

The study contributes by connecting transformational leadership theory, non-traditional security perspectives, and hexa-helix collaboration as a coherent framework for information resilience. Because the analysis is primarily normative and literature-based, its conclusions should be read as conceptually grounded rather than as causal estimates. Future research may incorporate surveys, platform data, or mixed methods to test disinformation patterns and evaluate the effectiveness of specific leadership and governance interventions.

Practical priorities for Indonesia include: (1) strengthening data protection and platform accountability through clearer due process, transparent enforcement standards, and co-regulation mechanisms; (2) scaling a national digital literacy ecosystem that targets civic media competence, community-based fact-checking, and resilience against identity-based polarization; and (3) institutionalizing hexa-helix coordination (government–academia–business–civil society–media–international partners) with defined roles, information-sharing protocols, and measurable performance indicators.

## BIBLIOGRAPHY

1) Andajani, K., Karmina, S., & Rahmania, L. A. (2024). Inclusive, Sustainable, and Transformational Education in Arts and Literature: Proceedings of the 7th International Seminar on Language, Education, and Culture, (ISoLEC, 2023), July 07—08, 2023, Malang, Indonesia. Taylor & Francis.
2) Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. (2020). A Comprehensive Study of the IoT Cybersecurity in Smart Cities. IEEE Access, 8, 228922–228941. https://doi.org/10.1109/ACCESS.2020.3046442
3) APJII. (2025). Indonesian Internet Service Providers Association—Survey. https://survei.apjii.or.id/

4) Banakar, R., & Travers, M. (2005). Theory and Method in Socio-Legal Research. Bloomsbury Publishing.
5) Benkler, Y., Faris, R., & Roberts, H. (2018). Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford University Press.
6) Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication. https://doi.org/10.1177/0267323118760317
7) Biddlestone, M., Azevedo, F., & Linden, S. van der. (2022). Climate of conspiracy: A meta-analysis of the consequences of belief in conspiracy theories about climate change. Current Opinion in Psychology, 46, 101390. https://doi.org/10.1016/j.copsyc.2022.101390
8) Bradshaw, S., & Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation [Report]. Oxford Internet Institute, University of Oxford. https://comprop.oii.ox.ac.uk/research/cyber-troops-2019/
9) Buil, I., Martínez, E., & Matute, J. (2019). Transformational leadership and employee performance: The role of identification, engagement and proactive personality. International Journal of Hospitality Management, 77, 64–75. https://doi.org/10.1016/j.ijhm.2018.06.014
10) Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. Proceedings of the National Academy of Sciences, 118(9), e2023301118. https://doi.org/10.1073/pnas.2023301118
11) Dijck, J. van, Poell, T., & Waal, M. de. (2018). The Platform Society: Public Values in a Connective World. Oxford University Press.
12) Farkas, J., & Schou, J. (2023). Post-Truth, Fake News and Democracy: Mapping the Politics of Falsehood (2nd ed.). Routledge. https://doi.org/10.4324/9781003434870
13) Gerhardt, M. (2018). Congress's Constitution: Legislative Authority and the Separation of Powers. https://dx.doi.org/10.1002/polq.12781
14) Grabe, M. E., & Bucy, E. P. (2022). Moral panics about the integrity of information in democratic systems:Comparing tabloid news to

disinformation. Journal of Broadcasting & Electronic Media. https://www.tandfonline.com/doi/abs/10.1080/08838151.2022.2120482

15) Heifetz, R. A. (2009). Leadership Without Easy Answers. Harvard University Press. https://doi.org/10.4159/9780674038479
16) Hennink, M., Hutter, I., & Bailey, A. (2020). Qualitative Research Methods. SAGE.
17) Herrera-Viedma, E., López-Robles, J.-R., Guallar, J., & Cobo, M.-J. (2020). Global trends in coronavirus research at the time of Covid-19: A general bibliometric approach and content analysis using SciMAT. Profesional de La Información, 29(3). https://doi.org/10.3145/epi.2020.may.22
18) Humprecht, E., Esser, F., & Aelst, P. V. (2020). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. The International Journal of Press/Politics. https://doi.org/10.1177/1940161219900126
19) Kalpokas, I. (2019). Algorithmic Governance: Politics and Law in the Post-Human Era. Springer International Publishing. https://doi.org/10.1007/978-3-030-31922-9
20) Kraus, S., Durst, S., Ferreira, J. J., Veiga, P., Kailer, N., & Weinmann, A. (2022). Digital transformation in business and management research: An overview of the current status quo. International Journal of Information Management, 63. https://doi.org/10.1016/j.ijinfomgt.2021.102466
21) Lee, S. M., & Trimi, S. (2021). Convergence innovation in the digital age and in the COVID-19 pandemic crisis. Journal of Business Research, 123, 14–22. https://doi.org/10.1016/j.jbusres.2020.09.041
22) Lim, M. (2025). Social Media and Politics in Southeast Asia. Cambridge University Press; Cambridge Core. https://doi.org/10.1017/9781108750745
23) Lindsey, T., & Butt, S. (2018). Indonesian Law. Oxford University Press.
24) Marzuki, M. (2017). Legal Research: Revised Edition. Medium Pregnancy.

