MIKAILALSYS
Journal of Multidisciplinary Sciences

e-ISSN : 2987-2286
p-ISSN : 2987-3924

Index: Harvard, Boston, Sydney, Copernicus, Sinta 4, Scilit, Semantic, Google, etc

https://doi.org/10.58578/mikailalsys.v4i3.11695

Digital Radicalization and Indonesia's Counterterrorism Strategies in Addressing Technology-Based Terrorism

Arini Sabila Hidayatika & Pujo Widodo
Defense University, Indonesia
asabila622@gmail.com

Article Info:

Submitted:	Revised:	Accepted:	Published:
Jun 22, 2026	Jul 20, 2026	Aug 1, 2026	Aug 6, 2026

Abstract

Although digital radicalization and technology-enabled terrorism have received considerable scholarly attention, research integrating the dynamics of digital radicalization, Indonesia's legal framework, and institutional counterterrorism strategies within a unified analytical perspective remains limited. This study aimed to analyze the characteristics of digital radicalization in Indonesia, evaluate the adaptation of the national legal framework to technology-based terrorism, and examine institutional strategies for addressing emerging digital security threats. A qualitative documentary research design was employed, with sources purposively selected from primary legal documents, official government reports, policy publications, and peer-reviewed academic literature relevant to digital radicalization and counterterrorism. Data were collected through systematic document review and analyzed using qualitative thematic analysis involving data reduction, coding, categorization, thematic synthesis, and interpretation. The findings reveal three major themes. First, digital radicalization has transformed terrorism from an organization-centered phenomenon into a digitally mediated process characterized by the online dissemination of extremist content, technology-enabled recruitment, self-radicalization, and increased vulnerability

among children and adolescents. Second, Indonesia's regulatory framework has expanded beyond conventional criminal justice approaches by incorporating preventive governance, institutional coordination, and counter-radicalization policies through Law Number 5 of 2018, Presidential Regulation Number 8 of 2026, and the National Medium-Term Development Plan 2025–2029. Third, Indonesia's counterterrorism strategy has undergone institutional transformation through the integration of digital surveillance, collaborative governance, digital literacy, counter-narrative initiatives, and community-based prevention programs. The study concludes that addressing technology-based terrorism requires adaptive governance that combines legal reform, cross-sectoral coordination, and preventive digital resilience. The findings contribute to digital counterterrorism scholarship by integrating digital radicalization, regulatory adaptation, and institutional transformation within a single analytical framework. They also provide practical implications for policymakers, law enforcement agencies, cybersecurity institutions, educational organizations, and digital platform stakeholders seeking to strengthen Indonesia's capacity to respond to evolving technology-driven terrorist threats. Future research should empirically evaluate the implementation and effectiveness of these strategies and compare their application across national contexts.

Keywords: Counterterrorism Strategy; Digital Radicalization; Digital Security Governance; Indonesia; Technology-Enabled Terrorism

INTRODUCTION

The rapid advancement of information and communication technology has fundamentally transformed the nature of terrorism worldwide, including in Indonesia. Whereas terrorist networks previously relied on face-to-face recruitment, clandestine training camps, and hierarchical organizational structures, radicalization and recruitment processes are now increasingly conducted through digital platforms (Prindani & Syauqillah, 2025; Wibisono et al., 2025). Social media, encrypted messaging applications, online forums, and online games have become strategic channels for disseminating extremist propaganda, recruiting supporters, coordinating activities, and mobilizing terrorist networks more efficiently than conventional methods (Marizaldi et al., 2025; Syamsurrijal et al., 2024). This transformation indicates that digital technology, while providing substantial societal benefits, has simultaneously created new vulnerabilities that challenge national security (Putri, 2019; Sabar et al., 2026).

Indonesia has experienced this transformation in a significant way. According to the National Counterterrorism Agency (Badan Nasional Penanggulangan Terorisme/BNPT), digital devices that have become an integral part of everyday life are increasingly exploited as tools for spreading radical ideologies. The accessibility, anonymity, and algorithm-driven nature of digital platforms enable extremist content to circulate rapidly and reach diverse segments of society without geographical or temporal limitations. Consequently, radicalization no longer depends solely on direct interpersonal interaction but can occur through continuous exposure to online extremist content, allowing individuals to become radicalized independently (Conway, 2016; Maysarah et al., 2025; Meleagrou-Hitchens et al., 2017).

Recent empirical evidence demonstrates the scale of this challenge. At the end of 2025, BNPT reported that the Counter-Radicalization Task Force comprising BNPT, the State Intelligence Agency (BIN), the Indonesian National Armed Forces Strategic Intelligence Agency (BAIS), the Ministry of Communication and Digital Affairs, and the National Cyber and Crypto Agency (BSSN) identified 21,199 online contents containing elements of intolerance, radicalism, and terrorism. The report also documented 137 active perpetrators who utilized digital platforms for terrorist activities, 32 individuals who were radicalized online and subsequently joined terrorist networks, and 17 individuals who engaged in terrorist activities independently without direct affiliation with any terrorist organization, a phenomenon commonly referred to as *self-radicalization* (BNPT, 2025). These findings suggest that contemporary radicalization has evolved into a more individualized, covert, and technologically mediated process that is considerably more difficult to detect using conventional counterterrorism approaches (Oktavianus & Davidson, 2023; Umam et al., 2022; Unlu & Yilmaz, 2025).

The growing influence of digital radicalization has also affected children and adolescents. BNPT reported that at least 112 children were exposed to radical ideologies through social media and online games, where terrorist groups exploited digital content such as videos, memes, music, gaming environments, and narratives of heroism and false solidarity to attract vulnerable audiences. Considering that Indonesia has more than 200 million internet users while digital literacy and ideological resilience remain uneven across society, digital platforms have become fertile environments for the dissemination of extremist narratives and violent ideologies (Alsihab et al., 2025; Binder & Kenyon, 2022; Sabrina, 2026).

