

Legal Reform in Preventing Cyber Radicalism by Optimizing the Role of Social Media as a Means of Building National Defense Awareness among the Younger Generation

Maulana Al Qurthubi*, Albertus Wahyurudhanto, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; maulanaalqurthubi@gmail.com
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; wahyurudhanto@stik-ptik.ac.id
Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia; kif.92pw@gmail.com

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6307>

*Correspondence: Maulana Al Qurthubi
Email: maulanaalqurthubi@gmail.com

Received: 08/08/2026

Accepted: 24/08/2026

Published: 31/08/2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

Abstract: This study aims to examine the legal challenges in preventing cyber radicalism through social media among the younger generation and to propose legal reforms by optimizing social media as a tool to strengthen national defense awareness in the digital era. The development of information technology has shifted the pattern of radicalism from conventional forms to digital radicalism, which utilizes social media as a medium for spreading extreme ideological propaganda quickly, anonymously, and across national borders. This condition has led to various legal issues, including weak normative regulation of digital radicalism, limited penal approaches, inadequate supervision of social media platforms, and low levels of digital literacy and legal awareness among the younger generation. This study employs a normative juridical research method using both a statutory and conceptual approach, analyzing the 1945 Constitution of the Republic of Indonesia, the Electronic Information and Transactions Law, the Law on the Eradication of Criminal Acts of Terrorism, and relevant regulations on national defense and cybersecurity. The results indicate that policies to combat cyber radicalism in Indonesia are still repressive and have not been able to accommodate the development of digital ideological threats in a preventive and participatory manner. Therefore, legal reform is needed through strengthening social media regulations, developing an integrated digital

monitoring system, integrating national defense education and digital literacy, and developing a digital counter-narrative based on Pancasila values to shape a younger generation with national defense awareness and ideological resilience in the digital age.

Keywords: legal reform, cyber radicalism, social media, national defense, young generation.

Introduction

The development of information and communication technology in the digital era has given rise to a transformation in radicalism patterns from conventional forms to cyber-based radicalism, which is far more complex, massive, and difficult for the state to control. Radicalism no longer develops through physical meetings, closed forums, or conventional organizational networks, but rather through digital media that allows for the rapid, anonymous, cross-border spread of ideology and without clear territorial control (Susanti, 2020). The internet and social media have become strategic media for the dissemination of

extremist propaganda through various forms of digital content, such as short videos, podcasts, memes, live streaming, closed discussion forums, and recommendation algorithms that create ideological echo chambers. This phenomenon is exacerbated by the emergence of radical self-learning, the process by which individuals learn radical ideologies independently through digital content without the direct involvement of specific organizations (Darmawan et al., 2023). Legally, this threat is actually closely related to the provisions of Article 28J paragraph (2) of the 1945 Constitution of the Republic of Indonesia, which emphasizes that the implementation of the rights and freedoms of every person must be subject to restrictions stipulated by law for the sake of respecting the rights of others, morality, security, and public order in a democratic society. In addition, Article 30 paragraph (4) of the 1945 Constitution also emphasizes that the Indonesian National Police is tasked with protecting, serving, and enforcing the law to maintain domestic security. In positive law, Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism has indeed expanded the concept of preventing terrorism, but has not explicitly regulated the normative construction of digital radicalism and the monitoring mechanism for extreme ideologies in cyberspace (Sabiq et al., 2025). This normative vacuum creates legal issues because the development of cyber radicalism moves faster than the development of national regulations, often leaving the state in a reactive, rather than preventive, position.

On the other hand, the younger generation is the social group most vulnerable to digital radical infiltration due to their high level of social media use and their psychological state, which is still in the process of searching for identity, existence, and social recognition. The adaptive nature of the younger generation to digital technology makes them a prime target for radical groups' propaganda through emotional, ideological, and algorithm-based information manipulation approaches (Teresia Anin et al., 2025). According to various national reports, the majority of internet users in Indonesia are from the productive age group and young people who are highly active on TikTok, Instagram, YouTube, Telegram, and other social media platforms. This situation becomes a serious problem when not balanced with digital literacy, legal awareness, and the ability to think critically about digital content (Shafa Budiman et al., 2024). From a legal perspective, the state actually has a constitutional obligation to protect the younger generation from ideological threats that can damage the nation's integrity, as reflected in the state's objectives in the fourth paragraph of the Preamble to the 1945 Constitution, namely to protect the entire Indonesian nation and all of Indonesia's territory. In addition, Article 31 paragraph (3) of the 1945 Constitution emphasizes that the government strives for and organizes a national education system that increases faith, piety, and noble morals in order to enlighten the nation's life. However, in practice, the national education system has not been fully able to integrate anti-radicalism digital literacy as part of civic education and national defense. As a result, the younger generation tends to become the object of transnational ideological penetration that exploits weaknesses in digital literacy and low constitutional awareness in cyberspace (Huda & Putra, 2025).

