Formosa Journal of Science and Technology (FJST)
Vol. 5, No. 7, 2026: 1805-1824

Family Apathy, Cyber Engagement, and Self-Radicalization in Lone Wolf Terrorism in Indonesia

Setyo Hermawan[1]*, Dhedi Ardi Putra[2], Supardi Hamid[3]
Sekolah Tinggi Ilmu Kepolisian
Corresponding Author: Setyo Hermawan, setyohermawan@stik-ptik.ac.id

A R T I C L E I N F O
Keywords: Family Apathy, Cyber Engagement, Self-Radicalization, Lone Wolf Terrorism, Significance Quest, Terrorism Prevention.

Received: 27, May
Revised: 29, June
Accepted: 25, July

A B S T R A C T
This article examines the relationship between family apathy, cyber engagement, and self-radicalization in the escalation of lone wolf terrorism in Indonesia. It highlights the shift of terrorist threats toward more fluid, individualized, and decentralized forms, positioning the family as an upstream factor influencing vulnerability or resilience to extremist propaganda. The study uses a qualitative multiple-case study design based on secondary data, including academic literature, policy documents, institutional reports, and relevant case narratives. The analysis applies concepts of lone wolf terrorism, self-radicalization, cyber engagement, family apathy, the staircase to terrorism theory, significance quest theory, and shortcut to terrorism. Findings indicate that family apathy does not directly cause terrorism but generates psychological vulnerabilities such as alienation, identity crisis, and the search for personal significance. These vulnerabilities are exploited through digital spaces that accelerate self-radicalization. The study proposes a family apathy–cyber engagement–lone wolf escalation model and recommends family-based prevention strategies

ISSN-E: 2964-6804
DOI: https://doi.org/10.55927/fjst.v5i7.110
https://journalfjst.my.id/index.php/fjst

INTRODUCTION

Terrorism nowadays no longer shows its identity directly through organized actions in one group or network. Instead, it reflects fundamental changes in threat patterns, actors, radicalization mediums, and violent mechanisms. In the early post-September 11, 2001 period, terrorism studies and counter-terrorism policies primarily focused on hierarchical organizations such as Al-Qaeda and Jemaah Islamiyah that operated through structured command systems, funding networks, and coordinated recruitment. However, in the last decade, terrorism has increasingly shifted toward more fluid, individualized, decentralized, and difficult-to-detect forms. One of the most significant manifestations of this transformation is the rise of lone wolf terrorism, where individuals carry out attacks independently while still being influenced by broader ideological ecosystems and online extremist propaganda.

This transformation presents serious challenges for state security systems. Lone wolf perpetrators often do not maintain clear communication with formal terrorist organizations, making traditional intelligence approaches less effective. Unlike structured networks that can be mapped through leadership hierarchies, funding flows, and logistical connections, lone actors often undergo covert radicalization through personal interaction with digital content, online communities, and algorithm-driven extremist narratives. Consequently, detection becomes increasingly limited because radicalization occurs in private digital environments that are largely inaccessible to external monitoring, particularly when it takes place in personal devices and isolated social spaces. Hegghammer (2013) emphasizes that violent behavior in jihadist movements cannot be generalized, as radicalization pathways vary depending on psychological and situational factors rather than organizational affiliation alone.

In Indonesia, the evolution of terrorism reflects similar patterns, where individuals are increasingly exposed to extremist narratives through digital platforms without direct organizational involvement. Several cases of attacks on symbolic targets demonstrate that perpetrators may emerge without formal training, structured recruitment, or direct allegiance to known terrorist groups. Instead, the process is characterized by self-radicalization, in which individuals construct ideological beliefs through online exposure, identity exploration, and internal justification of violence. In this context, digital space becomes more than a communication tool; it functions as a psychological and ideological environment that shapes identity formation, emotional reinforcement, and moral justification for violent action. De Bie et al. (2015) argue that technological development and geopolitical shifts significantly influence extremist behavior, accelerating radicalization from physical interaction-based processes to fast, individualized digital pathways.

Moghaddam (2005) conceptualizes radicalization through the staircase to terrorism model, which explains gradual psychological progression from perceived injustice to violent action. However, the emergence of digital environments modifies this linear progression by accelerating transitions between stages. Online platforms provide immediate access to narratives that justify anger, communities that validate alienation, and ideological content that

reinforces extremist beliefs. As a result, cyber engagement functions not merely as a medium but as an accelerative mechanism that shortens the psychological distance between grievance and violent readiness. In this process, digital ecosystems do not create vulnerability from zero but amplify pre-existing psychosocial conditions embedded in individual life experiences.

One critical psychosocial factor in this process is family apathy or dysfunction. The family is often positioned ambiguously in terrorism studies, as it can serve both as a protective environment and a potential enabling factor. Hafez (2016) notes that family relationships may contribute to radical socialization by providing emotional validation and reinforcing ideological commitment. However, families can also function as the earliest preventive institution when they provide emotional attachment, supervision, communication, and behavioral monitoring. In this study, family apathy is not limited to lack of attention but is understood as a failure in emotional bonding, communication patterns, digital supervision, and identity support systems within the household.

