

## Counter-Narrative Strategies in Preventing Radicalization in Indonesia's Digital Space

Luis Moya<sup>1\*</sup>, Rudy Sutanto<sup>2</sup>, Suhirwan<sup>3</sup>  
Republic of Indonesia Defense University

**Corresponding Author:** Luis Moya [luis moyasibuea@gmail.com](mailto:luis moyasibuea@gmail.com)

---

### ARTICLE INFO

*Keywords:* Digital  
Radicalization, Counter-  
Narratives, Warfare  
Asymmetric, Non- Military  
Defense

*Received :* 29, December

*Revised :* 30, January

*Accepted:* 23, February

©2026 Moya, Sutanto, Suhirwan: This is an open-access article distributed under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/).



### ABSTRACT

Digital radicalization represents a transformation of security threats within the context of asymmetric warfare, where non-state actors utilize social media as a tool for ideological propaganda and information warfare. This phenomenon positions extremist narratives as strategic instruments to undermine ideological resilience, social cohesion, and state legitimacy. This essay aims to analyze the role of counter-narratives and alternative narratives as communication strategies in preventing digital radicalization in Indonesia. The study employs a qualitative descriptive method through literature review and policy analysis, drawing on academic sources, official government documents, and national legal frameworks related to defense and counterterrorism. The analysis reveals that counter-narratives function as non-military defense instruments operating within the cognitive and affective domains of society, while alternative narratives contribute to long-term ideological resilience. The effectiveness of these strategies is highly influenced by dissemination mechanisms within the social media ecosystem, including algorithmic dynamics, message messengers, and content formats. This essay concludes that integrating counter-narratives into Indonesia's non-military defense strategy is a strategic necessity in addressing digital radicalization and asymmetric warfare threats.

---

## **INTRODUCTION**

Counter-narratives are understood as systematic efforts to challenge, dismantle, and undermine the legitimacy of radical narratives disseminated by non-state actors through digital spaces. This article addresses the theme "Counter-Narrative Strategies in Preventing Radicalization in Indonesia's Digital Space," focusing on the use of narrative-based strategic communication to counter the spread of extremist ideologies and terrorism on social media. In the Indonesian context, this strategy has become increasingly relevant with the increasing use of social media as a medium for propaganda, recruitment, and the normalization of violence by extremist groups. Digital radicalization no longer occurs through direct indoctrination, but rather through a gradual process that leverages issues of identity, injustice, religion, and politics, packaged in persuasive and emotional content. Therefore, a security approach that relies solely on legal enforcement is insufficient; non-military instruments capable of reaching the cognitive and psychological dimensions of individuals are needed, one of which is through counter-narrative strategies.

The phenomena of digital radicalization and terrorism are closely linked to asymmetric warfare, where non-state actors use unconventional means to challenge state superiority. In this context, extreme narratives function as weapons of influence that attack state legitimacy, erode social cohesion, and weaken national resilience without resorting to military action. Social media has become a new battlefield in asymmetric warfare, where public information, perceptions, and emotions are the primary targets. Counter-narratives can be positioned as part of non-military defense strategies and defensive information operations, aimed at closing off the enemy's ideological sphere of influence. Thus, preventing digital radicalization is not only an internal security issue but also part of a national defense strategy in the face of increasingly complex hybrid and asymmetric threats.

Indonesia has a long history of dealing with the threat of terrorism, both in the form of physical violence and the spread of extremist ideologies. In recent years, this threat has undergone a transformation, with the digital space becoming the primary means of spreading radical ideology. The high penetration of the internet and social media in Indonesia makes society, especially the younger generation, vulnerable to exposure to extremist narratives. This issue is crucial because digital radicalization not only threatens national security but also has the potential to undermine national values, tolerance, and unity in a pluralistic society. Therefore, developing effective counter-narrative strategies is an urgent need for Indonesia to maintain national stability and strengthen the nation's ideological resilience.

## **LITERATURE REVIEW**

The writing of this article is based on several main theoretical approaches, including:

1. Radicalization Theory explains the gradual process by which individuals adopt extreme ideologies, primarily through exposure to narratives on social media.