In contemporary developments, social media can no longer be viewed solely as an instrument of communication and entertainment, but has evolved into an arena for ideological battles, identity politics, and the construction of public opinion. Social media

algorithms work by reinforcing user preferences through content personalization systems that can indirectly create social polarization and amplify the spread of extremist narratives. Radical groups exploit the fast, viral, and emotional nature of social media to build anti-state propaganda, intolerance, and hatred against certain groups. (Sari & Farkhatan Mardiyah, 2026) The spread of this ideology is carried out through increasingly sophisticated digital propaganda techniques and is difficult to detect because it is often packaged in the form of motivational content, religious studies, and heroic narratives that target the psychology of the younger generation. From the perspective of Indonesian positive law, regulations regarding the misuse of electronic media are regulated in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, specifically Article 28, which regulates the prohibition of the dissemination of information that incites hatred based on ethnicity, religion, race, and intergroup relations (Marpaung et al., 2024). However, these norms are still general in nature and do not specifically regulate the characteristics of digital radical propaganda that develops through global platform algorithms. Furthermore, oversight of digital platforms still faces jurisdictional challenges because most social media companies are transnational corporations subject to the legal systems of other countries. This situation demonstrates the limited capacity of national law to address the highly dynamic developments in global cyberspace.

The threat of cyber radicalism ultimately raises the urgency of strengthening national defense awareness as part of a non-military defense strategy to address digital ideological threats. In the digital era, the concept of national defense is no longer limited to the physical obligation to defend the country from military threats, but also includes citizens' capacity to maintain ideological resilience, national unity, and social stability in cyberspace (Muallifah & Fatwa Dinal Maula, 2022). It has a strong constitutional basis as stipulated in Article 27 paragraph (3) of the 1945 Constitution, which states that every citizen has the right and obligation to participate in national defense efforts, and Article 30 paragraph (1) of the 1945 Constitution, which affirms the rights and obligations of citizens to participate in national defense and security efforts. In this context, the younger generation must be positioned as a strategic subject in building national resilience based on digital citizenship by strengthening legal awareness, digital literacy, religious moderation, and constitutional nationalism. However, the current state policy paradigm still tends to position the younger generation as mere objects of supervision, rather than as strategic partners in building counter-narratives against digital radicalism. In fact, a repressive approach without strengthening collective awareness will only create false resilience and fail to address the ideological roots of the development of cyber radicalism itself (Makbull Rizki, 2022).

The problem is further complicated by the fact that legal regulations related to preventing radicalism on social media still exhibit various normative and institutional weaknesses. To date, there is no clear legal definition of digital radicalism in the national legal system, leading to multiple interpretations in the implementation of prevention policies. This lack of norms has implications for weak coordination between institutions such as the National Counterterrorism Agency (BNPT), the Ministry of Communication and Information Technology (Kominfo), the National Police, and educational institutions in building an integrated prevention system. Furthermore, the dominant legal approach still

focuses on penal policy through criminal prosecution after acts of terrorism or the dissemination of harmful content. However, the process of digital radicalization is often latent, gradual, and difficult to prove under criminal law before resulting in concrete action. This situation indicates a normative gap in the national legal system, as existing regulations are unable to address the process of ideological indoctrination in the digital space. In fact, provisions in the Terrorism Law focus more on acts of terrorism as a material offense, rather than on the process of forming digital radicalism as a preventative threat to national security. Furthermore, Kominfo regulations regarding cutting off access to negative content are also ineffective because the takedown mechanism often lags behind the speed of content dissemination on social media. These legal arguments demonstrate the urgent need for legal reform to build a prevention system that is more adaptive to developments in information technology and the threat of transnational ideology (Ahmad Shabirin & Arjun, 2025).

Based on these various issues, legal reform to prevent cyber radicalism is an urgent need to build a legal system that is not only repressive but also preventive, educational, and participatory. Legal reform must be directed at reconstructing national policies that integrate social media monitoring, strengthen digital literacy, protect the younger generation, and foster national defense awareness based on digital citizenship. The state needs to develop regulations that position digital platforms as legal subjects with an active responsibility to prevent the spread of extremist content, rather than merely passive service providers. Furthermore, the legal approach must be expanded through strengthening digital counter-narratives, technology-based citizenship education, and synergy between the government, educational institutions, civil society, and digital communities in building a healthy and democratic cyberspace. Philosophically, this legal reform aligns with the values of Pancasila, the state ideology, which places humanity, unity, and social justice as the foundations of national life. From a legal perspective, legal reform is a logical consequence of the state's obligation to protect citizens as mandated by the 1945 Constitution. Meanwhile, from a sociological perspective, the development of digital radicalism shows that threats to the state in the modern era are no longer in physical aggression, but ideological infiltration through cyberspace that targets the younger generation as a strategic group for the nation's future.

Methodology

This research employs a normative juridical research method that focuses on the study of legal norms, legal principles, synchronization of laws and regulations, and legal doctrines related to the prevention of cyber radicalism through the optimization of social media in building national defense awareness among the younger generation. The approaches used are the statute and the conceptual approaches. The statutory approach is carried out by examining various relevant regulations, including the 1945 Constitution of the Republic of Indonesia, Law Number 5 of 2018 concerning the Eradication of Criminal Acts of Terrorism, Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions, Law Number 3 of 2002 concerning National Defense, as well as various regulations and policies related to cyberspace supervision and the prevention of digital radicalism. Meanwhile, a conceptual approach is used to examine legal concepts regarding cyber radicalism, cyber security, digital citizenship, national

defense, digital literacy, national resilience, and legal reform theories as a basis for building legal arguments regarding the need for reconstruction of policies to prevent radicalism on social media. The legal materials used consist of primary legal materials from relevant laws and decisions, secondary legal materials from books, scientific journals, research results, and doctrines of legal experts, and tertiary legal materials from legal dictionaries and encyclopedias. The legal material collection technique is achieved through library research, then analyzed prescriptively and analytically using legal interpretation and legal argumentation methods to find the ideal concept of legal reform in preventing cyber radicalism that is adaptive, preventive, and based on strengthening national defense awareness in the digital era.

