Bulletin of Community Engagement
Vol. 6, No. 2, August 2026
https://attractivejournal.com/index.php/bce//index

Virtual Directed Radicalization: Digital *Bai'at* and "DIY" Terrorism Among Adolescents

Muhamad Syauqillah [1*], Ami Prindani [2], Juwarti Hafsah [3], Achmad Sauri [4]
[1,2] *Universitas Indonesia, Indonesia*
[3] *Institute for Strategic Transformation, Indonesia*
[4] *Universitas Islam Jakarta, Indonesia*

muhamadsyauqillah@ui.ac.id

ARTICLE INFO
Article history:
Received
March 03, 2026
Revised
June 22, 2026
Accepted
July 18, 2026

Abstract

This study examines the cyber radicalization process among Indonesian adolescents, analyzing their transition from digital exposure to operational readiness for terrorism. Utilizing a qualitative case study approach, data were collected through in-depth interviews and document analysis of three adolescents exposed to radical ideologies. The findings were interpreted through the Three Stages of Terrorism Framework. Results reveal a structured progression: the pre-radicalism phase is driven by psychosocial vulnerabilities and identity crises; the exposure phase is accelerated by social media algorithms, filter bubbles, and echo chambers; and the terror act phase manifests in operational capabilities, including online pledges of allegiance (*bai'at*) and "Do-It-Yourself" (DIY) bomb-making. Furthermore, the study introduces the concept of *Virtually Directed Radicalization* (VDR), illustrating how anonymous online facilitators remotely guide vulnerable youth from passive content consumption to binding operational commitments. The study concludes that cyberspace now functions not merely as a propaganda medium, but as a comprehensive ecosystem for ideological indoctrination and clandestine operational preparation, necessitating urgent, digitally informed counterterrorism and psychosocial interventions.

Keywords: Cyber radicalization, Virtually Directed Radicalization, Do-It-Yourself Terrorism

Published by CV. Creative Tugu Pena
ISSN 2774-7077
Website https://attractivejournal.com/index.php/bce/

INTRODUCTION

The landscape of extremist recruitment has fundamentally shifted from traditional, face-to-face organizational networks to decentralized digital ecosystems. Cyberspace now serves as a primary arena for ideological mobilization, allowing extremist narratives to transcend geographical boundaries and reach global audiences instantaneously (Mohiuddin, 2023; Sholehoddin et al., 2025; Stockhammer, 2025; Whittaker, 2022). Unlike conventional models that require physical infrastructure, digital platforms enable continuous propaganda dissemination and decentralized radicalization, significantly lowering the barriers to extremist engagement.

This digital transformation poses a profound threat to adolescents, a demographic characterized by ongoing identity formation, emotional sensitivity, and a strong desire for social belonging. Vulnerable youth often turn to the internet to fulfill unmet psychological needs, making them highly susceptible to online grooming by extremist actors (Reyna et al., 2022; Widiarni et al., 2024; Windsor, 2020; Wolfowicz et al., 2021). In these digital environments, extremist groups frequently position themselves as surrogate communities, offering attention, emotional support, and a sense of purpose to isolated individuals.

The escalation of this vulnerability is heavily driven by the algorithmic architecture of social media platforms. Recommendation systems create "filter bubbles" that continuously feed users

increasingly extreme content based on their initial interactions, effectively isolating them from moderate perspectives (Areeb et al., 2023; Keijzer & Mäs, 2022; Yesilada & Lewandowsky, 2022). As users are funneled into encrypted, homogeneous online communities, these "echo chambers" reinforce extremist ideologies, normalize violence, and foster out-group antagonism through relentless social validation (Walther & Rice, 2024).

In Indonesia, this algorithmic radicalization is exacerbated by high internet penetration and a lack of digital supervision among the youth. Statistics indicate that a significant majority of internet users belong to Generation Z, with the vast majority accessing the web from the privacy of their homes. This unsupervised access within private domestic spaces creates an unmonitored gateway for virtual facilitators to manipulate emotions and recruit vulnerable adolescents through closed communication channels (Wolfowicz et al., 2021).

The real-world consequences of this unmonitored digital exposure have evolved into a tangible national security threat. Throughout 2025, the National Counterterrorism Agency (BNPT) identified over 21,000 pieces of online content containing elements of radicalism and intolerance (SinPo.id, 2025). Furthermore, data from the 2026 Technical Working Meeting of Densus 88 Anti-Terror revealed that 132 children had been exposed to digital radicalization, with many interacting with violent extremist ideologies exclusively through the internet (Polri, 2026).

To systematically understand these behavioral transformations, contemporary terrorism studies require frameworks that capture the nuances of digital indoctrination. This study utilizes the *Three Stages of Terrorism Framework* (Prindani & Syauqillah, 2025), which conceptualizes radicalization as a sequential progression: pre-radicalism (psychosocial vulnerabilities), exposure to radicalism (algorithmic and social reinforcement), and the terror act (operational readiness and preparation). This framework provides a structured lens to analyze how adolescents transition from passive consumers of digital content to active participants in extremist behaviors. Against this backdrop, this study aims to examine the behavioral transformations of adolescents within cyberspace as they navigate the radicalization process. By analyzing empirical cases of youth exposed to digital extremism, this research seeks to elucidate the mechanisms of *Virtually Directed Radicalization*, where online facilitators remotely guide vulnerable adolescents toward operational readiness. Ultimately, this study contributes to the development of more effective, digitally informed counterterrorism and prevention strategies in Indonesia.