25) Nugroho, H. Y. S. H., Wahyuningrum, N., Basuki, T. M., Supangat, A. B., Auliyani, D., Indrajaya, Y., Lisnawati, Y., & Samawandana, G. (2025). Sustainable Resilience for Integrated Watersheds Management Under Climate Change: Lesson Learned from Indonesia. In S. C. Pal, U. Chatterjee, A. Saha, & D. Ruidas (Eds.), Climate Change: Conflict and Resilience in the Age of Anthropocene (pp. 303–327). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-85359-3_13
26) Ong, J. C., & Cabañes, J. V. (2018). Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines [Report]. Newton Tech4Dev Network. https://newtontechfordev.com/newton-tech4dev-research-identifies-ad-pr-executives-chief-architects-fake-news-production-social-media-trolling/
27) Przeybilovicz, E., & Cunha, M. A. (2024). Governing in the digital age: The emergence of dynamic smart urban governance modes. Government Information Quarterly, 41(1). https://doi.org/10.1016/j.giq.2023.101907
28) Pulido, C. M., Villarejo-Carballido, B., Redondo-Sama, G., & Gómez, A. (2020). COVID-19 infodemic: More retweets for science-based information on coronavirus than for false information. International Sociology. https://doi.org/10.1177/0268580920914755
29) Sawy, O. A. E., Kræmmergaard, P., Amsinck, H., & Vinther, A. L. (2020). How LEGO Built the Foundations and Enterprise Capabilities for Digital Leadership. In Strategic Information Management (5th ed.). Routledge.
30) Schissler, M. (2025). Beyond Hate Speech and Misinformation: Facebook and the Rohingya Genocide in Myanmar. Journal of Genocide Research. https://www.tandfonline.com/doi/abs/10.1080/14623528.2024.2375122
31) Sinpeng, A. (2019). Digital media, political authoritarianism, and Internet controls in Southeast Asia. Media, Culture & Society. https://doi.org/10.1177/0163443719884052

32) Soderborg, S., & Muhtadi, B. (2023). Resentment and Polarization in Indonesia. Journal of East Asian Studies, 23(3), 439–467. https://doi.org/10.1017/jea.2023.17
33) Soekanto, S., & Mamudji, S. (2015). Normative Law Research: A Brief Review (Edition 1 of the 12th Edition (2010, reprinted 2015)). PT RajaGrafindo Persada.
34) Soto-Acosta, P. (2020). COVID-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear. Information Systems Management. https://www.tandfonline.com/doi/abs/10.1080/10580530.2020.1814461
35) Sousa, M. J., & Rocha, Á. (2019a). Leadership styles and skills developed through game-based learning. Journal of Business Research, 94, 360–366. https://doi.org/10.1016/j.jbusres.2018.01.057
36) Sousa, M. J., & Rocha, Á. (2019b). Leadership styles and skills developed through game-based learning. Journal of Business Research, 94, 360–366. https://doi.org/10.1016/j.jbusres.2018.01.057
37) Spohr, D. (2017). Fake news and ideological polarization. Business Information Review. https://doi.org/10.1177/0266382117722446
38) Tomsa, D. (2020). Public Opinion Polling and Post-truth Politics in Indonesia. Contemporary Southeast Asia, 42(1), 1–27. https://doi.org/10.1093/ia/iiz010
39) von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
40) Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policymaking (Report No. DGI(2017)09). Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
41) Wu-Ouyang, B., & Hu, Y. (2025). Internet Freedom and Social Media's Political Consequences: Political Nationalism and Authoritarian Orientation Among Six Asian Societies. Journalism & Mass Communication Quarterly. https://doi.org/10.1177/10776990241313183

42) Zeike, S., Bradbury, K., Lindert, L., & Pfaff, H. (2019). Digital Leadership Skills and Associations with Psychological Well-Being. International Journal of Environmental Research and Public Health, 16(14). https://doi.org/10.3390/ijerph16142628
43) Zhang, X., Wang, Z., Luo, W., Guo, F., & Wang, P. (2025). How Digital Orientation Affects Innovation Performance? Exploring the Role of Digital Capabilities and Environmental Dynamism. Systems, 13(5). https://doi.org/10.3390/systems13050346