Result and Discussion

Legal Issues in Preventing Cyber Radicalism through Social Media for the Younger Generation

The development of information and communication technology has shifted the dissemination of radicalism from conventional methods to digital-based forms, or cyber radicalism, which uses social media as a primary instrument for spreading extreme ideologies. This phenomenon creates complex legal challenges, as cyberspace is borderless, allows anonymity, operates at high speed, and is difficult for the state to monitor effectively. Social media such as TikTok, Instagram, YouTube, Telegram, Facebook, and X have become a medium for spreading radical propaganda through videos, discussion forums, podcasts, memes, and even live broadcasts targeting young people as the primary target. From a constitutional perspective, the state has an obligation to protect the public from threats to national security as regulated in the fourth paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia, which emphasizes the state's goal to protect the entire Indonesian nation and all of Indonesia's territory. In addition, Article 28G paragraph (1) of the 1945 Constitution guarantees protection of a sense of security and self-protection from the threat of fear, while Article 30 paragraph (4) of the 1945 Constitution emphasizes the duty of the Republic of Indonesia National Police in maintaining public security and order. However, the development of cyber radicalism demonstrates that the national legal system is not yet fully capable of responding to the changing patterns of digital threats, which are evolving at a much faster rate than the development of regulations and state oversight capacity (Usrinase et al., 2025).

This legal problem is further complicated by the lack of a clear normative definition of digital radicalism within the national legal system. Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism regulates various forms of terrorist crimes, but it does not explicitly define the concept of cyber radicalism or provide indicators for the dissemination of extremist ideologies through social media. This lack of a legal framework creates legal uncertainty in the prevention and enforcement process, as law enforcement officials tend to act only when an act fulfilling the elements of a terrorist offense has occurred. Yet, the process of digital radicalization often occurs gradually through ideological indoctrination, the dissemination of narratives legitimizing violence, recruitment, and the manipulation of information, which

are not always immediately categorized as direct criminal offenses. In the context of modern criminal law, this situation demonstrates the weakness of criminal policy, which remains overly repressive. At the same time, the absence of a specific definition should not justify the criminalization of radical thoughts, unpopular opinions, religious beliefs, political criticism, or other forms of constitutionally protected expression. Therefore, the development of a legal framework for cyber radicalism must be based on the principle of legality and formulated with sufficiently clear and objective elements so that the scope of prohibited conduct remains predictable and does not extend to legitimate ideological expression (Tri Wibowo & Hadiningrat, 2023).

For the purpose of legal reform, cyber radicalism may therefore be operationally understood as the intentional use of digital systems, social media platforms, or other electronic communication technologies to disseminate, promote, facilitate, recruit for, or substantially support ideological narratives that directly encourage, justify, organize, or facilitate violence, terrorism, coercive attacks against constitutional order, or discriminatory attacks against individuals or groups. Such a definition should be applied cumulatively by considering the digital medium, the content and context of the communication, the existence of a demonstrable nexus to serious harm or violence, and the intent or functional role of the actor in promoting or facilitating such harm. Accordingly, the mere expression of political dissent, religious discussion, academic analysis, journalistic reporting, artistic expression, or controversial ideological opinions should not, by itself, constitute cyber radicalism. The proposed legal framework must therefore distinguish between protected expression, harmful or high-risk digital content requiring non-penal intervention, and conduct that has reached the threshold of criminal liability. Such differentiation is essential to ensure that preventive measures against cyber radicalism remain compatible with Article 28E paragraph (3) of the 1945 Constitution while allowing restrictions only where they are prescribed by law and justified by legitimate concerns relating to the rights of others, morality, security, and public order as reflected in Article 28J paragraph (2) of the 1945 Constitution.

On the other hand, the provisions regarding the misuse of electronic media in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions also fail to fully accommodate the characteristics of the spread of radicalism in the digital space. Article 28, paragraph (2) of the ITE Law only prohibits the dissemination of information intended to incite hatred or hostility based on ethnicity, religion, race, and intergroup relations (SARA), while digital radicalism propaganda is often conveyed in the form of ideological narratives that do not always explicitly address hate speech. In addition, the provisions of Article 40 paragraph (2a) and paragraph (2b) of the ITE Law, which authorize the government to terminate access to unlawful electronic information, also still face various implementation obstacles, especially related to the speed of content dissemination, the use of anonymous accounts, and the existence of digital platform servers outside Indonesian jurisdiction. This condition shows that national regulations still have limitations in dealing with the dynamics of global social media controlled by transnational corporations. In addition, digital content

monitoring mechanisms often give rise to debates regarding the protection of human rights, especially freedom of expression as guaranteed in Article 28E paragraph (3) of the 1945 Constitution) (Basrawi, 2025). Therefore, the state faces a legal dilemma between maintaining national security and still guaranteeing the constitutional rights of citizens in the digital space.

