International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 08 Issue 08 August 2025

DOI: 10.47191/ijsshr/v8-i8-24, Impact factor- 8.007

Page No: 5937-5947

Counterterrorism in the Digital Era: Strengthening Indonesian Policies on Addressing the Lone-Wolf Threat and Online Radicalization

Deki Marizaldi[1], Kresnawan Husein[2], Angel Damayanti[3]

[1,2]Doctoral Program in Police Science, STIK LEMDIKLAT POLRI, Jakarta, Indonesia

[3]Professor of International Security, Faculty of Social and Political Sciences, Universitas Kristen Indonesia, Jakarta, Indonesia

ABSTRACT: The advancement of information technology has given rise to contemporary terrorism threats, such as the lone-wolf phenomenon and online radicalization. These threats are decentralized and challenging to detect, posing a significant security challenge for Indonesia. This study aims to analyze Indonesia's counterterrorism policy in addressing these issues by employing qualitative approaches and case study methods. It discusses Indonesia's strategies by referencing practices from the United States, the United Kingdom, and Australia. The findings reveal that although Indonesia has made progress in legal and institutional frameworks, it still faces major challenges in managing digital information and coordinating between agencies. Unlike other countries that adopt a holistic preventive approach, Indonesia needs to enhance its prevention strategies through community engagement and the utilization of technology for early detection. This research recommends strengthening digital intelligence capabilities, expanding international cooperation, and developing more effective communication strategies to bolster national resilience against terrorism in the digital age.

KEYWORDS: Digital threats, Indonesia, counterterrorism, *lone-wolf*, online radicalization.

I. INTRODUCTION

The rapid development of information and communication technology (ICT) has profoundly transformed the global landscape, ushering in a digital era that presents both opportunities and challenges. This transformation significantly impacts national and international security, particularly in the context of terrorism, which continues to evolve. Today, terrorist groups utilize digital platforms to spread extreme ideologies, recruit members, raise funds, and plan attacks, creating an increasingly complex and chaotic environment (Briggs & Feve, 2019). The digital age enables the rapid and widespread dissemination of terrorist propaganda, with social media, online forums, and instant messaging apps serving as primary tools for spreading violent narratives, influencing potential recruits, and inspiring acts of terrorism. The ease of access to information and anonymity in cyberspace exacerbate this situation (Jones & Smith, 2018).

One of the main challenges is the emergence of lone wolves—individuals who commit acts of terrorism independently and are often inspired by online propaganda. These lone-wolf perpetrators are challenging to detect because they lack direct ties to specific terrorist groups. Online radicalization serves as a significant trigger for these individuals, exposing them to extreme content and encouraging acts of violence (Miller, 2019). This form of radicalization also accelerates the recruitment and indoctrination processes of terrorists. By leveraging digital platforms, terrorist groups can reach wider audiences, disseminate propaganda, and establish support networks, enabling individuals to become terrorists in a relatively short period (Neumann, 2013).

The threat of lone wolves, driven by online radicalization, has become a global phenomenon. A prominent international example is the 2019 terror attack in Christchurch, New Zealand, perpetrated by Brenton Tarrant (BBC, 2019). He live-streamed his actions on social media and was heavily influenced by white supremacist propaganda accessed through online forums. A similar phenomenon has occurred in Indonesia, evidenced by attacks such as the one carried out by Zakiah Aini at the National Police Headquarters in 2021 (Kompas, 2021), and the suicide bombing at the Makassar Cathedral Church in the same year. Both perpetrators had no direct command relationship with a major terrorist organization but were radicalized through the internet and acted on their own initiative.

Indonesia, home to the largest Muslim population in the world and with extensive experience dealing with terrorism, is one of the countries most affected by the lone-wolf threat and online radicalization. Notable terrorist attacks, including the Bali bombings in 2002, prompted the government to implement decisive counterterrorism measures (ICG, 2021). However, with the rising threat of lone wolves and increasingly sophisticated online radicalization, existing counterterrorism policies must be evaluated and adjusted. This study aims to analyze Indonesia's counterterrorism policy in addressing these threats, drawing on policies

implemented in other countries, and provide recommendations for enhancing the effectiveness of these policies (National Agency for Countering Terrorism, 2020).

Building on the background provided, this study aims to address the following key questions:

1. How can Indonesia's counterterrorism policy be enhanced to effectively tackle the threats posed by lone-wolf attackers and online radicalization in the digital age?
2. In what ways can Indonesia learn from the counterterrorism strategies implemented by other countries facing similar challenges?
3. How can the effectiveness of Indonesia's counterterrorism measures be assessed in terms of preventing and responding to the threats of lone-wolf attacks and online radicalization?
4. What potential challenges and opportunities can Indonesia leverage in its counterterrorism efforts in the context of the digital era?

To address the research questions, this study uses a qualitative approach, specifically employing a case study method. The qualitative approach was selected because it allows researchers to explore Indonesia's counterterrorism policy in depth and gain a comprehensive understanding of the complexities surrounding the lone-wolf threat and online radicalization. The case study method provides an opportunity to closely examine various aspects of policies, strategies, and their implementation in practice (Yin, 2018).

The data sources for this study include:

1. Government Documents: This includes policies, laws, regulations, reports, and official documents from government agencies related to counterterrorism, such as the National Counterterrorism Agency (BNPT), the Coordinating Ministry for Political, Legal, and Security Affairs and other relevant institutions.
2. Public Documents: This category encompasses news articles, research reports, academic publications, and other publicly available resources pertinent to the research topic.

The data collection techniques employed in this study are document and content analysis. Document analysis is used to identify existing counterterrorism policies, strategies, and programs, as well as to assess their implementation and effectiveness. Content analysis is utilized to examine online content, including terrorist propaganda, social media posts, and online forums, to better understand the dynamics of online radicalization.