The link between family apathy and radicalization becomes more critical when viewed through the lens of psychological motivation. Kruglanski et al. (2014) highlight that the search for personal significance is a central driver of extremist behavior. Individuals who experience humiliation, social rejection, or lack of recognition are more likely to seek alternative pathways to restore meaning and identity. In conditions of family apathy, this psychological need often remains unmet within the domestic environment, making individuals more vulnerable to external ideological influences. Digital spaces then provide compensatory mechanisms through extremist narratives that offer belonging, heroism, and moral certainty. Thus, cyber engagement becomes a channel through which unmet emotional needs are redirected into ideological radicalization.

Despite extensive literature on lone wolf terrorism, existing studies still tend to emphasize ideological exposure, organizational disengagement, or technological factors without sufficiently addressing the interaction between family dysfunction and digital radicalization pathways. This creates a conceptual gap in explaining why individuals exposed to similar online environments exhibit different levels of vulnerability to extremist narratives. The present article addresses this gap by arguing that radicalization cannot be understood solely as exposure to extremist content but must also consider underlying psychosocial vulnerabilities. In this framework, family apathy operates as a push factor that creates identity instability, while cyber engagement functions as a pull factor that accelerates ideological consolidation and behavioral readiness toward lone wolf terrorism.

This gap carries both academic and policy implications. Academically, it integrates three previously separated domains: family sociology, psychological theories of radicalization, and digital security studies. Each contributes a distinct analytical layer in understanding how vulnerability, meaning-making processes, and technological environments interact in shaping extremist pathways. Policy-wise, current counter-terrorism strategies in Indonesia remain heavily focused

on law enforcement and post-incident deradicalization, which are insufficient for addressing pre-emptive radicalization among lone actors. Therefore, preventive strategies must expand to include family-based interventions such as digital literacy, psychoeducation, early behavioral detection, and structured communication within households as part of a comprehensive counter-radicalization framework.

THEORETICAL REVIEW

Konsep Lone Wolf Terrorism

The concept of lone wolf terrorism is used to describe forms of terrorism that are carried out by individuals independently, without direct involvement in the hierarchical command structure of terror organizations. In this article, lone wolf terrorism is not understood as an act completely independent of the ideological environment, but rather as a form of violence committed by individuals acting alone but still influenced by narratives, symbols, propaganda, and the broader ecosystem of extremism. Thus, the term "lone wolf" does not mean that the perpetrator is completely socially or ideologically isolated, but suggests that operational decisions, target selection, and execution of actions are more done individually. Hegghammer (2013) shows that some militants choose to attack within the country after going through a certain radicalization process, so that the choice of violent action cannot be explained only through group affiliation or conflict location.

This concept is relevant to read the dynamics of terrorism in Indonesia because a number of actions or action plans show symptoms of individualization of violence. Individuals do not always have to be part of an established organizational structure to adopt extreme ideologies. He has enough access to propaganda, experiences an identity crisis, obtains ideological validation, and forms a belief that violence is a legitimate act. Within this framework, lone wolf terrorism is positioned as the final output of the process of personal radicalization strengthened by the digital space.

Konsep Self-Radicalization

Self-radicalization refers to the process by which individuals experience a relatively independent change in beliefs, attitudes, and action orientation towards violent extremism. This process does not mean that individuals are completely free from outside influences, but that influence is more acquired through personal searches, digital content consumption, informal communication, or symbolic identification with extreme narratives. In this model, individuals are not always recruited directly by organizational actors. He can recruit himself through intensive engagement with narratives that justify violence.

Theoretically, self-radicalization is concerned with the process of searching for identity, the need for meaning, and the narrowing of moral choices. Moghaddam (2005) explains that radicalization towards terrorism can be understood as a gradual psychological journey when individuals move from the perception of injustice to the acceptance of the morality of violence. In the context of self-radicalization, these stages can take place without a face-to-face encounter

with the recruiter because the digital space allows individuals to find justification for their disappointment, anger, or alienation.

Cyber Engagement Concept

Cyber engagement is understood as an individual's engagement with a digital ecosystem that contains narratives, symbols, communications, propaganda, and extreme communities. This engagement not only means passive access to online content, but also includes the activity of searching, reading, watching, storing, sharing, interacting, and identifying with extreme narratives. In this study, cyber engagement is positioned as a mechanism for accelerating radicalization. De Bie et al. (2015) show that technological developments influence the modus operandi of extremist actors, including the way they prepare for actions and adapt to changing structure of opportunity.

Digital spaces have a different character than conventional recruitment arenas. It is anonymous, accessible, emotional, visual, repetitive, and can form echo spaces. In such echo chambers, individuals are more likely to encounter narratives that reinforce their own beliefs than critical comparative narratives. When individuals experience isolation in the family or community, digital spaces can become substitute communities that give a sense of belonging.

The Concept of Apathy and Family Dysfunction

Family apathy in this study is understood as the weak function of the family in providing emotional attention, dialogical communication, behavioral supervision, and assistance to the digital activities of family members. Apathy does not simply mean an absence of affection, but points to the failure of the family to read the psychological and behavioral changes of the individual. Family dysfunction can arise through closed communication, prolonged conflict, emotional neglect, authoritarian relationships, or weak control over online activities.

This concept is important because the family is the first social institution that shapes an individual's identity, emotional attachment, and value orientation. When family function is weakened, individuals may look for substitutes for affection and recognition outside the family. Hafez (2016) explained that family and friendship bonds can be utilized in extreme environments because close relationships are able to provide trust, loyalty, and emotional validation. In this study, the argument is expanded by placing the family not only as a reproductive channel of radicalism, but also as an arena of prevention.