These developments indicate that terrorism should no longer be understood merely as a physical security threat but also as a digital phenomenon facilitated by technological innovation and online communication ecosystems. Consequently, conventional counterterrorism strategies that primarily emphasize law enforcement and military responses are no longer sufficient. Addressing digital radicalization requires a comprehensive approach that integrates legal frameworks, cybersecurity governance, digital platform regulation, digital literacy initiatives, and multi-stakeholder collaboration involving government institutions, technology companies, educational institutions, and civil society. Therefore, the effectiveness of contemporary counterterrorism policies increasingly depends on the state's capacity to respond to technologically mediated security threats (Greenberg, 2016; Huda, 2019; Riyanta, 2022).

The phenomenon of digital radicalization has received growing scholarly attention in recent years. Conway et al. (2016) argue that digital media have fundamentally transformed terrorist propaganda and recruitment through social networking platforms, online communities, and encrypted communication technologies. Similarly, Howard et al. (2024) demonstrates that digital technologies have significantly expanded the operational capabilities of extremist organizations by facilitating transnational communication and online mobilization. Bastug et al. (2020) further emphasizes that online radicalization differs substantially from traditional radicalization because it is often individualized, gradual, algorithmically reinforced, and capable of occurring without direct organizational contact. Within the Indonesian context, previous studies have primarily examined BNPT's deradicalization programs, terrorist propaganda on social media, or the implementation of Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism.

Despite these contributions, existing studies generally examine digital radicalization, legal frameworks, or counterterrorism strategies as separate issues. Comprehensive analyses that integrate the dynamics of digital radicalization with Indonesia's legal framework and national strategies for addressing technology-based terrorism remain limited. As terrorist activities increasingly shift from physical networks to digital ecosystems, there is an urgent need to evaluate whether existing legal and policy frameworks adequately address the evolving characteristics of technology-enabled terrorism. This gap provides the primary scholarly justification for the present study.

Accordingly, this study contributes to the literature by integrating three interrelated dimensions: digital radicalization, Indonesia's legal framework for counterterrorism, and national strategies for addressing technology-based terrorism. Unlike previous studies that tend to analyze these dimensions independently, this research adopts the perspectives of *digital radicalization* and *security governance* to examine how technological transformation reshapes terrorist threats and how national legal and policy responses should evolve accordingly. This integrated perspective is expected to enrich the academic discourse on digital counterterrorism while providing policy recommendations for strengthening Indonesia's capacity to respond to emerging technology-driven security threats.

Based on the foregoing discussion, this study aims to analyze the development of digital radicalization in Indonesia, evaluate the adequacy of the existing legal framework in addressing technology-based terrorism, and identify appropriate counterterrorism strategies for responding to evolving digital threats. By addressing these objectives, the study seeks to contribute to the growing body of knowledge on digital counterterrorism and to provide practical insights for policymakers in developing more adaptive and effective strategies for preventing radicalization and terrorism in cyberspace.

METHODS

Type of Research

This study employed a qualitative research approach using a descriptive-analytical design. A qualitative approach was selected because the study aims to understand and critically analyze the phenomenon of digital radicalization and Indonesia's legal and policy responses to technology-based terrorism rather than to measure causal relationships quantitatively. Specifically, the research adopted a library research design, which relies on the systematic examination of legal documents, policy reports, scholarly publications, and other documentary evidence relevant to the research objectives. This approach enables an in-depth understanding of the evolving characteristics of digital radicalization and the adequacy of Indonesia's counterterrorism framework in responding to emerging technology-driven threats (Creswell, 2014; Sugiyono, 2024).

Research Design

The research was designed as a qualitative document-based analysis integrating legal and policy analysis with contemporary literature on digital radicalization and

counterterrorism. The analytical framework consisted of three sequential stages. First, the study identified the characteristics and trends of digital radicalization in Indonesia by examining official statistics, policy reports, and empirical studies. Second, the study analyzed Indonesia's existing legal framework governing counterterrorism, particularly Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism and its implementing regulations, to evaluate their relevance in addressing technology-based terrorism (Rahmadhani et al., 2023, 2025). Third, the findings from both analyses were synthesized to identify strategic policy responses that are consistent with the evolving characteristics of digital terrorist activities. This design ensures alignment between the research objectives, documentary evidence, and analytical procedures.

Data Sources and Document Selection

Because this study is based entirely on documentary evidence, no human participants or respondents were involved. Instead, the unit of analysis consisted of legal documents, government reports, policy publications, institutional reports, and peer-reviewed academic literature related to digital radicalization and technology-based terrorism.

Primary sources included Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism and related implementing regulations. Secondary sources consisted of official reports and press releases published by the National Counterterrorism Agency (BNPT), publications issued by relevant Indonesian government institutions, reports from internationally recognized research organizations such as RAND Corporation, peer-reviewed journal articles, and academic books discussing digital radicalization, cybersecurity, online extremism, and counterterrorism.

Documents were selected through purposive sampling based on three criteria: (1) direct relevance to digital radicalization, counterterrorism, cybersecurity, or technology-based terrorism; (2) publication by credible institutions or peer-reviewed academic publishers; and (3) publication within the last five to ten years whenever possible to ensure the currency and relevance of the evidence. Earlier seminal publications were included only when necessary to explain important theoretical concepts.

Data Collection Procedures

Data were collected through systematic document review. The collection process began with the identification of relevant legal documents and official government publications, followed by the retrieval of scholarly articles from internationally indexed

academic databases and reputable institutional reports. Each document was reviewed to identify information related to patterns of digital radicalization, legal provisions governing counterterrorism, institutional responses, and recommended policy strategies.

To enhance the trustworthiness of the findings, data triangulation was applied by comparing information obtained from multiple sources, including legislation, official government reports, international research institutions, and peer-reviewed academic literature. Cross-source verification was conducted to minimize potential bias and ensure consistency in interpreting the empirical evidence.