II. THEORETICAL FRAMEWORK

A. Lone-wolves and Terrorism in the Digital Age

The development of digital technology has significantly transformed the operations of terrorism, presenting new challenges for counterterrorism efforts. The internet and social media have become highly effective tools for terrorist groups to disseminate extremist ideologies, recruit new members, raise funds, and plan attacks (Briggs & Feve, 2019; Jones & Smith, 2018). The digital age has created an environment where terrorists can operate more efficiently, anonymously, and on a global scale, complicating detection and enforcement efforts (Weimann, 2014).

Social media platforms such as Facebook, Twitter, and Telegram are frequently used to promote radical ideologies, incite violence, and encourage individuals to commit acts of terrorism. Additionally, social media algorithms play a crucial role in amplifying the spread of extremist content, fostering an "echo chamber" where users are exposed only to views that reinforce their existing beliefs, ultimately accelerating the radicalization process (Zannettou et al., 2018).

Furthermore, terrorist groups utilize the internet for covert communication, attack planning, and gathering information about potential targets. The dark web provides an anonymous platform for terrorists to interact, share information, and engage in illicit activities without detection (Finklea, 2017). The increasing use of encryption and other anonymous technologies makes it more challenging for law enforcement to track terrorist activities online, thereby complicating intelligence and law enforcement efforts to address these threats (Rid, 2015).

The threat posed by lone wolves has become a significant focus in counterterrorism efforts in the digital age, largely due to the challenges in detecting and preventing their attacks. A lone wolf is an individual who engages in terrorism without any direct affiliation to a terrorist group, often operating independently or with minimal support from others (Miller, 2019). Since they leave few conventional traces, intelligence agencies and law enforcement find it particularly difficult to monitor their activities.

Key characteristics of lone wolves include:

1. Strong Ideological Motivations: Lone wolves are typically driven by extremist ideologies, such as white supremacy, Islamic radicalization, or anti-government sentiments, which they acquire through extensive exposure to online content (Gill et al., 2017).
2. Dependence on the Internet: The internet serves as a crucial tool for the radicalization of lone wolves, providing access to extremist propaganda, bomb-making guides, and online forums that facilitate ideological exchange and attack planning (Conway, 2017).

3. Lack of Formal Affiliation with Terrorist Groups: Lone wolves are not directly connected to any specific terrorist organization, making them difficult to track and prevent using conventional methods. They often plan their attacks independently and in secrecy, relying on the information they gather online (Gruenewald & Horgan, 2017).
4. Simple Planning and High Autonomy: Lone wolves typically plan relatively simple attacks, such as those involving firearms or small-scale bombs, using readily available information from the internet to assemble explosives or acquire weapons. Their high degree of autonomy complicates efforts to intervene (Alberts & Gjelstad, 2019).

The isolated nature of lone wolf threats, coupled with the abruptness of their actions, makes them challenging to detect and prevent. Addressing this threat requires a counterterrorism approach focused on early detection, increased surveillance in cyberspace, and intervention for individuals showing signs of radicalization (RAND Corporation, 2020).

B. Online Radicalization

Online radicalization is a complex process where individuals become exposed to extremist ideologies through the internet and social media. This exposure can lead them to adopt radical views and engage in acts of terrorism (McCauley & Moskalenko, 2017). Various personal, social, and ideological factors influence this process, which is further accelerated by the unparalleled access to information and communication in the digital world.

The role of the internet and social media in online radicalization is critical. Digital platforms provide immediate access to extremist content, forums, and communities that actively support radical ideologies. Through these channels, individuals can easily find information, connect with like-minded groups, and strengthen their beliefs without direct contact with terrorist organizations (Berger, 2016). Furthermore, social media algorithms often intensify the radicalization process by creating "echo chambers" that expose users only to information that reinforces their existing views (Zannettou et al., 2018).

Several key factors drive online radicalization:

1. Exposure to Extremist Content: Individuals are frequently confronted with extremist material through various online channels, including videos, articles, and social media posts. This content is often crafted to provoke strong emotions, spread hatred, and legitimizes violence.
2. Interactions with Extremist Communities: Engaging with online communities that promote radical ideologies provides individuals with the social support and validation they seek, deepening their beliefs and speeding up the radicalization process (Doosje et al., 2016).
3. Search for Identity and Meaning: Those who feel alienated or lack purpose in life often seek identity within extremist ideologies. This pursuit offers a compelling sense of belonging and purpose, particularly appealing to vulnerable individuals (Hogg & Abrams, 1988).
4. Involvement in Extreme Online Activities: Individuals often engage in a range of extreme online activities, including spreading propaganda, recruiting new members, and planning attacks. This engagement accelerates radicalization and encourages direct involvement in acts of terrorism (Sageman, 2004).

Online radicalization presents a formidable challenge to counterterrorism efforts. Therefore, law enforcement and intelligence agencies must adopt proactive strategies to monitor online activities, identify individuals at risk, and prevent the radicalization process. Additionally, community engagement and educational initiatives must be fortified to effectively address this issue (Lakhani, 2018).

C. Counter-Terrorism Policies

Counterterrorism refers to a comprehensive set of strategies, tactics, and actions designed to prevent and counter terrorism. This approach encompasses various aspects, including law enforcement, intelligence gathering, and social, economic, and ideological considerations. The focus of counterterrorism extends beyond merely arresting and prosecuting perpetrators; it also aims to address the root causes of terrorism and prevent the process of radicalization (Hoffman, 2006). This multidimensional approach requires cooperation among various sectors and institutions to achieve overarching goals, which include prevention, action, response, and mitigation (United Nations, 2006).