Teori Staircase to Terrorism

Moghaddam' s theory of the staircase to terrorism is used as a foundation for understanding radicalization as a gradual psychological process. Moghaddam described terrorism as the pinnacle of an increasingly narrow staircase. On the ground floor, individuals experience perceptions of relative injustice and deprivation. In the next stage, the individual seeks a solution, experiences frustration, shifts aggression to outside groups, accepts the moral legitimacy of the extreme organization, and finally is ready to commit violence. Moghaddam (2005) asserts that the higher an individual climbs the ladder, the fewer options he sees but destruction to himself or others.

In this study, the theory is used to explain the basic process of individual radicalization. However, this theory needs to be read adaptively because the development of the digital space changes the tempo and medium of radicalization. Stages that could initially take place through direct social interaction can now be accelerated through algorithms, visual propaganda, online communities, and closed communication. Therefore, the staircase to terrorism is not abandoned, but modified through the concept of cyber engagement.

Significance Quest Theories

Significance quest theory explains that one of the main drives toward violent extremism is the individual's need to feel meaningful, respected, and valued. When an individual experiences a loss of significance due to humiliation, failure, alienation, family conflict, or social marginalization, he or she can look for ways to restore self-esteem. Extreme violence can then be perceived as a way of acquiring moral status, recognition, or dignity. Kruglanski et al. (2014) explain that radicalization involves three important components, namely motivation to gain significance, an ideology that justifies violence as a means, and a social network that facilitates the internalization of these ideologies.

This theory is particularly relevant to the focus of the research because family apathy can be read as a source of loss of significance. Individuals who do not gain emotional recognition at home may be more easily attracted to propaganda that offers a heroic identity. In the digital space, extreme narratives often promise a powerful meaning: being a defender of religion, a warrior of truth, or part of a select community.

Konsep Shortcut to Terrorism

The concept of shortcut to terrorism is used to explain the acceleration of radicalization when individuals no longer go through the long stages of formal organization. In the classic pattern, a person might be recruited, fostered, tested for loyalty, trained, and directed by the organization. In a shortcut pattern, individuals can move faster through exposure to digital propaganda, ideological manual consumption, online interactions, and symbolic identification. It does not always require direct orders because the legitimacy of violence has been obtained through the internalization of extreme narratives.

This concept expands the theory of staircase to terrorism. If ladder theory explains the psychological sequence to violence, then the shortcut explains how digital space compresses that sequence. De Bie et al. (2015) show that the operational dynamics of extremism change with technological developments and social opportunities. Therefore, the shortcut to terrorism in this study is positioned as a mechanism that explains the acceleration from family vulnerability to the potential for action of a single perpetrator

Synthesis of Conceptual Frameworks

Based on these concepts and theories, this study builds a conceptual framework that connects family apathy, significance crisis, cyber engagement, self-radicalization, and lone wolf terrorism. Family apathy serves as an upstream condition that weakens an individual's emotional resilience and identity. This condition creates space for significance quests, which are the need to gain meaning and recognition. When those needs are not met through a healthy

family or community, individuals can seek compensation through digital spaces. Cyber engagement then brings individuals together with propaganda, echo chambers, pseudo-communities, and violent narratives. This process encourages self-radicalization, which is the internalization of extreme ideologies in a personal way. If not detected, the process can develop into a shortcut to terrorism and lead to lone wolf terrorism.

METHODOLOGY

This study uses a qualitative approach with a plural case study design to explain how family apathy contributes to the escalation of self-radicalization through cyber engagement in the lone wolf terrorism phenomenon in Indonesia. The choice of a qualitative approach is based on the character of the problem that does not only demand measurement of frequency or correlation, but requires a deep understanding of the processes, meanings, social relations, and psychological mechanisms that make up the individual's vulnerability to digital radicalization. In qualitative research, analysis is not rigidly separated from the process of data collection and reading, as researchers need to interpret narratives, documents, and traces of events to find patterns of meaning that answer the research questions (Miles et al., 2018).

The case study design was chosen because this study seeks to answer the question of "how" and "why" family apathy can be an initial condition that increases vulnerability to cyber radicalization. Case studies are appropriately used when researchers analyze contemporary phenomena, have limited control over the events being studied, and require an in-depth investigation of the relationship between context and social processes (Yin, 2009). With this framework, this study does not treat cases as mere illustrations, but rather as an empirical unit that allows the development of a conceptual understanding of the relationship between families, the digital space, and the escalation of single-perpetrator violence. The use of case studies is also not intended to generate statistical generalizations, but to build analytical generalizations through an in-depth reading of the mechanisms at work in a particular case. This is in line with the view that case studies can provide contextual knowledge that is important for the development of social theory, especially when cases are strategically chosen to explain the dynamics of complex phenomena (Flyvbjerg, 2006).

The analysis unit of this research is the process of individual radicalization of perpetrators or potential perpetrators of lone wolf terrorism which is formed through the interaction between family vulnerability, digital involvement, and the internalization of extreme ideologies. The focus of the analysis is not directed at terror organizations as the main actors, but on the social-psychological mechanisms that allow individuals to move from isolation, search for meaning, exposure to propaganda, to the potential readiness to commit acts of violence independently. This study places two main cases as the basis for analysis, namely the case of teenagers in Subang which shows the role of family detection and the case of Zakiah Aini which shows the escalation of digital radicalization to the actions of single perpetrators. The selection of these two cases is purposive because they show important variations: one case shows the family as a point of

early intervention, while the other case shows the weak detection of the family before the action occurs.