Data Analysis

The collected data were analyzed using qualitative thematic analysis. The analytical process consisted of four stages. First, data reduction was conducted by selecting documents and information directly relevant to the research objectives. Second, the selected data were coded and categorized into major themes, including patterns of digital radicalization, legal and regulatory frameworks, institutional counterterrorism responses, and strategic policy recommendations. Third, the categorized data were interpreted through descriptive and comparative analysis to identify relationships between the changing characteristics of digital terrorism and Indonesia's existing legal and policy responses. Finally, the findings were synthesized to formulate an integrated analysis of Indonesia's strategies for addressing technology-based terrorism and to identify areas requiring further policy development. This systematic analytical procedure enabled the study to produce a comprehensive understanding of digital radicalization while ensuring transparency and analytical rigor throughout the research process.

RESULTS

Digital Radicalization as an Evolving Modality of Contemporary Terrorism

The qualitative document analysis identified the transformation of radicalization from a predominantly organization-based process into a digitally mediated phenomenon as the first major analytical theme. This theme consistently emerged across the reviewed legal documents, official government publications, policy reports, and institutional documents issued by the National Counterterrorism Agency (BNPT), the Ministry of Communication and Digital Affairs, the National Cyber and Crypto Agency (BSSN), and other relevant

institutions. Rather than describing radicalization as an activity confined to physical interaction and organizational indoctrination, the reviewed documents consistently portray digital technology as the principal environment through which extremist narratives are disseminated, reinforced, and reproduced.

The coding process generated three interrelated analytical categories that characterize the contemporary landscape of digital radicalization in Indonesia. The first category concerns the digitalization of extremist dissemination, referring to the extensive use of digital communication platforms as the primary medium for spreading extremist narratives. The second category relates to the emergence of self-radicalization, in which individuals become exposed to and internalize extremist ideology without direct organizational recruitment. The third category concerns the growing vulnerability of children and adolescents, reflecting the increasing tendency of extremist actors to target younger internet users through digital entertainment platforms and social media ecosystems.

Across the reviewed documents, digital platforms are consistently portrayed not merely as communication channels but as operational environments in which ideological dissemination, recruitment, networking, and psychological reinforcement occur simultaneously. Official policy documents repeatedly indicate that terrorist organizations have adapted their operational strategies to technological developments by utilizing algorithm-driven platforms capable of amplifying extremist narratives to large audiences within a relatively short period. Consequently, digital radicalization is documented not as an isolated cyber phenomenon but as an integral component of contemporary terrorist operations.

The documentary evidence also demonstrates that digital radicalization extends beyond conventional social media platforms. Several official reports identify encrypted messaging applications, online discussion forums, video-sharing platforms, and online games as additional environments where extremist narratives circulate. This diversification of communication channels indicates that extremist organizations have increasingly adopted multi-platform communication strategies to maximize audience reach while simultaneously reducing the risk of disruption through single-platform enforcement mechanisms.

Table 1. Analytical Findings on the Characteristics of Digital Radicalization in Indonesia

No.	Analytical Category	Documentary Evidence	Empirical Indicators
1	Digital dissemination of extremist content	BNPT identified 21,199 online contents containing elements of intolerance, radicalism, and terrorism during 2025.	Large-scale dissemination of extremist narratives through digital platforms.
2	Technology-enabled terrorist activities	137 individuals actively utilized digital platforms to facilitate terrorist-related activities.	Digital technologies are increasingly incorporated into terrorist operational activities.
3	Online radicalization and recruitment	32 individuals were radicalized through online exposure before joining terrorist organizations.	Digital platforms function as channels for ideological dissemination and recruitment.
4	Self-radicalization	17 individuals engaged in terrorist activities without direct affiliation with established terrorist organizations.	Radicalization may occur independently through prolonged exposure to online extremist content.
5	Vulnerability of children and adolescents	BNPT documented 112 children exposed to radical ideologies through social media and online gaming platforms.	Children and adolescents constitute an emerging vulnerable group within digital environments.

Source: Processed by the author based on BNPT (2025).

As presented in Table 1, "Analytical Findings on the Characteristics of Digital Radicalization in Indonesia," the reviewed documents consistently indicate that digital radicalization is characterized by multiple interconnected dimensions rather than by the dissemination of extremist propaganda alone. The documentary evidence suggests that digital technology functions simultaneously as a medium for ideological transmission, organizational communication, recruitment, operational coordination, and psychological reinforcement. These functions collectively demonstrate the expanding role of digital ecosystems within contemporary terrorist activities.

The first analytical category concerns the increasing reliance on digital platforms for ideological dissemination. The reviewed policy documents consistently report that extremist narratives are distributed through multiple forms of digital content, including videos, images, memes, podcasts, discussion forums, short-form social media content, and encrypted communication channels. This pattern demonstrates that ideological dissemination has become highly diversified, allowing extremist organizations to adapt communication strategies according to platform characteristics and target audiences. Furthermore, official reports indicate that algorithm-driven recommendation systems contribute to repeated exposure to extremist narratives by continuously suggesting related content to users who have previously interacted with similar materials.

The second analytical category concerns the emergence of self-radicalization as a prominent characteristic of technology-based terrorism. Unlike conventional radicalization processes, which generally involve direct interaction between recruiters and prospective members, the reviewed documents describe self-radicalization as an individualized process resulting from sustained exposure to online extremist narratives. Documentary evidence indicates that individuals may gradually internalize extremist ideology through repeated engagement with digital content before eventually engaging in terrorist-related activities without formal organizational membership. This pattern reflects a significant shift in operational dynamics, whereby ideological commitment may develop independently from traditional organizational structures.