Some key elements of counterterrorism are as follows:

1. Prevention: This involves efforts to stop terrorism before it occurs, including early detection, surveillance, and counter-radicalization strategies (United Nations, 2006). Prevention often incorporates community-based approaches, education, and deradicalization programs aimed at reducing the risk of individuals being exposed to extremist ideologies (Silke, 2004).
2. Deterrence: These measures aim to prevent terrorists from launching attacks through law enforcement, punishment, and military action (Cronin, 2009). The goal of enforcement is to create a deterrent effect and ensure that perpetrators of terrorism are held accountable for their actions (Bueno de Mesquita, 2005).
3. Response: This refers to the measures taken in response to terrorist attacks, including crisis management, evacuation procedures, and the provision of medical assistance (Clarke, 2005). A prompt and effective response can help mitigate the impact of an attack and provide relief to the victims.

4. Mitigation: These actions aim to reduce the impact of terrorist attacks, including infrastructure protection and enhanced community preparedness (National Research Council, 2002). The goal of mitigation is to minimize the damage and losses caused by terrorist acts (Reich, 1998).

Various countries have developed counterterrorism policies to address the threat of terrorism, including issues related to lone-wolf attacks and online radicalization. The strategies employed vary depending on each country's political, social, and cultural context. However, certain best practices can serve as lessons for other nations (Byman, 2015).

1. United States: The United States has a long history of responding to terrorism, particularly since the 9/11 attacks. Its counterterrorism policy involves stringent law enforcement, extensive intelligence gathering, and military intervention abroad. In the digital space, the US focuses on monitoring online activities, enforcing laws against extremist content, and collaborating with technology companies to tackle digital threats (United States Department of Homeland Security, 2021).
2. United Kingdom: The UK implements a counterterrorism strategy known as CONTEST, which consists of four main pillars: Pursue (targeting terrorists), Prevent (addressing radicalization), Protect (safeguarding society), and Prepare (preparing for potential attacks). The UK places significant emphasis on preventing radicalization through deradicalization programs, education, and collaboration with local communities (HM Government, 2023).
3. Australia: Australia adopts a comprehensive approach to counterterrorism, encompassing law enforcement, intelligence gathering, and international cooperation. The country actively works to prevent online radicalization through educational programs, public awareness campaigns, and partnerships with technology companies. Additionally, Australia has strict regulations to manage the circulation of extremist content online (Australian Government, 2022).

From the above explanation, we can perceive that all three countries have established strict laws to counter terrorism, but their approaches differ. The US tends to emphasize aggressive law enforcement, whereas the UK prioritizes a balanced approach between enforcement and prevention. Furthermore, the UK and Australia offer more comprehensive programs for preventing radicalization than the US. These programs involve community collaboration, education, and deradicalization initiatives. All three nations also emphasise the importance of international cooperation in counterterrorism efforts, including the sharing of intelligence, cross-border law enforcement, and collaboration aimed at preventing online radicalisation.

III. RESULTS & DISCUSSION

A. An Analysis of Indonesia's Counterterrorism Policy

Analysis of Indonesia's counterterrorism policy reveals a significant and structured evolution, particularly in response to various terrorist attacks since the Bali bombings in 2002. The Indonesian government has gradually built a policy framework that focuses on not only repressive measures but also preventive and rehabilitative efforts. Key steps include strengthening the legal framework, establishing a special coordinating agency, implementing a deradicalization program, and enhancing international cooperation. This multifaceted approach addresses the complexity of the evolving terrorist threat, including new challenges in the digital age such as the lone-wolf phenomenon and online radicalization.

The foundation of Indonesia's current counterterrorism policy is a legal framework that has been substantially enhanced. A pivotal moment in this strengthening was the ratification of Law Number 5 of 2018, which amends Law Number 15 of 2003 concerning the Eradication of Terrorism Crimes. This amendment significantly impacts law enforcement officials by granting them broader authority to arrest, detain, and prosecute individuals involved in terrorist activities. With this law, actions can be taken at an earlier stage, not just after a terrorist act has occurred, but also during the preparation or planning stages.

Structurally, the National Counter-Terrorism Agency (BNPT) plays a crucial role in coordinating various efforts to combat terrorism in Indonesia. BNPT has a specific mandate as the primary coordinator for all programs and policies related to counter-terrorism in the country. Its responsibilities encompass developing national strategies and overseeing the implementation of programs across various ministries and agencies (National Counter-Terrorism Agency, n.d.). Additionally, BNPT conducts regular evaluations to assess the effectiveness of the policies that have been implemented, ensuring that every action taken remains relevant to the ever-changing landscape of threats (Kevin Akbar, 2020; Rachmawati, 2021).

At the implementation level, the law enforcement approach is one of the main pillars actively executed. This effort involves a series of actions, including the arrest, prosecution, and detention of terrorists. To enhance its effectiveness, the government continually seeks to improve intelligence capabilities and strengthen the law enforcement system. This capacity-building initiative explicitly aims to enhance early threat detection and prevent terrorist attacks before they occur, which is crucial in addressing increasingly concealed threats such as lone-wolf attacks.

In addition to the hard approach, Indonesia integrates deradicalization programs as a vital component of its counterterrorism policy. These programs aim to change the views and ideologies of extremist individuals, particularly terrorism prisoners and former terrorists. By transforming their mindset, the program seeks to prevent these individuals from reconnecting with terrorist networks and engaging in acts of terrorism in the future. The overarching goal is to break the cycle of violence and radicalism at the individual level.