The research data source uses secondary data consisting of scientific articles, institutional reports, policy documents, studies on digital radicalization, and case descriptions that are available in the main text. Secondary data was chosen because terrorism issues, especially those involving children, families, and digital footprints of perpetrators, have ethical sensitivity and limited access to primary data. The data used were selected based on their relevance to four main categories, namely apathy or family dysfunction, cyber engagement, self-radicalization, and lone wolf terrorism. Sources that are speculative, unclear in origin, contain technical propaganda, or have no direct connection to the focus of the research are excluded from the corpus of analysis.

Data analysis is carried out through thematic analysis with the stages of document reading, data reduction, initial coding, category grouping, and the formation of analytical themes. The initial coding was directed to identify indicators such as emotional neglect, weak family communication, behavioral changes, intensity of digital space use, extreme content consumption, identity search, online community validation, and the tendency to act independently. After that, the initial codes are grouped into broader categories, such as family vulnerability, identity crisis, digital acceleration, and escalation to action. The final stage was carried out by compiling a selective theme that explained the relationship between family apathy, significance quest, cyber engagement, and lone wolf escalation.

To maintain the credibility of the research, the data validity strategy is carried out through triangulation of sources, thick descriptions, and an analytical audit trail. Triangulation is carried out by comparing information from main texts, academic literature, institutional reports, and relevant news sources. Bold descriptions are used to ensure that each case is not cut out of its social and psychological context. The audit trail is carried out by explaining the reasons for selecting cases, the categories of analysis, and the process of pulling the theme so that the reader can assess the relationship between the data and the conclusions. In qualitative research, validity is not primarily attached to the raw data, but to the accuracy of the inferences drawn from the data; therefore, researchers need to show that the constructed interpretation is credible and accountable (Creswell & Miller, 2000).

Ethical considerations are an important part because this study discusses terrorism, the perpetrator's family, children or adolescents, and extreme digital exposure. The study does not present technical details regarding the manufacture of weapons, does not reproduce propaganda materials, and does not reveal the identities of minors excessively. The analysis is directed at social mechanisms and prevention, not at the glorification of perpetrators or the spread of extreme narratives. This precautionary principle is important for research to continue to meet academic responsibilities and public safety.

Table 1. Secondary Data Corpus and Its Relevance to Research Topics

Document Type	Focus of the Document	Functions in Analysis
Academic articles on terrorism and militancy	A study on variations in violence choices, *lone actors, foreign/domestic fighting*, and changes in the modus operandi of extremism (Hegghammer, 2013; De Bie et al., 2015).	Explain the context of changing threats, the relationship between the digital space and changing modus operandi, and the formation of an initial framework regarding *lone wolf terrorism*.
The Psychology of Radicalization	*Staircase to terrorism* dan *significance quest* (Moghaddam, 2005; Kruglanski et al., 2014).	It becomes an analytical knife to read identity crises, the search for meaning, the narrowing of moral choices, and the legitimacy of violence.
Family literature and social networks	The role of family ties and friendships in the process of radicalization and prevention (Hafez, 2016).	Helps explain family ambivalence as a risk factor as well as a protective factor.
Counter-radicalization policy literature	Deradicalization, *disengagement*, and prevention of extreme recruitment (Horgan, 2008; Viano, 2018).	It is the basis for formulating the implications of family-based policies, digital literacy, and early social interventions.
Qualitative methodology literature	Case studies, qualitative validity, data analysis, and analytical generalizations (Yin, 2009; Flyvbjerg, 2006; Miles et al., 2018; Creswell & Miller, 2000).	Supporting research design, case selection, thematic analysis, triangulation, and trail audits.

Table 2. Thematic *Analysis* Codebook

Tema Utama	Analytical Code	Operational Definition	Empirical Indicators
Apathy/Family Dysfunction	domestic isolation; emotional neglect; poor communication; absence of digital supervision; *significance loss*	Failure of family function in monitoring behavior, providing emotional safe spaces, and reading the psychological	Behavior changes are not responded to, family communication is closed, there is a lack of digital mentoring, or failure to read

		changes of family members.	identity crisis signals.
Cyber Engagement	*echo chamber*; propaganda consumption; virtual communities; pseudo-compensation; Digital Validation	An individual's engagement with an extremist digital ecosystem that provides narratives, identities, and justifications for violence.	Increased consumption of extreme content, interaction with violent narratives, use of closed channels, and self-identification with virtual communities.
Self-Radicalization	*self-selected; self-trained;* internalisasi mandiri; *shortcut to terrorism*	The process of changing attitudes and orientations of violence is relatively independent without the mediation of formal organizations.	Individuals build their own ideological justifications, seek digital legitimacy, and demonstrate readiness to act without direct instruction.
Family Resilience	assertive communication; early detection; reporting; Protective Interventions	The family's capacity to read behavioral anomalies and take preventive measures before the escalation of violence occurs.	Families pay attention to behavioral changes, build communication, seek help, and report risks to authorities.