Legal issues are also evident in the weak coordination and synchronization of authority between state institutions in preventing cyber radicalism. Currently, handling digital radicalism involves various institutions such as the National Counterterrorism Agency (BNPT), the Ministry of Communication and Digital, the Indonesian National Police, the National Cyber and Crypto Agency (BSSN), as well as educational institutions and community organizations. However, the lack of a unified legal system has resulted in a sectorial and ineffective handling of cyber radicalism. For example, the Ministry of Communication and Digital's authority to monitor content, while criminal prosecution falls to the Police and BNPT. This situation often leads to overlapping authority and weak data integration, as well as a lack of a national strategy. In fact, Article 6 of Law Number 3 of 2002 concerning National Defense stipulates that national defense is implemented through a comprehensive defense system involving all citizens, territories, and national resources in an integrated and sustainable manner. Regarding digital threats, this provision should serve as the legal basis for establishing a national coordination system to address cyber radicalism as a non-military threat to national resilience. However, in reality, there is no regulatory design that specifically integrates cyber security approaches, national defense education, and social media monitoring within a single, comprehensive legal framework (Arianti & Farhana, 2025).

This condition demonstrates the need for a clearer legal design concerning the distribution and coordination of institutional authority in preventing cyber radicalism. Rather than concentrating all powers within a single institution, the legal reform should establish an integrated but functionally differentiated coordination framework. The National Counterterrorism Agency (BNPT) may serve as the primary policy coordinator responsible for formulating national prevention strategies, coordinating counter-radicalization policies, and integrating early-warning information related to ideological threats. The Ministry of Communication and Digital Affairs should primarily exercise regulatory and supervisory functions concerning platform compliance, content governance obligations, transparency reporting, and coordination with digital service providers. The National Cyber and Crypto Agency (BSSN) should focus on the technical and cybersecurity dimensions of the monitoring infrastructure, including the security, reliability, and risk assessment of digital monitoring systems. Meanwhile, the Indonesian National Police (Polri) should retain responsibility for criminal investigation and law enforcement once the identified conduct fulfils the statutory threshold of a criminal offense. Educational institutions and relevant ministries should complement this framework through preventive programs aimed at strengthening digital literacy, legal awareness, critical thinking, and democratic resilience among younger generations.

Such a distribution of authority would allow cyber radicalism to be addressed through a coordinated continuum consisting of prevention, platform governance, technical risk assessment, education, and criminal law enforcement, rather than through overlapping institutional interventions. However, the exchange and integration of information between institutions should remain subject to clear legal procedures, purpose limitation, data protection requirements, and accountability mechanisms. BNPT, as the policy coordinating authority, should therefore not automatically exercise unilateral powers over content removal, criminal investigation, or intrusive digital surveillance, which should remain within the legally defined competence of the respective institutions and be subject to the applicable oversight mechanisms. In this manner, institutional integration can be achieved without creating an excessive concentration of power or weakening the protection of fundamental rights.

The younger generation, as the dominant users of social media, is the group most vulnerable to radical ideological infiltration due to their high level of internet use, which is not matched by adequate digital literacy skills and legal awareness. Radical groups exploit the psychological state of the younger generation, who are still in the process of searching for identity, social recognition, and the need for existence, to carry out a gradual indoctrination process through emotional and persuasive digital content. From a constitutional perspective, the state has a responsibility to build the national character of the younger generation, as stipulated in Article 31 paragraph (3) of the 1945 Constitution, which stipulates that the government organizes a national education system to enhance faith, piety, and noble character to educate the nation. Furthermore, Article 27, paragraph (3) of the 1945 Constitution also emphasizes that every citizen has the right and obligation to participate in national defense efforts. However, the implementation of national defense and digital literacy education in Indonesia remains inadequate to address the challenges of the massive growth of cyber radicalism on social media. The national education curriculum tends to focus on a formalistic approach and fails to integrate the strengthening of digital legal awareness and critical skills in addressing extremist propaganda in cyberspace. As a result, the younger generation is more easily influenced by narratives of intolerance, anti-state sentiment, and transnational ideologies that are prevalent on social media (Wahyudi & Hadi, 2021).

The legal challenges in preventing cyber radicalism through social media demonstrate the urgent need for legal reforms that are more adaptive to the development of digital technology and the threat of transnational ideologies. Legal reforms are needed not only in the form of regulatory revisions but also through a reconstruction of the legal paradigm that prioritizes prevention over solely criminal prosecution. The state needs to develop regulations that explicitly regulate digital radicalism, strengthen the obligations of social media platforms to prevent the spread of extremist content, and integrate digital monitoring systems with the strengthening of legal literacy and national defense for the younger generation. Philosophically, these legal reforms implement the values of Pancasila, the foundation of the state, which upholds unity, humanity, and social justice. From a legal perspective, legal reform is a consequence of the state's obligation to guarantee national

security and protect citizens as mandated by the 1945 Constitution. Meanwhile, from a sociological perspective, the development of cyber radicalism shows that threats to the state in the modern era are no longer merely physical, but rather take the form of ideological infiltration through social media that systematically targets the younger generation as a strategic group for the nation's future.