The approach taken in the deradicalization program is multifaceted, featuring a range of targeted interventions. These efforts consist of comprehensive counseling sessions that explore both psychological and ideological factors, the delivery of balanced educational materials both national and religious and the organization of vocational training opportunities (National Counter-Terrorism Agency, n.d.; Akbar, 2020; Rachmawati, 2021). All these activities share a common goal: facilitating the reintegration process of former perpetrators of terrorism, enabling them to be accepted and function normally in society once again.

Indonesia's approach to fighting terrorism goes beyond its borders, supported by vibrant international collaboration. The government actively forges partnerships with different countries and global organizations in the fight against cross-border terrorism. This cooperation manifests in several ways, such as sharing crucial intelligence information, conducting joint training exercises to strengthen law enforcement capabilities, and providing technical support in various fields (National Counter-Terrorism Agency, n.d.; Akbar, 2020; Rachmawati, 2021). Through these holistic efforts, which blend prevention, law enforcement, and international cooperation, Indonesia aims to build a strong and well-rounded counter-terrorism system.

B. Best Practices from Other Countries

This section discusses the counterterrorism policies of several countries, including the United States, the United Kingdom, and Australia, offering valuable insights. This analysis helps identify best practices that have been effective elsewhere while also highlighting areas where Indonesia's policies still need improvement and strengthening. It covers various important dimensions, from general law enforcement approaches to the design of strategies for preventing radicalization and the models of international cooperation that are in place.

Table 1. Counterterrorism Policy Comparison Matrix

Comparative Aspects	Indonesia	United States	United Kingdom	Australia
Key Approaches	A combination of law enforcement and deradicalization.	Focus on law enforcement, intelligence, and the military.	Holistic through the CONTEST (Pursue, Prevent, Protect, Prepare) strategy.	A balanced approach between law enforcement and prevention.
Prevention of Radicalization	A combination of deradicalization program inside and outside the prison, but need more comprehensive approaches.	Limited, more focused on early detection and intervention.	Very comprehensive, involving community, education, and programs	*Prevent*. Comprehensive, including education, public campaigns, and collaborations with technology companies.
Digital Content Handling	Monitoring and enforcement, however, still face the challenge of effectiveness.	Close cooperation with technology companies for law enforcement.	Comprehensive strategies to protect against harmful content, part of the pillars	*Protect*. Strict laws that specifically regulate online extremist content.
International Cooperation	It is active, but needs to be strengthened in real-time intelligence sharing.	The cooperation network is extensive, becoming a leader in global intelligence sharing.	Strong cooperation, especially with European countries and the "Five Eyes" alliance.	Solid, focusing on cooperation in the Asia-Pacific region.

Source: *Official Documents of the State Government Processed by the Authors (*Republik Indonesia, 2018; United States America, 2001, Gov UK, 2023; Australian Government, 2025).

Based on the description of the table above, the United States, particularly after the 9/11 attacks, adopted an approach focused heavily on aggressive law enforcement, large-scale intelligence gathering, and military action. Its top priority is to prevent terrorist attacks at home and protect its citizens abroad. Legal frameworks, such as the Patriot Act, grant law enforcement agencies broad powers to conduct surveillance and make arrests. While this approach has advantages, including superior intelligence capabilities and decisive law enforcement actions, it also has drawbacks. It places a more limited emphasis on preventing radicalization at the community level and tends to rely more on security approaches.

In contrast, the United Kingdom has adopted a more holistic and balanced strategy known as CONTEST. This strategy is built on four main pillars: (1). Pursue (targeting terrorists); (2). Prevent (preventing radicalization); (3). Protect (safeguarding citizens) and (4). Prepare (preparing for the impact of an attack). A key strength of the UK approach lies in the Prevent pillar, which heavily involves collaboration with local communities, educational institutions, and deradicalization programs to address the root causes of

radicalization. The comprehensive nature of this strategy is its strength; however, it faces challenges in balancing national security needs with the protection of civil liberties.

Australia also employs a balanced and comprehensive approach that combines law enforcement, radicalization prevention, and international cooperation. One of Australia's key focuses is on preventing online radicalization, which is addressed through educational programs, public awareness campaigns, and close collaboration with technology companies. Additionally, Australia has a stringent legal framework to regulate and combat the spread of extremist content online. The strength of Australia's approach lies in its emphasis on digital threats, though it faces challenges in striking a balance between security and freedom of expression.

As in the case of Indonesia, its law enforcement policies are relatively strong and align with those of the three countries mentioned. However, Indonesia faces the challenge of continuing to strengthen its intelligence and law enforcement capabilities, particularly in detecting and preventing attacks planned by lone-wolf perpetrators, which are difficult to trace. The ability to identify individuals who radicalize online is an area that requires ongoing improvement.

In terms of radicalisation prevention, Indonesia already has a deradicalization program, but can learn significantly from the models implemented by the United Kingdom and Australia. Both countries have successfully developed more comprehensive prevention programs that actively involve communities and educational institutions and implement evidence-based approaches. Indonesia's development of prevention programs needs to become more proactive and engage a broader range of stakeholders beyond the security apparatus to foster community resilience at the grassroots level.

Regarding international cooperation, Indonesia has actively established partnerships, but this collaboration needs to be further strengthened. Specifically, improvements are necessary in the speed and quality of intelligence information exchange and technical cooperation to combat online radicalization, which knows no national borders. By adopting best practices from other countries, particularly in developing comprehensive prevention programs and enhancing digital intelligence cooperation, Indonesia can significantly improve the effectiveness of its counterterrorism policies.

C. Policy Effectiveness in Addressing Lone-Wolf and Online Radicalization

Evaluating the effectiveness of Indonesia's counterterrorism policy necessitates a critical analysis that goes beyond mere normative descriptions, focusing instead on data-driven arguments at the practical level. In the context of lone-wolf threats and online radicalization, this evaluation can be structured around three main pillars: *the effectiveness of law enforcement*, *the success of countering digital content*, and *the actual impact of deradicalization program*s.