RESEARCH RESULTS

Based on the reading of the secondary data corpus and case descriptions, this study found four main themes: family apathy as the root of psychological vulnerability, *cyber engagement* as an accelerator of radicalization, *self-radicalization* as a process of self-internalization, and family resilience as a factor that breaks the escalation. The first findings suggest that family apathy works as an upstream condition that generates psychological vulnerability. Families that fail to provide affection, dialogical communication, and digital supervision create empty spaces in the formation of individual identities. This empty space does not automatically give birth to radicalism, but increases the possibility of individuals seeking recognition, meaning, and certainty outside the family. In such situations, extreme propaganda gains traction because it offers a resolute identity, a moral mission that is considered sacred, and a symbolic community that gives a sense of belonging.

The second finding suggests that *cyber engagement* accelerates the encounter between psychological vulnerability and extreme narratives. Digital spaces provide propaganda, echo spaces, virtual communities, and emotional validation mechanisms that can replace the function of the family as a source of recognition. Individuals who have previously experienced alienation may feel that they have found a new community that provides moral certainty and identity. Thus, the internet is not positioned as the sole cause of radicalization, but as an accelerator when meeting individuals who have a crisis of significance.

The third finding shows that the process *of self-radicalization* in single actors tends to take place through a pattern *of self-selection* and internalization of personal ideologies. Individuals do not necessarily need formal command, direct training, or a clear organizational structure to move toward violence. Through repeated digital exposure, individuals can build moral justification, choose symbolic enemies, and position themselves as mission-driven actors. At this point, the concept of *shortcut to terrorism* becomes relevant to explain how the usually gradual process of radicalization can experience time and medium compression.

The fourth finding suggests that the family can not only be a risk space, but also a protective factor. A comparison of the cases of Subang and Zakiah Aini shows that family sensitivity can stop escalation before an act of violence occurs, while failure to read behavior changes can increase the chances of action. Thus, the family must be read as a preventive actor, not just the social background of the perpetrator.

Table 3. Comparison of Lone Wolf Escalation in the Subang Case and the Zakiah Aini Case

Comparison Dimensions	**The Case of the Subang**	**The Case of Zakiah Aini**
Case profile	Adolescents who show indications of digital radicalization and readiness to take action, but are successfully prevented through family detection.	Young adult perpetrators who have experienced an escalation of radicalization to carry out solitary attacks on state security symbols.
The role of the family	Family resilience works. Behavioral changes are read as risk signals and responded to through reporting to the authorities.	Family detection doesn't work optimally. Behavioral changes and ideological communication are not fast enough to be the basis for intervention.
Bentuk *cyber engagement*	Digital exposure becomes an initial source of learning and legitimacy, but the process stalls before escalation leads to action.	Digital engagement is seen in the dissemination of ideological narratives and identification with violent missions ahead of the action.

Escalation rate	Radicalization stops in the readiness phase and can be broken by family intervention.	Radicalization moves quickly towards *a shortcut to terrorism* and ends in action.
Makna analitis	Showing the family as an *early warning system* that is able to break the escalation.	Showing the risks when the digital space takes over the function of providing meaning and families fail to intervene early.

Based on the comparative findings presented in Table 3, the dynamics of family intervention and digital exposure can be further synthesized into a conceptual model that explains the escalation process of lone wolf terrorism.

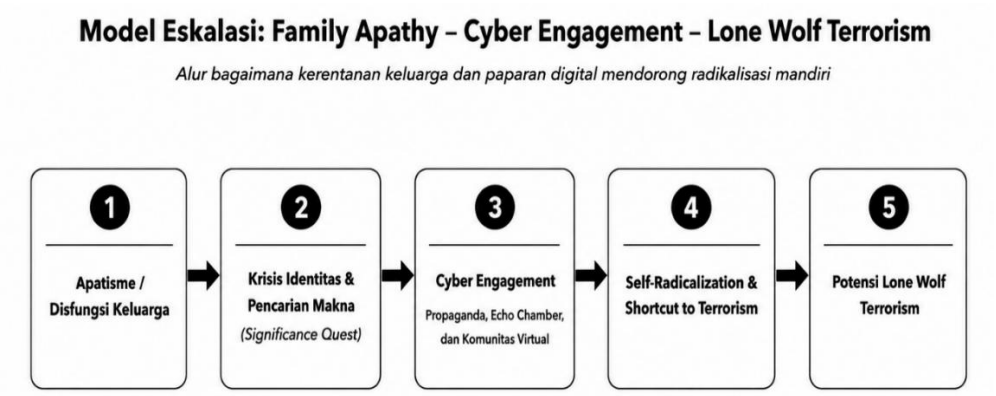

Figure 1. Model Konseptual *Family Apathy-Cyber Engagement-Lone Wolf Escalation*

The model in Figure 1 shows that family apathy creates psychological vulnerability that then drives identity crises and the search for significance. As individuals enter the digital space, *cyber engagement* brings together those vulnerabilities with propaganda, echo chambers, and virtual communities. These interactions accelerate *self-radicalization* and can encourage *shortcuts to terrorism* to the point of potential *lone wolf terrorism*. This model also emphasizes that the most important intervention point is to strengthen family resilience and digital literacy before the radicalization process reaches behavioral readiness.

DISCUSSION

Family Apathy as the Root of Psychological Vulnerability in the Process of Self-Radicalization

The main question of this study is how family apathy contributes to the escalation of self-radicalization through cyber engagement in the lone wolf terrorism phenomenon in Indonesia. Based on the findings, family apathy cannot be understood simply as a passive social setting, but as an upstream condition that forms an individual's psychological vulnerability before he or she interacts intensively with extreme propaganda in the digital space. In this perspective, the family is not only a domestic institution, but the starting field for

identity formation, self-control, moral orientation, and resilience to the infiltration of violent ideologies.