Weaknesses of Penal Policies and Digital Surveillance in Combating Cyber Radicalism in Indonesia

Indonesia's current policy for combating cyber radicalism is still dominated by a penal approach, which focuses on legal action after a crime has occurred. This approach is incapable of addressing the rapid development of digital radicalism in cyberspace. This penal approach is evident in the dominant use of criminal law instruments in Law Number 5 of 2018 concerning Amendments to Law Number 15 of 2003 concerning the Eradication of Criminal Acts of Terrorism, which focuses on the prosecution of perpetrators of terrorism, recruitment of terrorist organization members, military training, and the dissemination of teachings related to terrorist acts. Although this regulation has broadened the concept of prevention, its implementation remains largely directed at repressive measures through arrest, detention, and criminalization. Cyber radicalism, however, essentially develops through a gradual process of ideological indoctrination through social media, digital forums, and online communities, which does not always immediately constitute a criminal offense. Consequently, law enforcement officials often only act after the radicalization process has developed into a real threat to national security. This situation indicates a delay in the legal system in addressing the early stages of the spread of digital radicalism. From a modern criminal policy perspective, an approach that places too much emphasis on penal policies without the support of non-penal policies results in countering radicalism being merely symptomatic and failing to address the root causes of ideological and social problems developing in digital society.

The weakness of this penal approach is also related to the anonymous nature of cyberspace, which crosses national borders and utilizes digital technology that is difficult for law enforcement to track. In practice, radical groups utilize anonymous accounts, encrypted applications like Telegram, virtual private networks (VPNs), and even foreign servers to spread extremist ideological propaganda and recruit new members without being easily detected by the state. Although Article 43A of Law Number 5 of 2018 authorizes law enforcement officials to prevent and monitor terrorism-related activities, in practice, authorities still face limitations in technology, digital forensic human resources, and international jurisdictional constraints. Furthermore, the provisions in Article 31 of Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law concerning interception or wiretapping are also not fully effective in addressing increasingly complex and encrypted digital communication patterns. Empirically, various cases demonstrate that the process of radicalizing young people through social media often goes undetected until the perpetrators are directly involved in terrorist networks or acts of violence. This demonstrates that Indonesia's digital surveillance

system remains reactive and lacks early detection of the development of extreme ideologies in cyberspace.

Another problem is the weak oversight of social media platforms, the primary medium for the spread of digital radicalism. Currently, social media platforms such as TikTok, Instagram, YouTube, Facebook, Telegram, and X have become strategic vehicles for the dissemination of radical propaganda through short videos, digital lectures, memes, podcasts, and even closed discussion forums targeting young people. Although Article 40 paragraphs (2a) and (2b) of the ITE Law authorizes the government to block access to electronic information containing unlawful content, the implementation of this policy still faces numerous empirical obstacles. Radical content often reappears through new accounts, spreads rapidly through repost features and social media algorithms, and evolves faster than the state's ability to block it. Furthermore, most social media platforms are transnational corporations whose servers and internal policies are located outside Indonesian jurisdiction, thus limiting state oversight. In practice, content takedowns are often delayed due to the need for reporting, verification, and coordination with digital platforms. This position demonstrates that national regulations lack sufficient coercive power over digital platforms to prevent the spread of radical content. Consequently, Indonesian cyberspace is highly vulnerable to exploitation by extremist groups to propagate anti-state ideologies systematically.

The weakness of digital surveillance policy is also evident in the lack of integrated coordination between state institutions in combating cyber radicalism. Currently, handling authority is spread across various institutions such as the National Counterterrorism Agency (BNPT), the Indonesian National Police (Polri), the National Cyber and Crypto Agency (BSSN), and the Ministry of Communication and Digital. However, in empirical practice, coordination between these institutions remains sectoral and not based on an integrated surveillance system. For example, data regarding the spread of radical content on social media is not always integrated in real time between the Ministry of Communication and Information, law enforcement officials, and intelligence agencies. On the other hand, the national cyber security approach also still focuses more on protecting digital infrastructure than monitoring the infiltration of extreme ideologies in cyberspace. This is despite Article 30 paragraphs (2) and (4) of the 1945 Constitution affirming that national defense and security efforts are implemented through a total people's defense and security system with the Indonesian National Police as a state instrument tasked with maintaining public security and order. Furthermore, Law Number 3 of 2002 concerning National Defense emphasizes that threats to the state are not limited to military threats but also non-military ones that can disrupt the nation's sovereignty and integrity. However, to date, there has been no specific regulation that comprehensively integrates a national digital surveillance system to address the threat of cyber radicalism as part of the non-military threats to national resilience.

Nevertheless, the strengthening of digital surveillance and content moderation mechanisms must not result in an overly broad system of censorship or the criminalization of constitutionally protected expression. The identification of radical or extremist content

should therefore not be based solely on keywords, religious symbols, political affiliations, ideological positions, or the controversial nature of an opinion. Rather, an objective and contextual assessment should be applied by considering the substance of the content, the intention of the communication, its target or audience, the surrounding context, and whether there is a sufficiently identifiable nexus between the expression and the encouragement, justification, recruitment, facilitation, organization, or substantial support of violence or terrorism. This approach is necessary to distinguish unlawful digital conduct from legitimate political criticism, religious discussion, academic analysis, journalistic reporting, artistic expression, and peaceful ideological advocacy. In this regard, digital monitoring should operate through a graduated response mechanism in which content presenting an identifiable risk may be subject to contextual assessment, reduced algorithmic amplification, warning measures, or human review, whereas criminal law enforcement should be reserved for conduct that clearly fulfils the statutory elements of a criminal offense. Such differentiation is essential to ensure that the expansion of digital surveillance remains consistent with the principles of legality, necessity, proportionality, and accountability, while preserving freedom of expression as guaranteed by the 1945 Constitution.