The document analysis further reveals that self-radicalization complicates institutional monitoring efforts because radicalization may occur entirely within private digital environments. Unlike traditional recruitment processes involving identifiable interpersonal networks, digitally mediated radicalization frequently develops through personalized online interactions, algorithmically recommended content, and anonymous communication channels. Consequently, documentary evidence indicates that the identification of radicalization pathways has become increasingly challenging for law enforcement and counterterrorism agencies.

The third analytical category emerging from the coding process concerns the increasing vulnerability of children and adolescents. Across the reviewed documents, younger internet users are consistently identified as priority targets due to their intensive engagement with digital technologies and interactive online environments. Rather than relying exclusively on ideological materials explicitly associated with extremist organizations, terrorist actors increasingly embed narratives of heroism, solidarity, identity, and belonging within entertainment-oriented digital content. Such narratives are disseminated through social media platforms, online gaming communities, digital videos, music, memes, and other forms of interactive media that are widely consumed by younger audiences.

The documentary evidence also indicates that children and adolescents are not targeted solely because of their age but because of their position within highly interconnected digital ecosystems characterized by continuous information exposure and algorithmically personalized content recommendations. As internet penetration continues to expand throughout Indonesia, digital platforms provide extremist actors with opportunities to reach

increasingly diverse demographic groups regardless of geographical location. Consequently, the reviewed documents consistently portray digital radicalization as an issue extending beyond national security to encompass broader concerns relating to education, digital literacy, child protection, and cyber governance.

Taken together, the findings generated from the document analysis demonstrate that the operational landscape of radicalization in Indonesia has undergone a substantial transformation. The reviewed documents consistently identify digital technology as a central enabling environment through which extremist organizations disseminate ideological narratives, facilitate recruitment, strengthen organizational communication, and influence vulnerable individuals. These findings establish digital radicalization as the dominant empirical pattern emerging from the documentary evidence analyzed in this study and provide the analytical basis for examining the adequacy of Indonesia's legal and institutional responses presented in the subsequent sections.

Regulatory Adaptation toward Technology-Based Terrorism

The second analytical theme generated from the qualitative document analysis concerns the regulatory adaptation of Indonesia's counterterrorism framework in response to the emergence of technology-based terrorism. The reviewed legal documents consistently indicate that the evolution of terrorist activities into digital environments has been accompanied by significant developments in Indonesia's legal and policy architecture. Rather than relying solely on criminal prosecution, the current regulatory framework increasingly incorporates preventive governance, institutional coordination, and multi-sectoral collaboration as integral components of national counterterrorism policy.

The coding process identified four major regulatory dimensions that characterize Indonesia's contemporary counterterrorism framework. The first dimension relates to the expansion of criminal jurisdiction, reflecting the state's effort to accommodate emerging forms of terrorism within the national legal system. The second dimension concerns the institutionalization of preventive measures, emphasizing that counterterrorism extends beyond law enforcement through national preparedness, counter-radicalization, and deradicalization initiatives. The third dimension refers to inter-agency coordination, highlighting the collaborative roles of multiple governmental institutions in responding to terrorism. Finally, the fourth dimension concerns policy mainstreaming, whereby counterterrorism has been integrated into broader national development planning.

The reviewed legislation demonstrates that Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism represents the principal legal instrument governing Indonesia's counterterrorism efforts. The documentary evidence indicates that the law significantly broadens the scope of criminal liability by recognizing new forms of terrorist activities, strengthening preventive mechanisms, and expanding the authority of law enforcement agencies and BNPT in coordinating counterterrorism initiatives. The reviewed documents also show that the law establishes a more comprehensive approach by combining punitive and preventive measures within a single regulatory framework.

In addition to statutory provisions, the document analysis identified Presidential Regulation Number 8 of 2026 concerning the National Action Plan for Preventing and Countering Violent Extremism Leading to Terrorism (2026–2029) as the primary policy instrument guiding the implementation of preventive strategies. The regulation provides an institutional framework through which ministries, government agencies, regional governments, educational institutions, civil society organizations, and other stakeholders coordinate counter-radicalization and deradicalization programs. The reviewed policy documents consistently describe this regulation as an operational mechanism for translating statutory provisions into coordinated institutional actions.

Furthermore, documentary evidence indicates that counterterrorism has become increasingly embedded within Indonesia's broader development agenda. The reviewed planning documents demonstrate that the National Medium-Term Development Plan (RPJMN) 2025–2029 explicitly incorporates counterterrorism into national priorities concerning defense, security, and social resilience. This finding suggests that counterterrorism is positioned not merely as a criminal justice issue but also as a strategic component of national governance and sustainable development planning.

Table 2. Regulatory Characteristics of Indonesia's Counterterrorism Framework

Analytical Category	Primary Documentary Sources	Empirical Evidence Identified
Expansion of legal authority	Law Number 5 of 2018	Broader criminalization of terrorism-related offences, strengthened investigative powers, and enhanced preventive authority.
Institutionalized prevention	Law Number 5 of 2018; Presidential Regulation Number 8 of 2026	Counterterrorism policy formally incorporates national preparedness, counter-radicalization, and deradicalization as preventive pillars.
Multi-agency governance	BNPT policy documents; Presidential Regulation Number 8 of 2026	Formal coordination among BNPT, ministries, intelligence agencies, law enforcement institutions,

Analytical Category	Primary Documentary Sources	Empirical Evidence Identified
		regional governments, and non-governmental stakeholders.
Policy mainstreaming	RPJMN 2025–2029	Counterterrorism is incorporated into Indonesia's long-term national development and security agenda.

Source: Processed by the author from Law Number 5 of 2018, Presidential Regulation Number 8 of 2026, RPJMN 2025–2029, and BNPT policy documents.

As presented in Table 2, "Regulatory Characteristics of Indonesia's Counterterrorism Framework," the documentary evidence demonstrates that Indonesia's legal and policy architecture has evolved through four complementary regulatory dimensions. The reviewed documents consistently indicate that legal adaptation is reflected not only in the expansion of substantive criminal provisions but also in the institutionalization of preventive governance mechanisms and broader intergovernmental coordination.