1. **Law Enforcement Effectiveness: The Paradox Between Arrests and Early Detection Failures**
   The government often highlights impressive arrest statistics as a measure of its success in law enforcement. For example, the Special Detachment (Densus) 88 of the Indonesian National Police announced that they arrested 142 terrorists in 2023, 149 in 2022, 370 in 2021, and 232 in 2020 (Kompas, 2023; Kompas, 2022).While these figures quantitatively demonstrate the capacity of law enforcement to crack down on terrorist networks and individuals, this argument weakens when considering the continued occurrence of significant lone-wolf attacks that often evade early detection. The case of Zakiah Aini's attack on the National Police Headquarters in 2021 serves as a clear illustration of this failure, where an individual radicalized online managed to infiltrate one of the most critical security facilities in Indonesia (Detiknews, 2021). This vulnerability highlights that while repressive enforcement is vigorous, the preventive aspect focusing on individuals acting independently remains a critical weak point.
2. **Countering Online Radicalization: The War of Attrition Against Digital Content**
   The effectiveness of addressing online radicalization presents a rather ambiguous picture. When viewed quantitatively, the government's efforts seem substantial. For example, in 2024, the National Counterterrorism Agency (BNPT) and the Ministry of Communication and Digital (Komdigi) successfully blocked 180,954 pieces of content related to intolerance, radicalism, extremism, and terrorism on the internet. Much of this blocked content originated from terrorist groups like ISIS, HTI, and JAD, which actively propagate violent ideologies through digital channels (BNPT, 2024). This figure reflects significant efforts to eliminate extremist propaganda from the cyber realm. However, the argument regarding the effectiveness of these blocks diminishes due to the rapid and widespread nature of such content. Terrorist groups can readily reproduce and disseminate material through alternative platforms, particularly encrypted messaging apps like Telegram. This results in a "war of attrition," where the government remains primarily reactive. Its effectiveness is limited, as it addresses only visible content while failing to disrupt the production chain and the dissemination of narratives within closed online communities.
3. **Deradicalization Programs: The Challenge of Measuring Ideological Transformation**
   Deradicalization programs are an essential component of Indonesia's counterterrorism strategy; however, evaluating their effectiveness poses a considerable challenge. Although the government often boasts about achieving high success rates, there is a noticeable lack of trustworthy quantitative data indicating a steady decrease in recidivism rates among former militants. Real-world examples underscore this difficulty. For instance, the recidivism case in Pacitan, where two individuals threatened to bomb the Pacitan Police Headquarters in East Java, is not an isolated incident in Indonesia. In

2023, the National Counterterrorism Agency (BNPT) disclosed that out of 1,036 former terrorist inmates, 116 returned to crime, translating to roughly 11 percent of these individuals re-offending (RM.id Rakyat Merdeka, 2025). This indicates that existing programs have not entirely succeeded in permanently altering extremist ideologies. The success of these programs should not only be measured by inmate participation but also through long-term quantitative data indicating what percentage of participants abandon extreme ideologies and do not revert to violence. Without such data, claims regarding the effectiveness of deradicalization programs remain largely normative and lack a robust evidence base.

The explanation above highlights a central argument: Indonesia has successfully established a robust policy framework, but it continues to face significant challenges in effectively implementing it in the digital age. Comparisons with countries like the UK and Australia indicate that Indonesia needs to shift its focus from law enforcement and post-incident deradicalization to a more comprehensive and data-driven preventive approach.

Several key findings support this argument. First, the reliance on repressive measures, as demonstrated by the high number of arrests, has proven inadequate in addressing the lone-wolf threat. This issue necessitates intelligence capabilities that not only track networks but also conduct behavioral analysis and trend monitoring in cyberspace to identify at-risk individuals before they take action. Second, efforts to "cleanse" the internet of radical content are inherently reactive and can never be entirely comprehensive. Although the data showing the blocking of tens of thousands of items by Ministry of Communication and Digital (Komdigi) indicates seriousness (BNPT, 2024), it is analogous to drawing water from a leaking boat. A more effective strategy would involve significantly reallocating resources to develop intelligent counter-narrative initiatives and flooding the digital space with positive narratives about tolerance and national identity. Additionally, enhancing people's digital literacy will help make them more resistant to propaganda.

Third, the effectiveness of deradicalization programs should be assessed based on clear quantitative evidence rather than simply reporting on their implementation. The issue of radicalization within correctional facilities demonstrates that existing programs are not optimal. There is a need for transparent data on recidivism rates and periodic evaluations involving independent experts to determine whether these programs are genuinely changing perceptions or merely encouraging temporary compliance. Without this data, funding for deradicalization initiatives risks becoming inefficient.

Therefore, this discussion argues that, to be truly effective in the digital age, Indonesia's counterterrorism policy must evolve. Crucial steps include shifting the focus from enforcement to prevention, from content blocking to counter-narrative development, and from merely implementing programs to conducting quantitative data-driven evaluations of their impact. These changes should be prioritized and implemented without delay.