Theoretically, the position of the family in this study has two faces. On the one hand, the family can be a protective space that provides affection, communication, supervision, and correction to behavior changes. On the other hand, an apathetic family can create an emotional void that leads individuals to seek validation outside of the home environment. Hafez (2016) explained that family ties and friendships have a big role in the radicalization process because close relationships can provide trust, loyalty, peer pressure, and validation from people who are considered valuable. This argument suggests that the family is not just a biographical background, but part of a relational structure that can reinforce or inhibit the process of radicalization.

In the case of self-radicalization, family failure works more through indirect mechanisms. Family apathy does not necessarily radicalize a person, but it creates a psychosocial condition that makes it easier for individuals to accept extreme narratives when they offer meaning, certainty, and identity. Individuals who feel misunderstood at home tend to look for alternative spaces to explain their disappointment and anxiety. When families fail to establish dialogical communication, behavioral changes such as self-isolation, intensity of internet use, interest in violent narratives, or changes in patterns of social relationships can occur without correction.

In the framework of the psychology of radicalization, this vulnerability can be read through significance quest theory. Kruglanski et al. (2014) state that the search for personal significance is a motivational drive that can drive individuals toward violent extremism when the need for meaning and recognition meets ideologies that justify violence. Family apathy becomes important because it can result in a loss of significance at the most intimate level. When the individual does not gain emotional recognition from the family, he or she is more easily drawn to narratives that promise heroic status, moral purity, and privileged position as part of a group that is considered righteous.

Cyber Engagement as a Catalyst and Accelerator of Radicalization

Once vulnerability is formed at the family level, cyber engagement becomes a mechanism that brings together individuals with extreme narratives, online communities, and violent justifications. In this study, cyber engagement is not only interpreted as an activity of accessing the internet, but as active or repeated engagement with extremist content, symbols, networks, conversations, and echo spaces. This engagement can take the form of searching for ideological content, following specific accounts, joining closed channels, reading hate narratives, consuming visual content, or building emotional identification with extreme communities.

The role of the digital space is becoming increasingly important as it changes the way radicalization takes place. In the old pattern, radicalization often relied on physical encounters, closed recitations, training, ideological mentoring, and network involvement. In the new pattern, individuals can experience accelerated radicalization through personal screens without having to leave the house. De Bie et al. (2015) show that technological developments, changes in the

structure of social opportunities, and geopolitical dynamics influence the modus operandi of extremist actors, including how they prepare for actions and adjust strategies. These findings are relevant because digital radicalization is not just a change in the medium of communication, but a change in the structure of opportunities for isolated individuals to access extreme ideologies quickly and privately.

Cyberspace also strengthens radicalization through echo chamber mechanisms. In echo chambers, individuals tend to accept narratives that confirm their own disappointment, resentment, and perceptions of injustice. When algorithms, content consumption choices, and closed networks bring together individuals with homogeneous narratives, the likelihood of social correction becomes increasingly weak. Extreme propaganda doesn't always work through lengthy arguments; He often works through the repetition of symbols, emotions, images of the victim, the glorification of the perpetrator, and the narrative of hostility.

This answers part of the research question: family apathy contributes to the escalation of self-radicalization because it creates a void that is then filled by cyber engagement. Without psychological vulnerability, digital exposure does not necessarily result in radicalization. Conversely, without the digital space, family vulnerability does not necessarily move quickly towards the legitimacy of violence. Problems arise when the two meet: individuals who are isolated, do not gain family recognition, experience an identity crisis, and then find an extreme narrative that offers certainty, solidarity, and mission.

Staircase to Terrorism and Compression of Radicalization Stages

The staircase to terrorism theory helps explain that terrorism is not a sudden event, but rather the result of a gradual psychological process. Moghaddam (2005) describes individuals who move from perceptions of injustice to frustration, diversion of aggression, acceptance of the morality of violence, categorization of "us versus them", and finally readiness to commit destructive actions. This theory is important because it provides a framework that single-actor radicalization still has a process, even if that process is not always visible from the outside.

However, the discussion of this study shows that the digital space changes the tempo of the ladder theory. If in the classical model the individual climbs the ladder of radicalization through relatively observable social stages, in the digital context some of these stages can be compressed. Individuals do not have to attend physical gatherings to accept the morality of violence. It can derive ideological justification, symbolic enemies, and legitimacy of action from content consumed repeatedly. Nor does he have to be recruited by a formal organization to feel part of an extreme struggle.

Thus, the shortcut to terrorism is not a rejection of Moghaddam's theory, but a modification of the rhythm and medium of radicalization. This theory is useful in understanding psychological processes, but the development of cyberspace makes inter-stage transfers faster, more private, and more difficult to supervise. Therefore, the concept of shortcut to terrorism in this study does not

mean that radicalization does not have stages, but that these stages can be passed more densely through digital interaction.

Significance Quest as a Connecting Mechanism between Family and Digital Propaganda

Significance quest theory provides a sharp analytical knife to explain why individuals who experience family apathy may be drawn to extreme propaganda. Kruglanski et al. (2014) explain that radicalization towards violence involves the urge to acquire significance, ideologies that justify violence, and social networks that help internalize those ideologies. In this study, the drive to gain significance emerged from the experience of family alienation; ideologies that justify violence obtained through extreme content; Social networks are not always in the form of physical organizations, but can take the form of virtual communities, echo spaces, or symbolic relationships with the global narrative of extremism.