2. Strategic Communication Theory, which views narrative as an instrument of power and influence in the context of conflict and security.
3. The theory of Counter-Narratives and Alternative Narratives, which emphasizes the importance of counter-narratives and positive narratives in reducing the appeal of extremism, as discussed in the study of counter-narratives of extremism and self-control in social media.
4. The Theory of Asymmetric Warfare and Information Warfare, which places information and ideology as strategic domains of conflict.

### ***Benefit Writing***

This article is expected to be beneficial for various parties. For academic and defense institutions, particularly the Defense University (UNHAN RI), this article contributes to the development of non-military defense studies, information warfare, and national security based on a multidisciplinary approach. For the general public, this article provides a critical understanding of the dangers of digital radicalization and the importance of media literacy and ideological resilience. For the nation and state, this study can serve as a conceptual reference in formulating more adaptive, humanistic, and sustainable terrorism prevention policies, in line with efforts to strengthen national resilience.

### **METHODOLOGY**

This article uses a qualitative-descriptive research method with a literature review and policy analysis approach. Primary data was obtained from official government documents, regulations, and institutional statements related to terrorism prevention and cybersecurity. Secondary data is sourced from scientific journals, books, and academic articles discussing digital radicalization, counter-narratives, and asymmetric warfare, including the references you have provided.

### **RESEARCH RESULTS AND DISCUSSION**

#### ***Radicalization in Digital Space as Manifestation War Asymmetric***

Radicalization in the digital space represents a significant transformation in the nature of security threats in the context of modern asymmetric warfare. In the conventional warfare paradigm, threats to the state are generally physical and territorial, characterized by the overt use of military force. However, in asymmetric warfare, non-state actors, including extremist and terrorist groups, adopt indirect strategies by exploiting structural, social, and ideological gaps to weaken the state. One of the primary instruments used is ideological propaganda based on digital information and communication.

Social media and digital platforms have evolved into a new domain of warfare, enabling extremist groups to systematically conduct influence operations. Ideological narratives are disseminated not only to recruit new members but also to establish alternative legitimacy to state authority. In the context of asymmetric warfare, these narratives function as non-kinetic weapons

that attack the cognitive and psychological aspects of society, with the ultimate goal of weakening public trust in the state and official institutions. The advantages of digital space lie in its characteristics of being cheap, fast, anonymous, and difficult for the state to fully control. This provides a strategic advantage for non-state actors, who, despite limited military resources, are able to compensate through narrative dominance. Extremist ideologies are packaged in the form of discourses of injustice, discrimination, identity marginalization, and narratives of moral and religious crisis. This pattern aligns with asymmetric warfare strategies oriented toward internal erosion, namely weakening the state's internal resilience through social and ideological fragmentation.

From a strategic defense perspective, digital radicalization can be understood as part of the non-military threats as regulated in the Indonesian National Defense System. Law Number 3 of 2002 concerning National Defense emphasizes that threats to state sovereignty are not only military in nature, but also include ideological, political, economic, social, cultural, and information technology threats. Digital radicalization is directly related to ideological and social threats that have the potential to disrupt national stability and national unity. Furthermore, Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism recognizes that terrorism is a multidimensional crime and requires a comprehensive preventive approach, including through counter-radicalization and deradicalization. This demonstrates that the state views the spread of extreme ideologies, including through digital media, as part of the spectrum of strategic threats that must be addressed not only through law enforcement but also with non-military approaches.

The complexity of this threat is further exacerbated by the diverse nature of society and the high penetration of social media. Indonesia has one of the world's largest social media users, making the digital space a primary arena for shaping public opinion. Digital radicalization has the potential to trigger horizontal conflict, deepen identity-based polarization, and undermine the social cohesion that has long been the foundation of national resilience. From an asymmetric warfare perspective, this situation greatly benefits extremist actors, allowing them to create instability without having to confront state officials directly.