D. Challenges and Opportunities

Indonesia undeniably faces critical and well-documented challenges, as well as significant strategic opportunities, in its counterterrorism efforts in the digital age. These challenges are as follows:

1. Limitations of Intelligence in Lone-Wolf Detection. The inadequacy of conventional intelligence methods to address lone-wolf attackers has already resulted in devastating consequences. The attack executed by Zakiah Aini at the National Police Headquarters in 2021 starkly illustrates this issue (Detiknews, 2021). This incident exemplifies how individuals radicalized independently through online content can evade detection, allowing them to strike vital national targets. It is clear that traditional intelligence approaches, which rely heavily on tracking structured networks, are insufficient to confront independent perpetrators lacking formal affiliations with terrorist organizations.
2. Suboptimal Inter-Institutional Coordination. The lack of effective coordination among government agencies is evident in the execution of counter-narrative and deradicalization programs. Overlapping initiatives among the BNPT, the Ministry of Religious Affairs, the Ministry of Communication and Informatics, and other entities lead to fragmented efforts and a lack of a cohesive communication strategy. While Kominfo focuses on content blocking (upstream) and BNPT oversees deradicalization (downstream), the absence of systematic feedback between the two undermines overall effectiveness. Consequently, the initiatives are piecemeal and fail to produce the comprehensive impact required for meaningful progress.
3. Reactive Digital Information Management. The management of digital information is critically reactive, as evidenced by the ongoing "war of attrition" between authorities and propagandists. When social media accounts or groups, such as those on Facebook, are shut down, they frequently resurface within hours under new identities or migrate to more secure platforms like Telegram. This situation highlights that mere blocking strategies are woefully inadequate to contain the swift and pervasive spread of ideologies in cyberspace.
4. Advanced Radicalization in Correctional Institutions. Radicalization within prisons represents a serious and pressing challenge, as demonstrated by recurring cases of recidivism where terrorism offenders are re-arrested for new terrorist activities. This alarming trend, often referred to as "schools of terrorism" in prisons, reveals that current deradicalization programs have failed to fundamentally alter the ideologies of these prisoners or sever their connections with extremist networks during incarceration.

There are several key opportunities that can also be seized:

1. Increased International Cooperation. This opportunity is not merely theoretical; it is already being realized and delivering tangible results. A prime example is the robust collaboration between Densus 88 Anti-Terror Police and the Australian Federal Police (AFP), established during the Bali I bombing investigation (Operation Alliance, 2019). This partnership continues to expand, including intelligence sharing on foreign terrorist fighters (FTF) and joint training in digital forensics. The successful dismantling of various terror networks in Indonesia clearly demonstrates that bolstering international cooperation significantly enhances counterterrorism effectiveness.
2. Technology Development and Utilization. The potential for leveraging technology for early detection is both concrete and actionable. For instance, the BNPT and intelligence agencies must develop integrated data analysis dashboards that harness Artificial Intelligence (AI) and Machine Learning (ML) technologies. Such systems can process vast amounts of data from social media, effectively map the spread of narratives, identify key influencers within extremist networks, and detect behavioral anomalies indicative of the radicalization process. This technological implementation will fundamentally shift the approach from reactive to predictive. (BNPT, 2016).
3. Structured Civil Society Engagement. There are substantial opportunities to engage actively with communities, as evidenced by successful implementations. A notable illustration is the establishment of the Terrorism Prevention Coordination Forum (FKPT) by the BNPT in 34 provinces. (BNPT, 2022) Through FKPT, the government systematically involves community leaders, academics, religious leaders, and youth organizations in dialogue programs, seminars, and counter-radicalism campaigns. The existence of FKPT is a testament to the critical role of civil society in bolstering community resilience against extremist ideologies.
4. Strengthening Evidence-Based Deradicalization Programs. Enhancing deradicalization programs is essential and can be achieved by adopting methods proven effective in practice. A concrete example of this enhancement is the implementation of more personalized and sustainable social reintegration programs. These programs should provide psychological assistance not only to ex-convicts but also to their families, along with economic support such as business capital or skills training tailored to labor market demands. This comprehensive approach is far more effective in preventing recidivism than merely delivering ideological lectures.

From the above explanation, this study firmly advocates for several essential strategies to enhance counterterrorism effectiveness in Indonesia:

1. Intelligence and Law Enforcement Capacity Building:
   - Enhancing intelligence capacity by increasing the counterterrorism intelligence budget by 15% over the next three years, focusing on training high-quality human resources and digital analysis (BNPT, 2020; RAND Corporation, 2020); establishing an integrated intelligence data analysis center with advanced AI and ML technologies to monitor online activities and conduct predictive analyses (Jones & Smith, 2018; Weimann, 2014); strengthening intelligence cooperation with countries like the U.S., U.K., and Australia through information exchange and joint training (U.S. Department of State, 2023).
   - Law Enforcement by revising Law Number 5 of 2018 to better define terrorism, expanding the scope of online radicalization offenses, and grant law enforcement clearer authority to address these issues (ICG, 2021); enhancing training for law enforcement on digital forensics, cyber intelligence, and handling online evidence (Briggs & Feve, 2019); establishing specialized units in police and prosecutors' offices for digital-age terrorism cases.
2. Strengthening Radicalization Prevention:
   - Implement comprehensive radicalization prevention programs involving communities, religious organizations, and social media platforms (HM Government, 2023). Increase funding for these programs by 20% over the next three years, ensuring they are evidence-based and regularly evaluated (Australian Institute of Criminology, 2020).
   - Build partnerships with civil society organizations fighting radicalization, ensuring their active involvement in prevention efforts.
   - Countering online radicalization through collaboration closely with social media platforms to monitor and remove extremist content, and block promoting accounts (Zannettou et al., 2018). Develop strategies to counter extremist narratives and enhance digital literacy among the public to combat terrorist propaganda (UNESCO, 2019).
3. Strengthening the Deradicalization Program:
   - Conduct regular evaluations of deradicalization programs using indicators like recurrence rates, changes in extremist views, and success in social reintegration (BNPT, 2016). Adjust programs based on evaluation results, including modifications to counselling methods and educational curricula (Silke, 2004).
   - Enhance facilitator training in areas such as terrorism psychology, counselling, and communication skills (Horgan, 2009). Offer better counselling, psychological support, and rehabilitation services for ex-terrorists and their families. Develop

effective social reintegration programs, including skills training, financial aid, and support for employment and social relationships (Hossain, 2013).