The first regulatory dimension concerns the expansion of criminal jurisdiction. The reviewed legislation indicates that Law Number 5 of 2018 broadens the legal definition of terrorism and provides additional authority for addressing evolving terrorist activities. Documentary evidence further shows that the revised legislation introduces provisions enabling earlier intervention against terrorist activities while strengthening sanctions applicable to individuals and corporate entities involved in terrorism-related offences.

The second dimension concerns preventive governance. The document analysis reveals that preventive measures are systematically incorporated into Indonesia's counterterrorism framework through programs addressing national preparedness, counter-radicalization, and deradicalization. These preventive components appear consistently across statutory and policy documents, indicating that prevention constitutes a formal component of national counterterrorism governance rather than an auxiliary policy initiative.

The third analytical dimension emerging from the reviewed documents relates to institutional coordination. Documentary evidence consistently identifies BNPT as the coordinating institution responsible for integrating the activities of multiple governmental bodies, including intelligence agencies, law enforcement institutions, ministries, and regional governments. The reviewed policy documents demonstrate that counterterrorism

implementation increasingly depends upon institutional coordination across administrative sectors rather than upon isolated organizational responses.

The fourth regulatory dimension concerns policy integration within national development planning. The reviewed RPJMN documents indicate that counterterrorism policies are increasingly linked with broader objectives relating to social resilience, national security, human resource development, and community empowerment. This integration reflects the positioning of counterterrorism as a cross-sectoral governance issue within Indonesia's national policy framework.

Overall, the qualitative document analysis demonstrates that Indonesia's regulatory response to technology-based terrorism has developed through a multidimensional governance framework characterized by expanded legal authority, preventive policy instruments, coordinated institutional arrangements, and integration into long-term national development planning. These empirical findings establish the regulatory context within which national counterterrorism strategies are implemented and provide the basis for examining institutional responses presented in the following analytical theme.

Institutional Transformation of Indonesia's Counterterrorism Strategy

The third analytical theme generated from the qualitative document analysis concerns the institutional transformation of Indonesia's counterterrorism strategy in responding to technology-based terrorism. The reviewed policy documents consistently demonstrate that Indonesia's counterterrorism approach has evolved from a predominantly law enforcement-oriented model toward a broader governance framework emphasizing prevention, institutional coordination, community engagement, and digital resilience. This transformation is reflected not only in the expansion of institutional responsibilities but also in the diversification of strategic instruments employed to address the changing characteristics of digital terrorism.

The coding process identified four principal strategic components that consistently appeared across the reviewed documentary sources. The first component relates to digital monitoring and online content management, reflecting efforts to identify and disrupt the dissemination of extremist content across digital platforms. The second component concerns multi-stakeholder governance, characterized by institutional collaboration among governmental agencies, academia, civil society organizations, media institutions, and the private sector. The third component refers to digital literacy and counter-narrative initiatives,

aimed at strengthening public resilience against extremist propaganda. The fourth component concerns early prevention and community engagement, emphasizing preventive intervention among vulnerable communities before radicalization develops into violent extremism.

Across the reviewed documents, BNPT is consistently identified as the central coordinating institution responsible for integrating counterterrorism policies across multiple governmental sectors. Documentary evidence indicates that institutional coordination involves intelligence agencies, law enforcement bodies, the Ministry of Communication and Digital Affairs, the National Cyber and Crypto Agency (BSSN), educational institutions, regional governments, and community organizations. This institutional arrangement illustrates that counterterrorism implementation increasingly relies upon collaborative governance mechanisms rather than isolated organizational responses.

The document analysis also reveals that digital monitoring has become one of the principal operational components of Indonesia's counterterrorism strategy. Official reports describe the establishment of coordinated mechanisms for identifying, verifying, and responding to online content containing elements of radicalism, violent extremism, and terrorism. The reviewed documents indicate that these monitoring activities involve inter-agency coordination aimed at supporting timely intervention and limiting the circulation of extremist narratives across digital platforms.

Another recurrent finding concerns the implementation of digital literacy and counter-narrative programs. The reviewed policy documents consistently identify public education as an important institutional strategy for strengthening societal resilience against extremist ideology. Documentary evidence indicates that these initiatives target diverse segments of society through educational campaigns, public awareness activities, and community-based engagement programs designed to improve critical understanding of digital information.

The documentary evidence further demonstrates that preventive intervention increasingly focuses on children, adolescents, educational institutions, and local communities. Programs such as *Sekolah Damai*, *Kampus Kebangsaan*, and *Desa Siapsiaga* are repeatedly identified in official reports as institutional mechanisms intended to strengthen community resilience and facilitate early prevention. The reviewed documents also highlight the role of the Forum Koordinasi Pencegahan Terorisme (FKPT) in implementing

preventive initiatives across Indonesia's provinces through collaboration with local governments and civil society organizations.

Table 3. Institutional Strategies for Countering Technology-Based Terrorism in Indonesia

Analytical Category	Primary Documentary Sources	Empirical Evidence Identified
Digital surveillance and content moderation	BNPT Annual Reports; Ministry of Communication and Digital Affairs; BSSN publications	Coordinated monitoring, verification, and removal of online content containing elements of radicalism, violent extremism, and terrorism.
Collaborative institutional governance	BNPT Strategic Documents; Presidential Regulation Number 8 of 2026; RAN PE	Formal coordination among BNPT, ministries, intelligence agencies, law enforcement institutions, regional governments, academia, civil society organizations, media, and the private sector.
Digital literacy and counter-narrative programs	BNPT Policy Reports; National Action Plan for Preventing and Countering Violent Extremism (RAN PE)	Implementation of public education, digital literacy campaigns, and counter-narrative initiatives designed to strengthen societal resilience against extremist content.
Community-based prevention and early intervention	FKPT Reports; BNPT Community Programs	Preventive initiatives implemented through Sekolah Damai, Kampus Kebangsaan, Desa Siapsiaga, early warning systems, and community engagement mechanisms across Indonesia's provinces.