Family apathy works by weakening the individual's sense of worth. Individuals who feel unnoticed, unheard, or unacknowledged can experience a crisis of meaning. In this phase, extreme propaganda often comes with a very strong language: it offers the mission, identity, enemies, status, and feeling of being part of something bigger. Extreme propaganda not only says that violence is true, but also that the perpetrator will become meaningful through violence. At this point, the search for significance turns into a path to acceptance of violence.

The comparison of the cases of Subang and Zakiah Aini shows how the process of individualization of radicalization can occur when personal vulnerability meets digital propaganda. In the case of Subang, the family is present as an early detection system that stops the escalation. In the case of Zakiah Aini, the process of radicalization has developed into acts of violence. This comparison shows that the need for significance does not always lead to action if there is timely family intervention. Conversely, when families fail to read behavioral changes or lack the literacy to understand indicators of digital radicalization, cyberspace can take over meaning-giving functions.

Lone Wolf Terrorism as a Result of the Intersection of Family Vulnerability and Digital Acceleration

The concept of lone wolf terrorism in this study is used to read acts of violence committed by individuals independently without direct command from the terror organization. However, operational independence does not mean ideological independence. The single perpetrator remains influenced by the narratives, symbols, propaganda, and extreme communities that shape his or her frame of mind. Hegghammer (2013) shows that not all radical individuals choose the same path of violence, and some choose to attack within the country after undergoing a certain radicalization process. This confirms that the focus of analysis should be directed at the process that turns vulnerabilities into action options.

Lone wolf terrorism in this article is positioned as the culmination of the intersection between the vacuums of family control functions and rapid cyber radicalization. This statement is important because it rejects a view that separates

domestic and digital factors. A single perpetrator does not appear just because of the internet, and it does not appear just because the family is in trouble. It emerged when the family failed to become a protective fortress, while the digital space managed to become an alternative source of identity. Here, lone wolf terrorism is not only a problem of a single actor, but a symptom of the failure of the social ecosystem in detecting and responding to private radicalization.

The Subang case shows the protective side of the family. Analytically, this case shows that families can be an effective early warning system. The father's actions in reading about behavior changes and taking reporting steps show that families have access to microindicators that are not always accessible to security forces. On the other hand, the case of Zakiah Aini shows how digital radicalization can develop into action when the process of internalizing ideology is not detected or responded to too late.

Policy Implications: From Hard Approaches to Family-Based Prevention and Digital Literacy

This discussion resulted in a policy implication that the prevention of lone wolf terrorism does not rely enough on a repressive state security approach. Prevention needs to move towards social-preventive that is earlier, participatory, and family-based in the family community. This does not mean diminishing the importance of law enforcement, digital monitoring, and security intelligence, but it does affirm that security approaches need to be complemented by strengthening families as protective actors.

The first implication is the need for a family digital literacy program. Parents and family members need to be equipped with the ability to recognize indicators of digital radicalization without falling into moral panic. Digital literacy does not only mean the ability to use technology, but the ability to understand the risks of echo chambers, visual propaganda, hate narratives, closed channels, and behavioral changes related to extreme content consumption. This program can be developed through cooperation between BNPT, the National Police, schools, local governments, moderate religious organizations, and community communities.

The second implication is the need for family psychoeducation. Since radicalization is related to the search for meaning, recognition, and identity, the family needs to be strengthened in emotional communication skills. Prevention is not enough with prohibitions, harsh surveillance, or authoritarian control. Harsh controls without dialogue can actually reinforce alienation. Families need to build a conversation space that allows the child or young family member to talk about anxiety, religious questions, experiences of discrimination, and the search for identity without fear of judgment.

The third implication is the establishment of a community-based early detection system that is not stigmatized. Families need to know where to turn for help when they see suspicious behavior changes. Reporting mechanisms should be designed not as early criminalization, but as a path of consultation, assessment, and social intervention. The fourth implication is the need for integration between digital monitoring and social interventions. Extreme content removal is important, but not enough. As long as the need for meaning and

recognition is not met, individuals may move to other platforms or find a replacement narrative.

CONCLUSIONS AND RECOMMENDATIONS

This study concludes that lone wolf terrorism in Indonesia cannot be explained solely through ideological approaches, formal terrorist networks, or weak state surveillance. The escalation of self-radicalization occurs through a complex interaction between psychosocial vulnerability within the family, the search for personal meaning, and individual involvement in extremist digital ecosystems. Family apathy functions as an initial condition that weakens emotional resilience, leading to alienation, identity crises, and a heightened need for recognition. Within the framework of significance quest theory, radicalization develops when individuals find meaning, moral status, and self-worth through extremist narratives. Cyber engagement acts as an accelerator that intensifies this process by providing digital spaces that offer identity validation, pseudo-communities, and ideological propaganda.

Theoretically, the staircase to terrorism model remains relevant; however, in the digital era, the process becomes faster and forms a shortcut to terrorism. Exposure to online narratives that promote hatred and legitimize violence accelerates the narrowing of individuals' psychological choices, leading toward the acceptance of violent behavior. Accordingly, family apathy contributes indirectly by creating psychological vulnerability, while cyber engagement accelerates the internalization of extremist ideology and increases the potential for individual violent action. Lone wolf terrorism emerges as the result of the interaction between family dysfunction, the search for meaning, and digital acceleration.