Empirically, the weaknesses of the penal and digital surveillance approaches have also led to the increased involvement of young people in digital radicalism networks. Numerous cases demonstrate that teenagers and students are exposed to extreme ideologies through social media, online forums, and digital content packaged in a persuasive and emotional manner. Radical groups exploit the weak digital literacy and low legal awareness of young people to systematically construct narratives of hatred, intolerance, and anti-government sentiment. In this context, a legal approach that relies solely on criminal prosecution is ineffective because the process of radicalization essentially develops through psychological and ideological manipulation, which is difficult to prove criminal in its early stages. Furthermore, state policy remains minimal in developing digital counter narratives and social media-based legal literacy education. Article 31, paragraph (3) of the 1945 Constitution stipulates that the government is obliged to implement a national education system that fosters faith, piety, and noble morals to educate the nation. However, in practice, national defense education and anti-radicalism digital literacy have not been optimally integrated into the national education system or national digital media policy. As a result, the younger generation is more easily influenced by extremist propaganda than by the national narrative developed by the state.

The weaknesses of penal policies and digital oversight in countering cyber radicalism in Indonesia demonstrate that the national legal system remains immature to the evolving threat of digital ideology in the information technology era. An overly repressive legal approach, weak oversight of digital platforms, a lack of integrated coordination between institutions, and low levels of public legal awareness have rendered countering cyber radicalism ineffective. Therefore, legal reform is needed that emphasizes not only penal policies but also integrates preventive, educational, participatory, and digital technology-based approaches. The state needs to develop more progressive regulations by

strengthening the obligations of social media platforms to prevent the spread of extremist content, establishing an integrated digital monitoring system, and expanding national defense and digital literacy education for the younger generation. Philosophically, these legal reforms implement the values of Pancasila in maintaining national unity and the resilience of the nation's ideology. Legally, these reforms are a consequence of the state's obligation to protect citizens, as mandated by the Preamble to the 1945 Constitution. Sociologically, the development of cyber radicalism demonstrates that threats to the state in the digital era are no longer limited to physical violence, but also ideological infiltration through social media, requiring a more adaptive, progressive legal system based on digital national resilience.

Legal Updates through Optimizing Social Media as a Means of Strengthening National Defense Awareness for the Younger Generation in the Digital Era

The increasingly massive development of cyber radicalism in the digital era demands legal reform that is no longer solely oriented towards a repressive approach, but also positions social media as a strategic instrument in building national defense awareness among the younger generation. Social media has been viewed more as a source of threat because it becomes a medium for spreading radicalism, intolerance, and anti-state ideology propaganda. However, from a progressive legal perspective, social media can be optimized as a tool for national education, enhancing digital literacy, and strengthening ideological resilience at the national level. This legal reform has a strong constitutional basis as stipulated in Article 27 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, which emphasizes that every citizen has the right and obligation to participate in national defense efforts. In addition, Article 30 paragraph (1) of the 1945 Constitution also states that every citizen has the right and obligation to participate in national defense and security efforts, while Article 31 paragraph (3) of the 1945 Constitution requires the government to organize a national education system that increases faith, piety, and noble character. These provisions provide the state with constitutional authority to develop a legal framework that incorporates social media into a non-military defense strategy by enhancing national defense awareness through digital citizenship. Consequently, legal reform should move away from a solely supervisory model toward a participatory approach that engages the younger generation as key actors in sustaining national resilience in the digital environment.

The first concrete step that needs to be taken is to reconstruct national regulations by incorporating the concept of digital radicalism and the obligation to strengthen national literacy in cyberspace into the national legal system. The government needs to revise the Electronic Information and Transactions Law and strengthen derivative regulations that specifically address the obligations of social media platforms to conduct early detection, rapid blocking, and monitoring of digital radical content. Furthermore, specific regulations need to be established regarding the protection of the younger generation from the infiltration of extremist ideologies on social media by strengthening digital content moderation systems. In this context, the state can require digital platforms to provide rapid reporting features for radical content, transparency in recommendation algorithms, and

active collaboration with law enforcement and educational institutions. Another concrete step is the establishment of a national cyber radicalism monitoring center integrated with the National Counterterrorism Agency (BNPT), the Indonesian National Police (Polri), the National Cyber and Crypto Agency (BSSN), and the Ministry of Communication and Digital to conduct artificial intelligence-based monitoring of the spread of extremist propaganda on social media. Thus, legal reform should not only produce formal norms but also build institutional mechanisms that adapt to developments in digital technology.

In addition to strengthening regulations, legal reform should also be directed at developing a digital-based national defense education system integrated into the national curriculum and social media. Currently, national defense education tends to be formalistic and has not been able to address the challenges of ideological infiltration in cyberspace. Therefore, the government needs to develop a national policy that mandates the integration of digital literacy, legal awareness, anti-radicalism, and digital citizenship education in the education system from elementary school through university. A concrete step that can be taken is the development of a social media-based digital national education platform that includes creative content on Pancasila, tolerance, religious moderation, and the dangers of cyber radicalism, with an approach relevant to the younger generation. The government also needs to partner with influencers, content creators, academics, religious figures, and digital communities to build a national counter-narrative movement against extremist propaganda. From a legal perspective, this policy implements Article 31 paragraph (5) of the 1945 Constitution, which affirms the government's obligation to advance science and technology while upholding religious values and national unity. Thus, social media serves not only as a communication space but also as a strategic instrument in building the ideological resilience of the younger generation.