Source: Processed by the author from BNPT annual reports, Presidential Regulation Number 8 of 2026, the National Action Plan for Preventing and Countering Violent Extremism (RAN PE), FKPT reports, publications of the Ministry of Communication and Digital Affairs, and BSSN documents.

As presented in Table 3, "Institutional Strategies for Countering Technology-Based Terrorism in Indonesia," the reviewed documents consistently demonstrate that Indonesia's counterterrorism strategy is implemented through four complementary institutional dimensions. Rather than emphasizing a single operational approach, the documentary evidence indicates that technology-based terrorism is addressed through coordinated digital monitoring, institutional collaboration, public resilience programs, and preventive community engagement.

The first strategic dimension concerns digital monitoring and online content management. Documentary evidence indicates that government institutions have established coordinated mechanisms to identify extremist digital content, verify potential threats, and implement appropriate response measures. These activities constitute one of the primary operational components identified throughout the reviewed policy documents.

The second strategic dimension relates to multi-stakeholder governance. The reviewed documents consistently describe counterterrorism implementation as a collaborative process involving multiple governmental institutions together with academic institutions, civil society organizations, media organizations, and private-sector actors. This collaborative arrangement appears repeatedly across national policy documents as an institutional mechanism supporting coordinated implementation of preventive programs.

The third strategic dimension concerns digital literacy and counter-narrative initiatives. The documentary evidence identifies these programs as institutional efforts designed to strengthen public awareness and resilience against extremist propaganda disseminated through digital platforms. Across the reviewed documents, educational campaigns and public awareness initiatives are consistently presented as complementary measures supporting broader national prevention strategies.

The fourth strategic dimension emerging from the qualitative document analysis concerns early prevention and community engagement. Documentary evidence indicates that preventive programs increasingly prioritize vulnerable communities through educational institutions, community organizations, and regional coordination mechanisms. Programs coordinated by FKPT across Indonesia's provinces demonstrate the institutionalization of community-based prevention within Indonesia's broader counterterrorism strategy.

Overall, the documentary evidence indicates that Indonesia's institutional response to technology-based terrorism has developed into a multidimensional governance framework integrating digital monitoring, preventive education, institutional collaboration, and community engagement. These findings demonstrate that the reviewed policy documents consistently position counterterrorism as a cross-sectoral governance responsibility implemented through coordinated institutional arrangements at both national and regional levels.

DISCUSSION

Digital Radicalization and the Transformation of Contemporary Terrorism

The findings demonstrate that digital radicalization has fundamentally transformed the operational characteristics of terrorism in Indonesia. The document analysis indicates that terrorist organizations no longer depend primarily on hierarchical organizational structures or face-to-face recruitment. Instead, digital platforms have become integrated

environments where ideological dissemination, recruitment, socialization, and operational communication occur simultaneously. This finding suggests that the locus of radicalization has shifted from physical interaction toward digitally mediated engagement, thereby altering both the mechanisms of ideological transmission and the institutional challenges faced by counterterrorism agencies.

From the perspective of digital radicalization, this transformation reflects the capacity of digital technologies to reshape extremist communication patterns through algorithm-driven content distribution, personalized information exposure, and networked online communities. Digital platforms not only accelerate the dissemination of extremist narratives but also create conditions that facilitate prolonged ideological exposure. Consequently, radicalization increasingly develops through repeated interaction with online content rather than direct organizational indoctrination. This interpretation is consistent with Conway et al. (2023), who argue that contemporary terrorist organizations strategically exploit digital communication technologies to expand ideological outreach while minimizing operational risks associated with conventional recruitment.

The emergence of self-radicalization identified in this study further reinforces the changing nature of contemporary terrorism. Unlike conventional recruitment models that rely upon interpersonal relationships and organizational supervision, self-radicalization enables individuals to internalize extremist narratives independently through sustained online engagement. This finding supports the observations of Koehler (2021), who emphasizes that online radicalization increasingly occurs through individualized pathways in which algorithmic recommendation systems continuously reinforce ideological preferences. Such developments complicate early detection because radicalization may occur without direct organizational affiliation or observable interpersonal interaction.

Another important finding concerns the increasing vulnerability of children and adolescents within digital environments. The documentary evidence indicates that extremist actors deliberately utilize social media platforms, online games, and entertainment-oriented digital content to reach younger audiences. Rather than presenting ideological messages explicitly, extremist narratives are frequently embedded within themes of identity, belonging, heroism, and solidarity. This pattern suggests that digital radicalization should not be understood solely as a cybersecurity issue but also as a challenge involving digital literacy, education, child protection, and social resilience. Consequently, preventing online

radicalization requires broader societal interventions extending beyond conventional law enforcement measures.

Overall, these findings indicate that the transformation of terrorism is not merely technological but structural. Digital technology has altered how extremist organizations communicate, recruit supporters, construct ideological identities, and maintain operational continuity. Therefore, counterterrorism strategies should recognize digital ecosystems as primary operational spaces rather than supplementary communication channels.

Regulatory Adaptation and the Evolution of Counterterrorism Governance

The second major finding demonstrates that Indonesia's legal framework has evolved from a predominantly punitive approach toward a more comprehensive governance model incorporating preventive measures, institutional coordination, and long-term policy planning. The document analysis indicates that Law Number 5 of 2018 and Presidential Regulation Number 8 of 2026 collectively establish a regulatory architecture that extends beyond criminal prosecution by formally integrating national preparedness, counter-radicalization, and deradicalization into Indonesia's counterterrorism policy.