From a policy perspective, prevention efforts need to shift from a predominantly repressive approach to a social-preventive strategy based on family engagement and digital literacy. These strategies include strengthening family digital literacy, establishing safe and confidential early consultation and reporting systems, providing family psychoeducation, and developing counter-narratives that address identity and meaning needs. However, this study is limited by its reliance on secondary data; therefore, further research is required through field studies, interviews, and case analysis to comprehensively test the family apathy–cyber engagement–lone wolf escalation model.

REFERENCES

Bjørgo, T., & Carlsson, Y. (2005). Early intervention with violent and racist youth groups. Norwegian Institute of International Affairs (NUPI).

Campelo, N., Oppetit, A., Neau, F., Cohen, D., & Bronsard, G. (2018). Who are the European youths willing to engage in radicalisation? A multidisciplinary review of their psychological and social profiles. European Psychiatry, 52, 1–14. https://doi.org/10.1016/j.eurpsy.2018.03.001

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. Theory Into Practice, 39(3), 124–130. https://doi.org/10.1207/s15430421tip3903_2

De Bie, J. L., De Poot, C. J., & Van der Leun, J. P. (2015). Shifting modus operandi of jihadist foreign fighters from the Netherlands between 2000 and 2013: A crime script analysis. Terrorism and Political Violence. Advance online publication. https://doi.org/10.1080/09546553.2015.1021038

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. Qualitative Inquiry, 12(2), 219–245. https://doi.org/10.1177/1077800405284363

Hafez, M. M. (2016). The ties that bind: How terrorists exploit family bonds. CTC Sentinel, 9(2), 15–17.

Hegghammer, T. (2013). Should I stay or should I go? Explaining variation in Western jihadists' choice between domestic and foreign fighting. American Political Science Review, 107(1), 1–15. https://doi.org/10.1017/S0003055412000615

Hoffman, B., & Reinares, F. (2014). The evolution of the global terrorist threat: From 9/11 to Osama bin Laden's death. Columbia University Press.

Horgan, J. (2008). Deradicalization or disengagement? A process in need of clarity and a counterterrorism initiative in need of evaluation. Perspectives on Terrorism, 2(4), 3–8. https://www.jstor.org/stable/26298340

Jafar, T. F., Sudirman, A., & Rifawan, A. (2019). National Resilience faces the threat of lone wolf terrorism in West Java. Journal of National Resilience, 25(1), 73–91. https://doi.org/10.22146/jkn.41244

Kruglanski, A. W., Gelfand, M. J., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., & Gunaratna, R. (2014). The psychology of radicalization and deradicalization: How significance quest impacts violent extremism. Advances in Political Psychology, 35(S1), 69–93. https://doi.org/10.1111/pops.12163

McCauley, C., & Moskalenko, S. (2014). Toward a profile of lone wolf terrorists: What moves an individual from radical opinion to radical action. Terrorism and Political Violence, 26(1), 69–85. https://doi.org/10.1080/09546553.2014.849916

Miles, M. B., Huberman, A. M., & Saldaña, J. (2018). Qualitative data analysis: A methods sourcebook (4th ed.). SAGE Publications.

Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. American Psychologist, 60(2), 161–169. https://doi.org/10.1037/0003-066X.60.2.161

Nuraniyah, N. (2019). The evolution of online violent extremism in Indonesia and the Philippines. Global Research Network on Terrorism and Technology, Paper 5. Royal United Services Institute (RUSI).

Pantucci, R. (2011). A typology of lone wolves: Preliminary analysis of lone Islamist terrorists. The International Centre for the Study of Radicalisation and Political Violence (ICSR).

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

Riyanta, S. (2022). Shortcut to terrorism: Self-radicalization and lone-wolf terror acts: A case study of Indonesia. Journal of Terrorism Studies, 4(1), Article 2. https://doi.org/10.7454/jts.v4i1.1043

Sageman, M. (2008). Leaderless jihad: Terror networks in the twenty-first century. University of Pennsylvania Press.

Sarour, E. O., & El Keshky, M. E. S. (2022). Understanding extremist ideas: The mediating role of psychological well-being in the relationship between family functioning and extremism. Children and Youth Services Review, 136, 106420. https://doi.org/10.1016/j.childyouth.2022.106420

Scremin, N. (2020). Family matters: A preliminary framework for understanding family influence on Islamist radicalization. Studies in Conflict & Terrorism, 45(11), 921–944. https://doi.org/10.1080/1057610X.2020.1841242

Spaaij, R. (2012). Understanding lone wolf terrorism: Global patterns, motivations and prevention. Springer.

Susetyo, H., Arimbi, R. S., Andersen, M. K., & Wang, S.-J. (2026). Analysis of social networks and peer contagion in terrorism-related offences in Indonesia. Journal of Law and Legal Reform, 7(1), 203–250. https://doi.org/10.15294/jllr.v7i1.40357

Viano, E. C. (2018). Female migration to ISIS: Conclusions and recommendations. International Annals of Criminology, 56(1–2), 220–226. https://doi.org/10.1017/cri.2018.20

Webber, D., & Kruglanski, A. W. (2017). The social psychological makings of a terrorist. Current Opinion in Psychology, 19, 131–134. https://doi.org/10.1016/j.copsyc.2017.03.024

Yin, R. K. (2009). Case study research: Design and methods (4th ed.). SAGE Publications.