The next concrete step is to strengthen the national digital surveillance and security system through a collaborative approach between the state, civil society, and global technology platforms. The government needs to establish regulations requiring social media companies to have representative offices and legal compliance centers in Indonesia to facilitate coordination of law enforcement against radical content. Furthermore, it is necessary to develop an early warning system based on big data and artificial intelligence capable of detecting patterns of radical propaganda distribution, extremist account networks, and ideological infiltration trends on social media in real time. The state also needs to establish an integrated cyber patrol involving law enforcement officers, digital forensic experts, and digital communities to actively monitor the national cyberspace. In practice, such oversight must adhere to the principles of the rule of law and the protection of human rights, as stipulated in Article 28J paragraph (2) of the 1945 Constitution, which emphasizes that restrictions on rights and freedoms may only be imposed in the interests of security, public order, and the morality of a democratic society. Therefore, legal reform must balance national security interests with the protection of freedom of expression in the digital space.

Furthermore, legal reform must also strengthen a non-penal approach through community empowerment and strengthening the participation of the younger generation

in building a healthy digital ecosystem. To date, policies to combat radicalism have tended to be top-down and state-dominated, resulting in suboptimal participation by digital citizens. Therefore, the government needs to establish a national "digital citizenship and national defense" program involving students, creative communities, youth organizations, and civil society as agents of counter-radicalism on social media. Concrete steps that can be taken include anti-radicalism creative content competitions, community-based digital literacy training, a national campaign for religious moderation on social media, and the formation of digital national defense ambassadors in educational settings and youth communities. Furthermore, the government needs to provide budgetary support and incentives for the production of positive content that promotes tolerance, nationalism, and national unity. This policy implements the concept of a comprehensive defense system as stipulated in Law Number 3 of 2002 concerning National Defense, which positions all citizens as part of the national defense system in the face of non-military threats.

Based on these various steps, legal reform through optimizing social media as a means of strengthening national defense awareness among the younger generation must be understood as a national strategy for building the nation's ideological resilience in the digital era. Legal reform is not sufficient only through the creation of new regulations, but must also be realized through the development of an integrated digital monitoring system, strengthening technology-based national education, active involvement of the digital community, and strengthening the responsibility of social media platforms in safeguarding national cyberspace. Philosophically, this legal reform is an implementation of the values of Pancasila in maintaining national unity and sovereignty from transnational ideological threats. Legally, this reform is an implementation of the constitutional mandate to protect citizens and maintain national resilience as stipulated in the 1945 Constitution. Meanwhile, sociologically, the development of information technology has shifted the pattern of threats to the state from physical threats to digital threats based on ideological infiltration through social media. Therefore, the state must build a legal system that is progressive, adaptive, and based on public participation so that social media does not become a space for the development of cyber radicalism, but rather becomes a strategic tool in shaping a young generation with a strong awareness of national defense, digital literacy, and a commitment to nationalism.

Conclusion

The investigation shows that the development of cyber radicalism in the digital era has given rise to a new form of threat to national resilience, utilizing social media as a means of disseminating extremist ideological propaganda to the younger generation. The transformation of radicalism from conventional to digital patterns has caused the national legal system to face various problems, both in terms of regulation, digital oversight, and the still predominantly repressive approach to countermeasures. Legal weaknesses are evident in the absence of clear normative regulations regarding digital radicalism, weak oversight of social media platforms, the lack of integrated coordination between state institutions, and the limitations of the penal approach in addressing the process of ideological indoctrination that occurs latently and systematically in cyberspace. On the other hand, the younger

generation is the group most vulnerable to exposure to digital radicalism due to the high intensity of social media use that is not balanced by digital literacy, legal awareness, and the ability to think critically about extremist propaganda. Therefore, legal reform is an urgent need by shifting the paradigm of countering radicalism from a repressive approach to a preventive, educational, participatory, and digital national resilience-based approach. Optimizing social media as a means of strengthening national defense awareness among the younger generation must be positioned as a national strategy to build the nation's ideological resilience through the integration of digital regulations, national education, digital literacy, counter-extremist narratives, and strengthening the responsibility of social media platforms in safeguarding the national cyberspace.

Based on the findings, it is recommended that the government immediately implement legal reforms by revising and harmonizing various regulations related to preventing cyber radicalism, particularly the Electronic Information and Transactions Law and national policies regarding social media monitoring and digital security. The state needs to establish specific regulations regarding digital radicalism that outline normative definitions, oversight mechanisms, digital platform obligations, and an early detection system for the spread of extremist propaganda in cyberspace. Furthermore, the government needs to establish an integrated digital monitoring system based on artificial intelligence technology, involving the National Counterterrorism Agency (BNPT), the Indonesian National Police (Polri), the National Cyber and Crypto Agency (BKSDA), and the Ministry of Communication and Digital Affairs within a unified national coordination system. In terms of education, strengthening digital literacy, national defense education, and legal awareness based on digital citizenship is needed, integrated into the national education curriculum and developed through social media with the involvement of influencers, academics, creative communities, and civil society organizations. The government also needs to encourage the development of a massive digital counter-narrative movement through the production of creative content that promotes the values of Pancasila, tolerance, religious moderation, and national unity so that social media does not become a space for the spread of radicalism, but rather becomes a strategic tool in shaping a young generation with nationalism, a sense of national defense, and strong ideological resilience in the digital era.