4. Increased International Cooperation:
   - Strengthen mechanisms for secure and efficient information exchange between countries (Department of Foreign Affairs and Trade, 2021) and create a unified intelligence-sharing platform.
   - Enhance cross-border cooperation to arrest and prosecute terrorists (U.S. Department of State, 2023) and develop extradition treaties and legal cooperation with partners.
   - Collaborate with social media platforms to counter online radicalization by sharing extremist content and enforcing policies (Zannettou et al., 2018) and engage in international forums to strategize against radicalization.
5. Role of Technology:
   - Early Detection by implementing AI and big data systems to identify signs of radicalization (Jones & Smith, 2018).
   - Develop tools to analyze intelligence data and predict terrorism patterns (Weimann, 2014). Improve digital forensics for electronic evidence analysis (Briggs & Feve, 2019).

CONCLUSIONS

This study demonstrates that Indonesia has made significant progress in its counterterrorism efforts. These advancements include strengthening the legal framework, enhancing intelligence capabilities, implementing deradicalization programs, and fostering international cooperation However, the complexities of terrorism in the digital age, marked by the unpredictable emergence of lone wolves and the rapid spread of online radicalization, require a more adaptive and comprehensive approach.

Best practices from other countries, such as the United States, the United Kingdom, and Australia, offer valuable insights for improvement. For instance, the UK and Australia employ a more holistic strategy for preventing radicalization, which involves close collaboration with civil society, educational initiatives, and evidence-based programs (This approach highlights the importance of addressing the root causes of radicalization and building community resilience against extremist ideologies. In contrast, the United States places a greater emphasis on law enforcement and intelligence, which are also critical components of counterterrorism. However, this focus may be less effective in preventing radicalization at the individual level.

The policy recommendations outlined in this study highlight the need for a comprehensive approach that integrates robust law enforcement, effective radicalization prevention efforts, sustainable deradicalization programs, enhanced international cooperation, and strategic use of technology. Building intelligence capacity, including the development of AI and machine learning-based data analysis tools, is vital for the early detection of terrorist threats. Furthermore, strengthening radicalization prevention programs through the engagement of civil society, religious leaders, and community leaders is essential for building resilience against extremist ideologies.

Implementing these recommendations necessitates a strong commitment from the government, collaboration across various agencies, and support from civil society. By adopting a comprehensive and sustainable approach and continuously adapting to technological advancements and evolving terrorist threats, Indonesia can enhance its national resilience to terrorism in the digital age and ensure the security and welfare of its communities. The study also underscores the importance of regularly evaluating the effectiveness of counterterrorism policies to ensure that initiatives have a meaningful and lasting impact.

REFERENCES

1) Akbar, K. (2020). *Peran BNPT dalam penanggulangan radikal terorisme*. E-Jurnal UMBIMA. Accessed from https://ejurnal.umbima.ac.id/index.php/jurnalhukum/article/view/188.
2) Australian Government. (2022). *Counter-Terrorism Strategy*.
3) Australian Government. (2025). *Australia's Counter-Terrorism Strategies*. http://nationalsecurity.gov.au/what-australia-is-doing/a-national-approach/australias-counter-terrorism-strategies.
4) Australian Institute of Criminology. (2020). *Preventing violent extremism: A guide for practitioners*
5) Badan Nasional Penanggulangan Terorisme (BNPT). (2016). *Evaluasi Program Deradikalisasi*.
6) Badan Nasional Penanggulangan Terorisme (BNPT). (2019). *Undang-Undang Nomor 5 Tahun 2018: Analisis dan Implikasi*.
7) Badan Nasional Penanggulangan Terorisme (BNPT). (2020). *Strategi Nasional Penanggulangan Terorisme*
8) Badan Nasional Penanggulangan Terorisme (BNPT). (n.d.). *Tugas pokok dan fungsi*. accessed from https://www.bnpt.go.id/tupoksi, on June 29, 2025.
9) BBC, 2020, https://www.bbc.com/indonesia/dunia-53885031, accessed on June 29, 2025.
10) Berger, J. M. (2016). *Extremism*. MIT Press.
11) BNPT, 2024, https://www.bnpt.go.id/bnpt-180-ribu-konten-bermuatan-terorisme-diblokir-sepanjang-2024 accessed on June 29, 2025.