Radicalization in the digital space cannot be reduced to merely a matter of crime or internal security. This phenomenon must be understood as part of a strategic threat to national defense, particularly within the spectrum of non-military threats and information warfare. Failure to manage this threat has the potential to weaken the nation's ideological resilience and open the door to broader conflict escalation. Therefore, addressing digital radicalization requires integration of defense policy, national security, and strategic communications strategies as part of the state's response to contemporary asymmetric warfare.

### ***The Concept and Role of Counter-Narratives in Prevention Digital Radicalization***

Counter-narratives are a strategic instrument in preventing digital radicalization that operate in the cognitive and psychological domains of society.

From a strategic defense perspective, counter-narratives can be understood as part of defensive information operations, aimed at protecting the public cognitive space from the infiltration of extremist ideologies. Unlike repressive approaches that emphasize law enforcement and security controls, counter-narratives work by challenging the construction of meaning constructed by radical groups through ideological propaganda in the digital space.

In the context of asymmetric warfare, extreme narratives function as a force multiplier for non-state actors with limited military capacity. Through narratives, radical groups are able to frame the state as illegitimate, oppressive, or contrary to certain religious and moral values. Counter-narratives exist to dismantle this logic by presenting rational, fact-based counterarguments aligned with national and humanitarian values. Thus, narratives are no longer merely communication tools but become ideological defense instruments with strategic value equal to other non-military instruments.

Conceptually, counter-narratives aim to delegitimize extreme ideologies by highlighting their internal contradictions, value deviations, and the destructive impact of ideologically motivated violence. This approach aligns with the principles of terrorism prevention as stipulated in Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, which emphasizes the importance of counter-radicalization and deradicalization efforts as part of the national strategy. The law implicitly recognizes that terrorism is not merely a criminal act but also an ideological phenomenon that requires narrative-based management and public awareness.

In addition to counter-narratives, alternative narratives play a strategic role in building long-term ideological resilience. Alternative narratives are not oriented toward direct confrontation with extreme narratives, but rather offer a positive discourse that emphasizes the values of inclusivity, tolerance, nationalism, and social participation. From a non-military defense perspective, alternative narratives serve as a structural prevention mechanism that minimizes the growth of extreme ideologies by strengthening national identity and a sense of belonging to the nation.

These two approaches align with the concept of total defense as mandated by Law Number 3 of 2002 concerning National Defense, which places all components of the nation as part of the national defense system. In this context, the public is not merely an object of protection but also an active subject in maintaining the nation's ideological resilience. Counter-narratives and alternative narratives enable civil society participation in non-military defense efforts through the production and dissemination of constructive narratives in the digital space.

The effectiveness of counter-narratives is largely determined by sensitivity to cultural, religious, and social aspects. Counter-narratives delivered in a normative, formalistic, or overly institutional manner tend to be less effective in reaching audiences, particularly the younger generation, who are the primary users of social media. Therefore, counter-narrative strategies need to be designed

adaptively, utilizing popular language, cultural symbols, and communication media closely related to the daily lives of Indonesians. Failure to manage narratives in the digital space has the potential to create strategic vulnerabilities that can be exploited by extremist actors. Conversely, systematically strengthening counter-narratives and alternative narratives can function as an ideological defense layer that strengthens national resilience. Thus, counter-narratives cannot be positioned as mere communication activities, but rather as an integral part of Indonesia's non-military defense strategy in the face of asymmetric threats and contemporary information warfare.

### *Mechanism The Spread of Counter-Narratives in the Indonesian Social Media Ecosystem*

The mechanism for the spread of counter-narratives in Indonesia's social media ecosystem must be understood within the framework of information warfare and asymmetric warfare, where the digital space functions as a strategic domain affecting national stability. Social media does not operate neutrally but is instead governed by engagement-based algorithms that prioritize content with high levels of interaction, such as anger, fear, and empathy. These characteristics inherently favor extreme narratives that are provocative and emotional, posing a major challenge for the state in disseminating constructive counter-narratives. From a strategic defense perspective, social media algorithms can be viewed as an operational environment that shapes the information battlefield. Extremist groups utilize these algorithms to expand the reach of ideological propaganda at low cost and with minimal risk. Therefore, counter-narratives cannot be disseminated using conventional, one-way, normative communication approaches. Counter-narratives must be packaged competitively, visually, emotionally, and narratively, to compete in the dense and rapidly changing flow of information.