References

- Ahmad Shabirin, & Arjun. (2025). Asas Legalitas dalam Penanggulangan Radikalisme Online: Perspektif Hukum Pidana Indonesia. *Jejak Digital: Jurnal Ilmiah Multidisiplin*, 1(3), 333–344. <https://doi.org/10.63822/czsz4m55>
- Arianti, F. M., & Farhana. (2025). Upaya Penanggulangan Penyebaran Paham Radikal Terorisme Melalui Media Sosial: Platform Facebook. *The Juris*, 9(2), 519–526. <https://doi.org/10.56301/juris.v9i2.1727>
- Basrawi, B. (2025). Jejak Digital Menuju Ekstremisme: Fenomena Radikalisasi dalam Lingkungan Pendidikan. *Biomatika Jurnal Ilmiah Fakultas Keguruan Dan Ilmu Pendidikan*, 11(2), 129. <https://doi.org/10.35569/biomatika.v11i2.2226>
- Darmawan, B., Wijaya, I. P., & Alhuzaini, M. (2023). Radikalisme dan Intoleransi terhadap Generasi Muda dalam Memanfaatkan Teknologi Era Globalisasi di Indonesia. *At-Tajdid : Journal of Islamic Studies*, 3(2), 53. <https://doi.org/10.24014/at-tajdid.v3i2.25512>

- Huda, M. D., & Putra, A. G. P. (2025). Strategi pencegahan terorisme melalui pendidikan karakter dan literasi digital di kalangan remaja. *Jurnal Riset Multidisiplin Edukasi*, 2(12), 462–474.
- Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, 14(1), 54–62. <https://doi.org/10.32734/politeia.v14i1.6351>
- Marpaung, S., Purwanto, Bakara, I. W., & Muhayan. (2024). Tantangan Masyarakat dalam Memahami dan Menggunakan Media Elektronik yang Bijak Sesuai Dengan UU ITE. *Jurnal Kolaboratif Sains*, 7(1), 460–466. <https://jurnal.unismuhpalu.ac.id/index.php/JKS>
- Muallifah, & Fatwa Dinal Maula, H. (2022). Perempuan dan Radikalisme di Media Siber: Strategi Pendidikan Kontra-Radikalisme Terhadap Perempuan dalam Media Harakatussalam. *Jurnal Kajian Islam Interdisipliner*, 7(2), 59–80. <https://doi.org/10.14421/jkii.v7i2.1330>
- Sabiq, M., Iskandar, I., Burhanuddin, A., & Arisnawawi, A. (2025). Transformasi Perilaku Kelompok Radikal ke Moderat di Era Digital. *Equilibrium: Jurnal Pendidikan*, 13(1), 96–108. <https://doi.org/10.26618/equilibrium.v13i1.17188>
- Sari, A., & Farkhatun Mardiyah, T. (2026). Tinjauan Teoretis Pendidikan Karakter Moderat sebagai Instrumen Preventif Radikalisme Online di Era Digital. *Jurnal Pendidikan Agama Islam (JURPAI)*, 2(1), 32–37.
- Shafa Budiman, A., Gracia Tumimomor, E., Ekklesia Anastasia Saragih, D., & Parhusip, J. (2024). Analisis Proporsi Pengguna Internet Berdasarkan Karakteristik Sosial Ekonomi Di Indonesia. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 9(1), 374–377. <https://doi.org/10.36040/jati.v9i1.12304>
- Susanti, E. (2020). Sosialisasi Membangun Literasi Karakter Berbasis Pancasila di Era Digital 4.0 dalam Upaya Pencegahan Radikalisme dan Terorisme pada Remaja. *Jurnal Sumbangsih*, 1(1), 9–18. <https://doi.org/10.23960/jsh.v1i1.3>
- Teresia Anin, Anjulin Yonathan Kamlasi, Fredik Lambertus Kollo, Triyanti Gloria Dubu, Eroi Marten Selan, & Dedi Riwu. (2025). Peran Media Sosial dalam Mencegah Bahaya Radikalisme di Kalangan Generasi Muda. *Jurnal Pendidikan Ips*, 15(4), 1469–1476. <https://doi.org/10.37630/jpi.v15i4.3667>
- Tri Wibowo, K., & Hadiningrat, W. (2023). Penanggulangan Penyebaran Radikalisme Melalui Media Sosial dalam Hukum Pidana Indonesia. *Jurnal Hukum Lex Generalis*, 4(2), 187–212. <https://doi.org/10.56370/jhlg.v4i2.304>
- Ushrinas, Y., Rusmana, I. P. E., Darma, I. M. W., & Antari, P. E. D. (2025). Implementasi Asas Legalitas dalam Penegakan Hukum terhadap Tindak Pidana Radikalisme Digital yang Berimplikasi pada Terorisme. *Perahu (Penerangan Hukum): Jurnal Ilmu Hukum*, 13(2), 140–150. <https://doi.org/10.51826/perahu.v13i2.1705>
- Wahyudi, S. T., & Hadi, S. (2021). Pengoptimalan Peran Penggiat Media Sosial Dalam Manangkal Radikalisme Di Dunia Maya. *Esensi Hukum*, 3(2), 134–143. <https://doi.org/10.35586/esensihukum.v3i2.101>