Viewed through the perspective of security governance, these developments illustrate a transition from state-centric law enforcement toward collaborative governance involving multiple public institutions and non-state actors. Rather than assigning sole responsibility to security agencies, the reviewed policy documents position ministries, intelligence agencies, regional governments, educational institutions, civil society organizations, and community stakeholders as complementary actors within Indonesia's national counterterrorism framework. This institutional arrangement reflects the recognition that technology-based terrorism cannot be addressed effectively through criminal justice mechanisms alone.

The findings also demonstrate that counterterrorism has become increasingly integrated into Indonesia's broader development agenda. The incorporation of counterterrorism priorities into the National Medium-Term Development Plan (RPJMN) indicates that violent extremism is increasingly understood as a multidimensional governance issue with implications for national resilience, social cohesion, and sustainable development. This institutional mainstreaming broadens the policy scope of counterterrorism beyond emergency response toward long-term prevention and resilience building.

Nevertheless, the rapid evolution of digital technologies continues to challenge regulatory adaptation. Terrorist actors frequently exploit technological innovations that evolve faster than formal legal and institutional responses. Consequently, legal frameworks require continuous review to ensure that emerging technologies including encrypted communication platforms, artificial intelligence, decentralized digital infrastructures, and evolving online ecosystems remain adequately addressed within Indonesia's counterterrorism governance.

Institutional Transformation and Strategic Implications for Technology-Based Counterterrorism

The third major finding demonstrates that Indonesia's institutional response has progressively shifted toward a multidimensional counterterrorism strategy integrating digital surveillance, collaborative governance, digital literacy, and community-based prevention. This finding suggests that institutional transformation has occurred alongside the changing characteristics of terrorism itself. As terrorist activities become increasingly technology-driven, institutional responses have likewise expanded beyond operational enforcement toward preventive and adaptive governance mechanisms.

The identification of digital surveillance and online content moderation as central institutional strategies reflects the increasing importance of cyberspace within national security governance. However, the findings also indicate that surveillance alone cannot eliminate the underlying processes of radicalization. Extremist narratives continuously migrate across digital platforms, adopt new communication formats, and exploit emerging technologies, thereby requiring institutional flexibility and continuous policy adaptation.

The prominence of digital literacy and counter-narrative initiatives identified in this study further demonstrates that prevention has become a strategic priority within Indonesia's counterterrorism framework. Strengthening citizens' ability to critically evaluate digital information reduces susceptibility to extremist narratives and complements conventional security measures. These findings reinforce the view that public resilience constitutes an essential component of contemporary counterterrorism governance.

The document analysis also highlights the importance of community-based prevention through programs such as *Sekolah Damai*, *Kampus Kebangsaan*, *Desa Siapsiaga*, and the activities coordinated by the Forum Koordinasi Pencegahan Terorisme (FKPT). These initiatives illustrate how national policy is operationalized through local institutional

networks capable of engaging vulnerable communities before radicalization develops into violent extremism. Such institutional arrangements strengthen the preventive dimension of Indonesia's counterterrorism strategy while promoting greater coordination between national and regional stakeholders.

This study contributes to the literature by integrating analyses of digital radicalization, regulatory adaptation, and institutional transformation within a single analytical framework. Previous studies have generally examined these dimensions separately, focusing either on online radicalization, legal reform, or deradicalization programs. By synthesizing these dimensions, the present study demonstrates that effective responses to technology-based terrorism require simultaneous adaptation of legal frameworks, institutional governance, and preventive strategies. This integrated perspective provides a more comprehensive understanding of how Indonesia is responding to the evolving challenges posed by digital terrorism and offers a conceptual basis for strengthening future counterterrorism policies in increasingly complex digital environments.

CONCLUSION

This study demonstrates that the emergence of digital technologies has fundamentally transformed the characteristics of terrorism in Indonesia from a predominantly physical and organization-based phenomenon into a digitally mediated security challenge. The findings indicate that digital platforms have evolved beyond communication tools into operational environments that facilitate ideological dissemination, online recruitment, self-radicalization, and the targeting of vulnerable groups, particularly children and adolescents. In response to these developments, Indonesia has progressively adapted its legal and institutional framework through the enactment of Law Number 5 of 2018, the implementation of Presidential Regulation Number 8 of 2026, and the integration of counterterrorism into broader national development policies. Furthermore, the study finds that Indonesia's counterterrorism strategy has expanded from a predominantly law-enforcement approach toward a multidimensional governance model incorporating preventive measures, digital surveillance, institutional coordination, digital literacy, and community-based engagement.

The findings contribute to the growing body of knowledge on digital counterterrorism by integrating three interrelated dimensions digital radicalization, regulatory

adaptation, and institutional transformation within a single analytical framework. While previous studies have generally examined these dimensions separately, this study demonstrates that effective responses to technology-based terrorism require the simultaneous adaptation of legal frameworks, institutional governance, and preventive strategies. Accordingly, the study provides both a conceptual contribution to the understanding of contemporary counterterrorism governance and a practical contribution by highlighting the importance of coordinated, multi-sectoral approaches in responding to increasingly complex digital security threats.

Future research should extend the present study by examining the implementation and effectiveness of Indonesia's counterterrorism policies through empirical approaches, including interviews, case studies, or mixed-methods research involving relevant stakeholders at both national and regional levels. Comparative studies across countries or analyses focusing on emerging technologies, such as artificial intelligence, encrypted communication platforms, and decentralized digital ecosystems, would also provide deeper insights into the evolving dynamics of technology-based terrorism. Such research would strengthen the evidence base for developing adaptive counterterrorism policies capable of responding to the rapidly changing digital landscape.