This challenge aligns with the state's recognition of threats in cyberspace and information. Law No. 3 of 2002 concerning National Defense emphasizes that threats to the state encompass non-military dimensions, including ideological and informational threats. Furthermore, Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) and its amendments provide a legal basis for managing digital space, although in practice, these regulations remain more oriented toward enforcement than strategic narrative management. This demonstrates the need to strengthen non-repressive strategies, including counter-narratives, to complement legal policy. Messengers are a key element in the dissemination of counter-narratives. In the Indonesian context, public trust in state institutional accounts on social media is relatively limited, especially among the younger generation. Conversely, moderate religious figures, influencers, academics, and digital communities enjoy greater social legitimacy and are able to reach audiences more organically. From a holistic defense perspective, the involvement of these non-state actors reflects the principle of participation by all components of the nation in maintaining national resilience.

This approach aligns with the mandate of Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, which emphasizes the importance of community involvement in prevention, counter-radicalization, and deradicalization efforts. Disseminating counter-narratives through non-state actors allows the state to expand its reach without appearing dominant, while also reducing audience resistance to messages deemed overly political or institutional. In the context of asymmetric warfare, this strategy is effective because it leverages existing social networks as a force multiplier.

The form and format of content also play a strategic role in the success of counter-narratives. Content based on storytelling, personal experiences, short videos, educational memes, and visual narratives has proven more adaptable to Indonesians' information consumption patterns. This approach aligns with the emotional and identity-based nature of digital radicalization. By engaging with the audience's affective aspects, counter-narratives have a greater chance of influencing perceptions and attitudes than messages delivered in a formal and instructive manner.

The mechanism for disseminating counter-narratives demonstrates that preventing digital radicalization is a form of layered defense in the non-military realm. The state plays not only a regulatory and law enforcement role but also a facilitator of a healthy and resilient narrative ecosystem. The success of this strategy is largely determined by the ability of the state and society to adapt to the dynamics of digital technology, changes in audience behavior, and the evolution of extremist groups' propaganda tactics. Therefore, the mechanism for disseminating counter-narratives in Indonesia cannot be separated from the national defense strategy in facing asymmetric threats and information warfare. Managing narratives in the digital space must be viewed as a long-term strategic investment to strengthen ideological resilience, maintain social cohesion, and protect national stability amidst the complexity of contemporary security threats.

## **CONCLUSION AND RECOMMENDATION**

Radicalization in the digital space represents a transformation of security threats within the context of asymmetric warfare, where non-state actors utilize ideological narratives and information manipulation to undermine ideological resilience, social cohesion, and state legitimacy. Social media functions as a non-kinetic battlefield, enabling the massive, rapid, and difficult-to-control spread of extremist ideologies through conventional security approaches. Therefore, digital radicalization cannot be understood solely as a criminal issue, but rather as a strategic threat to national defense within the spectrum of non-military threats.

In facing these threats, counter-narratives and alternative narratives have proven to be crucial as non-military defense instruments. This approach operates within the cognitive and affective domains of society by challenging the legitimacy of extreme ideologies while simultaneously constructing positive narratives that reinforce national values, tolerance, and social participation. From a strategic defense perspective, counter-narratives can be positioned as part of

defensive information operations aimed at protecting the public's cognitive space from the infiltration of extreme ideologies.

The effectiveness of counter-narratives is heavily influenced by their dissemination mechanisms within Indonesia's social media ecosystem. Engagement-based algorithms, the credibility of the message-delivering actors, and the form and format of the content are key factors in the strategy's success. The involvement of socially legitimate non-state actors, such as moderate religious figures, academics, and digital communities, allows for a more organic and participatory spread of counter-narratives, while simultaneously reducing public resistance to state-delivered messages.

Based on these findings, it can be concluded that preventing digital radicalization in Indonesia requires a comprehensive approach that integrates defense policy, national security, and strategic communications. Counter-narratives cannot be treated as incidental communications activities, but must be an integral part of non-military defense strategies in the face of asymmetric threats and information warfare. Strengthening synergy between the state, civil society, and digital platforms is key to building a resilient narrative ecosystem to maintain national stability and the ideological resilience of the Indonesian nation.