12) BNPT, 2025, https://www.bnpt.go.id/presidential-lecture-bnpt-2022-tanggulangi-terorisme-melalui-sinergisitas-seluruh-elemen-bangsa accessed on June 29, 2025.
13) Kemhan, 2025, https://www.kemhan.go.id/balitbang/2025/03/20/pemanfaatan-ai-artificial-intelligence-di-bidang-militer.html accessed on June 29, 2025.
14) Briggs, R., & Feve, S. (2019). *The digital age and terrorism: A new landscape*. Routledge.
15) Byman, D. (2015). *The dynamics of counterterrorism*. Oxford University Press.
16) Clarke, R. (2005). *Defeating the jihadists: A blueprint for action*. Brookings Institution Press.
17) Conway, M. (2017). "Terrorism and the internet: The state of research." *Perspectives on Terrorism*, 11(3), 1-18.
18) Creswell, J. W., & Plano Clark, V. L. (2017). *Designing and conducting mixed methods research*. Sage publications.
19) Cronin, A. K. (2009). *Ending terrorism: Lessons for defeating al-Qaeda*. Oxford University Press.
20) Department of Foreign Affairs and Trade. (2021). *Australia's counter-terrorism cooperation*.
21) Detiknews, 2021, https://news.detik.com/berita/d-5519366/serangan-zakiah-aini-ke-mabes-polri-dan-isi-wasiat-yang-bikin-gempar, accessed on June 29, 2025.
22) Doosje, B., Moghaddam, F. M., & Kruglanski, A. W. (2016). *The psychology of radicalization*. Routledge.
23) Finklea, K. M. (2017). *The dark web: Overview and issues for Congress*. Congressional Research Service.
24) Gill, P., Corner, E., & Thornton, A. (2017). "Lone-actor terrorism: A typology." *Terrorism and Political Violence*, 29(4), 597-616.
25) Gov UK. (2023). *Counter-terrorism strategy (CONTEST) 2023*. https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023
26) Gruenewald, J., & Horgan, J. (2017). *The psychology of lone-actor terrorism*. Oxford Research Encyclopedia of Criminology and Criminal Justice.
27) Hillyard, P., & Tombs, S. (2004). *Beyond criminology: An introduction to critical criminology*. Pluto Press.
28) HM Government. (2023). *CONTEST: The United Kingdom's strategy for countering terrorism*.
29) Hoffman, B. (2006). *Inside terrorism*. Columbia University Press.
30) Hogg, M. A., & Abrams, D. (1988). *Social identifications: A social psychology of intergroup relations and group processes*. Routledge.
31) Home Office. (2021). *The Prevent duty: Departmental guidance*.
32) Horgan, J. (2009). "Walking the line: The psychological health of terrorists." *Terrorism and Political Violence*, 21(2), 249-269.
33) Hossain, M. (2013). "Rehabilitating former militants: Lessons from Bangladesh." *Journal of Strategic Studies*,36(5), 740-764.
34) ICG. (2021). *Indonesia: Counter-Terrorism and the Digital Realm*. International Crisis Group.
35) Jones, S. G., & Smith, H. (2018). *The internet and terrorism: Assessing the threat*. RAND Corporation. (
36) Kemenko Polhukam. (2022). *Laporan Tahunan Kerjasama Kontraterorisme*.
37) Kompas, 2021, https://www.kompas.tv/klik360/160336/kronologi-lengkap-aksi-penembakan-di-mabes-polri-oleh-terduga-teroris-zakiah-aini accessed on June 29, 2025.
38) Kompas, 2022, https://nasional.kompas.com/read/2022/03/21/17030661/sudah-tangkap-56-teroris-hingga-maret-2022-densus-88-terorisme-masih-ada accessed on June 29, 2025.
39) Kompas, 2023, https://nasional.kompas.com/read/2023/12/20/16412601/sepanjang-2023-densus-88-at-polri-tangkap-142-tersangka-terorisme accessed on June 29, 2025.
40) Lakhani, A. (2018). *Counter-terrorism and community engagement*. Palgrave Macmillan.
41) McCauley, C., & Moskalenko, S. (2017). *Mechanisms of political radicalization: Pathways toward terrorism*. Oxford University Press.
42) Miller, A. (2019). *Countering lone-wolf terrorism*. Georgetown University Press.
43) National Counterterrorism Center. (2021). *Strategic plan for countering terrorism*.
44) National Research Council. (2002). *Making the nation safer: The role of science and technology in countering terrorism*. National Academies Press.
45) Neumann, P. R. (2013). *Radicalization in the digital age*. International Centre for the Study of Radicalisation
46) Operation Alliance, https://www.70yearsindonesiaaustralia.com/kerja-sama-antara-australia-dan-indonesia/operation-alliance-nab5z, accessed on June 29, 2025.
47) Press Release, 2019. https://pressrelease.kontan.co.id/release/kominfo-blokir-11803-konten-radikalisme-dan-terorisme, accessed on June 29, 2025.
48) Rachmawati, D. (2021). *Analisis peran BNPT dalam pemberantasan terorisme di Indonesia*. E-Journal Undip. Accessed from https://ejournal2.undip.ac.id/index.php/jphi/article/view/7215.
49) Reich, W. (1998). *Securing the homeland: The role of the social sciences*. Cambridge University Press.

50) Republik Indonesia, 2018, Perubahan Atas Undang-Undang Nomor 15 Tahun 2003 Tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2002 Tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang, Pub. L. No. 5 (2018).
51) Rid, T. (2015). *Terrorism and the internet*. Columbia University Press.
52) RM.id Rakyat Merdeka, 2025. https://rm.id/baca-berita/nasional/273390/mantan-napi-terorisme-jadi-teroris-lagi-kriminolog-ui-analisis-penyebabnya accessed on July 19, 2025.
53) Sageman, M. (2004). *Understanding terror networks*. University of Pennsylvania Press.
54) Silke, A. (2004). *Psychological perspectives on terrorism*. Routledge.
55) U.S. Department of Justice. (2022). *The Patriot Act*.
56) U.S. Department of State. (2023). *Country Reports on Terrorism.*
57) UNESCO. (2019). *Media and Information Literacy for countering disinformation*.
58) United States America. (2001). *H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*. https://www.congress.gov/bill/107th-congress/house-bill/3162
59) Weimann, G. (2014). *New terrorism: The internet as a means of international terrorism*. Routledge.
60) Winterbotham, E. (2018). *Countering online radicalisation*. Palgrave Macmillan.
61) Yin, R. K. (2018). *Case study research and applications: Design and methods*. Sage publications.
62) Zannettou, S., Caulfield, T., & Blackburn, J. (2018). *The spread of extremist content on social media*. arXiv preprint arXiv:1809.08582.