REFERENCES

Aprilia, N. Alsihab, M. A., Sriwidodo, J., & Rohman, A. N. (2025). Analisis Yuridis Penanganan Strategi Deradikalisasi Digital oleh Densus 88 Anti Teror Polri dalam Mencegah Rekrutmen Terorisme di Media Sosial. *Jurnal Hukum Sasana, 11*(2), 179–196. https://ejurnal.ubharajaya.ac.id/index.php/SASANA/article/view/4647

Bastug, M. F., Douai, A., & Akca, D. (2020). Exploring the "demand side" of online radicalization: Evidence from the Canadian context. *Studies in Conflict & Terrorism, 43*(7), 616–637. https://doi.org/10.1080/1057610X.2018.1494409

Binder, J. F., & Kenyon, J. (2022). Terrorism and the internet: How dangerous is online radicalization? *Frontiers in Psychology, 13*, Article 997390. https://doi.org/10.3389/fpsyg.2022.997390

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism, 40*(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE Publications.

Greenberg, K. J. (2016). Counter-radicalization via the internet. *The ANNALS of the American Academy of Political and Social Science, 668*(1), 165–179. https://doi.org/10.1177/0002716216672635

Howard, T., Poston, B., & Lopez, A. (2024). Extremist radicalization in the virtual era: Analyzing the neurocognitive process of online radicalization. *Studies in Conflict & Terrorism, 47*(8), 862–887. https://doi.org/10.1080/1057610X.2021.2016558

Huda, A. Z. (2019). Melawan Radikalisme melalui Kontra Narasi Online. *Journal of Terrorism Studies, 1*(2), 1–15. https://doi.org/10.7454/jts.v1i2.1007

Marizaldi, D., Husein, K., & Damayanti, A. (2025). Counterterrorism in the digital era: Strengthening Indonesian policies on addressing the lone-wolf threat and online radicalization. *International Journal of Social Science and Human Research, 8*(8), 5937–5947. https://doi.org/10.47191/ijsshr/v8-i8-24

Maysarah, M. M., Fakhreja, R., & Supriyadi, A. A. (2025). Social media as a catalyst for future terrorist recruitment: A bibliometric analysis of emerging trends and countermeasures. *Indonesian Journal of Counter Terrorism and National Security, 4*(2), 227–274. https://doi.org/10.15294/ijctns.v4i2.30287

Meleagrou-Hitchens, A., Alexander, A., & Kaderbhai, N. (2017). The impact of digital communications technology on radicalization and recruitment. *International Affairs, 93*(5), 1233–1249. https://doi.org/10.1093/ia/iix103

Oktavianus, J., & Davidson, B. (2023). Countering terrorism on social media: An analysis of online anti-terrorism movement in Indonesia. *Communication and the Public, 8*(4), 308–323. https://doi.org/10.1177/20570473231189898

Prindani, A., & Syauqillah, M. (2025). Digital pathways to radicalization: Step to terrorism with understanding social, psychological, and technological dimensions of terrorism in Indonesia. *Salud, Ciencia y Tecnología, 5*, Article 2365. https://doi.org/10.56294/saludcyt20252365

Putri, R. N. R. C., & Putranti, I. R. (2019). Efektivitas Kerja Sama PPATK dan AUSTRAC dalam Memberantas Tindak Pidana Pendanaan Terorisme di Indonesia Tahun 2014–2017. *Journal of International Relations Diponegoro, 5*(4), 636–645. https://doi.org/10.14710/jirud.v5i4.24911

Rahmadhani, P., Apriwan, & Setyaka, V. (2023). Perubahan Kebijakan Luar Negeri Amerika Serikat dalam Mengatasi Imigran Ilegal di Perbatasan dengan Meksiko. *Politics, Humanities, Laws, International Relations and Social Journal, 2*(2), 39–53. https://doi.org/10.25077/palito.2.2.39-53.2023

Rahmadhani, P., Perwita, A. A. B., & Ramsi, O. (2025). Building regional readiness: Indonesia's leadership in enhancing AHA Centre's disaster response capabilities. *International Journal of Humanities, Education, and Social Sciences, 3*(3), 907–928. https://doi.org/10.58578/ijhess.v3i3.6951

Riyanta, S. (2022). Shortcut to terrorism: Self-radicalization and lone-wolf terror acts: A case study of Indonesia. *Journal of Terrorism Studies, 4*(1). https://doi.org/10.7454/jts.v4i1.1043

Sabar, A., Meliala, A. E., & Mustofa, M. (2026). The propaganda of hyper-terrorism: Analyzing 516 cases of former terrorism convicts in Indonesia. In E. Aslan & K. Öktem (Eds.), *When faith kills: Understanding religious extremism* (pp. 201–220). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-50490-8_11

Sabrina, R. (2026). Fenomena Radikalisasi Digital di Indonesia dan Implikasinya terhadap Kebijakan Kontraterorisme di ASEAN. *Jurnal Ilmu Sosial dan Ilmu Politik, 7*(2), 406–426. https://doi.org/10.56552/jisipol.v7i2.326

Sugiyono. (2024). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Syamsurrijal, M., Nurmandi, A., Jubba, H., Hidayati, M., & Hariyanto, B. (2024). De-radicalization through social media: Social media literacy in countering terrorism in Indonesia. *Wawasan: Jurnal Ilmiah Agama dan Sosial Budaya, 9*(1), 1–12. https://doi.org/10.15575/jw.v9i1.16788

Umam, K., Aeni, R. Q., & Astuti, F. (2022). Counter narrative policy to handling radicalism in Indonesia. *Khazanah Sosial, 4*(4), 601–615. https://doi.org/10.15575/ks.v4i4.20202

Unlu, A., & Yilmaz, K. (2025). Online terrorism studies: Analysis of the literature. *Studies in Conflict & Terrorism, 48*(9), 1032–1055. https://doi.org/10.1080/1057610X.2022.2122108

Wibisono, A. A., Kumendong, R., & Maulana, I. (2025). Indonesia's handling of terrorists' cyber activities: How repressive measures still fall short. *Journal of Asian Security and International Affairs, 12*(1), 134–160. https://doi.org/10.1177/23477970241298764