#### **ADVANCED RESEARCH**

This study advances the understanding of digital radicalization in Indonesia as a strategic manifestation of asymmetric warfare operating within the cognitive domain, where non-state actors exploit social media architectures to erode ideological resilience, social cohesion, and state legitimacy. The findings demonstrate that counter-narratives and alternative narratives function not merely as communicative responses, but as structured non-military defense instruments embedded in defensive information operations designed to safeguard the public's cognitive space. Their effectiveness is contingent upon algorithmic dynamics, actor credibility, and adaptive content formats within Indonesia's digital ecosystem, with socially legitimate non-state actors playing a pivotal role in enhancing organic diffusion and minimizing resistance to state-aligned messaging. Accordingly, this research recommends the institutionalization of counter-narrative strategies within national defense doctrine through integrated coordination among defense institutions, civil society, and digital platforms, thereby constructing a resilient narrative ecosystem capable of mitigating information warfare and strengthening long-term national ideological stability.

## REFERENCES

- Ayu, A. M., Shabirah, S., & Putri, A. A. (2025). Penggunaan Media Sosial Instagram Sebagai Sarana Promosi Program Derakalisasi Oleh Bnpt Di Indonesia. *Jurnal Netnografi Komunikasi*, 4(2), 154-167.
- Hukumonline Newsroom. (2025, 6 Januari). Terorisme: Pengertian, faktor penyebab, dan jenis-jenisnya. <https://www.hukumonline.com/berita/a/terorisme-adalah-1t6183b09848f15/>
- Jasmine, B. N. M. (2021). Perlindungan hukum terhadap korban terorisme berdasarkan Undang-Undang Nomor 5 Tahun 2018 tentang perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 tentang pemberantasan tindak pidana terorisme menjadi undang-undang. *Jurnal ilmiah, Fakultas Hukum, Universitas Mataram*.
- Kementerian Pertahanan Republik Indonesia. (2025, 25 Juli). Peranan militer dalam pemberantasan aksi teror. Direktorat Jenderal Potensi Pertahanan. <https://www.kemhan.go.id/pothan/2025/07/25/peranan-militer-dalam-pemberantasan-aksi-teror.html>
- Prabangkaranews.com. (2020, Juli). Peran TNI dalam pemberantasan terorisme di Indonesia. <https://prabangkaranews.com/2020/07/peran-tni-dalam-pemberantasan-terorisme-di-indonesia/>
- Republik Indonesia. (2002). *Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara*. Jakarta: Sekretariat Negara.
- Republik Indonesia. (2004). *Undang-Undang Republik Indonesia Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia*. Jakarta: Sekretariat Negara.
- Republik Indonesia. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jakarta: Sekretariat Negara.
- Republik Indonesia. (2018). *Undang-Undang Republik Indonesia Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme*. Jakarta: Sekretariat Negara.
- Schmid, A. P. (2013). *Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review*. The Hague: ICCT.
- Snow, D. A., & Benford, R. D. (1988). Ideology, frame resonance, and participant mobilization. *International Social Movement Research*, 1, 197-217.
- Sugiarta, Y. R., Timur, F. G. C., & Sutanto, R. (2024). Analisis Konsep Kontra-Narasi Ekstrimisme dan Self-Control di Media Sosial Dalam Tinjauan Psikologi (Studi Kasus Kelompok Ekstrimisme ISIS). *Jurnal Kewarganegaraan*, 8(1), 331-339.

- Sulaiman, A., Sauki, M., & Susanto, J. (2023). Analisis Wacana Kritis Norman Fairclough Terhadap Gerakan Kontra Narasi Radikalisme Di Media Nu Online. *Communicative: Jurnal Komunikasi Dan Penyiaran Islam*, 4(1), 45-52.
- Ummah, A. H. (2020). Digital Media and Counter-Narrative of Radicalism. *Jurnal Theologia*, 31(2), 233-256.