METHOD

This study employed a descriptive qualitative case study design to investigate the psychosocial dynamics and behavioral trajectories of cyber-radicalization among adolescents in Indonesia. Using purposive sampling, three information-rich cases were selected from law enforcement and psychosocial records to represent varying stages of radicalization, ranging from early psychological vulnerability to operational readiness for "Do-It-Yourself" (DIY) terrorism. Data were collected through multiple sources to ensure comprehensive contextual insights, including semi-structured in-depth interviews with the subjects, their families, psychologists, and educators, alongside a thorough documentary analysis of law enforcement reports, psychological assessments, and social rehabilitation records. To maintain research integrity and protect the vulnerable participants, strict ethical protocols were enforced, including the complete anonymization of all identifying information and restricted access to confidential legal documents solely for academic purposes.

The collected data were analyzed using qualitative content analysis, which involved systematic data reduction, coding, and categorization to identify recurring themes related to the subjects' radicalization pathways. These empirical themes were subsequently interpreted through the *Three Stages of Terrorism Framework*—comprising pre-radicalism, exposure to radicalism, and the terror act—to map the progression from psychosocial vulnerabilities to operational capabilities. To ensure the trustworthiness and credibility of the findings, the study utilized methodological and source triangulation, cross-verifying interview transcripts with official documents and collateral reports. This rigorous analytical procedure allowed for a robust reconstruction of how digital ecosystems, algorithmic exposure, and virtual facilitation interact to drive the radicalization process among vulnerable youth.

RESULT AND DISCUSSION

1. Psychosocial Vulnerabilities and the Pre-Radicalization Vacuum

The initial phase of cyber radicalization among the researched adolescents was fundamentally rooted in profound psychosocial vulnerabilities and structural deficiencies within their immediate domestic environments. During this critical transitional period of youth, the subjects experienced severe identity crises, chronic loneliness, and social exclusion that severely weakened their psychological resilience against extremist narratives. Subject B endured chronic alienation following his parents' divorce, while Subject C faced persistent marginalization due to an inability to form meaningful friendships within his formal educational setting. Meanwhile, Subject A carried the heavy burden of familial responsibility caused by his mother's deteriorating health, which inadvertently resulted in a complete absence of parental supervision over his digital activities. These structural deficiencies severely limited their access to positive offline role models, leaving them entirely exposed to the manipulative influences of the digital world. These compounding emotional and social deficits created a profound psychological vacuum that systematically drove the adolescents to seek alternative coping mechanisms and virtual escapes.

In response to these overwhelming offline challenges, the adolescents increasingly retreated into the privacy of their bedrooms, transforming these domestic spaces into isolated sanctuaries for continuous digital immersion. The unrestricted access to smartphones and internet-connected devices allowed them to bypass traditional socialization agents, such as family members and educational institutions, in favor of anonymous virtual communities. As one subject articulated during the in-depth interview process, *"I spent most of my nights alone in my room because the internet was the only place where I felt understood and valued by others."* This profound detachment from physical social reality triggered a critical cognitive opening, making them exceptionally susceptible to the welcoming narratives of online extremist facilitators. Consequently, these virtual environments functioned as surrogate families, offering the emotional compensation, sense of belonging, and heroic purpose that were conspicuously absent in their offline lives.

Table 1. Synthesis of Psychosocial Vulnerabilities and Digital Entry Points Among Research Subjects

Research Subject	Vulnerabilities and Home Situation	Social Media Entry Point	Peak Physical Escalation
Subject A	Mother's prolonged illness resulted in limited parental supervision; unrestricted digital access in the bedroom.	Jihad-related content on TikTok; transitioned to closed WhatsApp group (One Ummah).	Refused to salute the flag; online bai'at; downloaded bomb-making manuals; sketched targets.
Subject B	Chronic loneliness due to parental divorce and mother's work; isolated with devices up to six hours daily.	Daulah nasheeds on YouTube/TikTok; migrated to WhatsApp and closed Telegram groups.	Online bai'at via Telegram; independent physical training; assembled suicide vest and remote detonators.
Subject C	Social isolation due to lack of close friendships; compensated through intensive online interactions.	Conflict videos on TikTok/YouTube since elementary school; invited to Telegram group (Munasirin).	Adopted exclusive terminology; normalized martyrdom; searched for Molotov cocktail tutorials.

The comprehensive synthesis presented in the table clearly illustrates a consistent and alarming pattern across all three cases, demonstrating that cyber radicalization emerged from a dangerous intersection of psychosocial fragility and unrestricted digital exposure. Although each subject navigated distinct personal circumstances, they universally shared deep-seated feelings of isolation, emotional neglect, and inadequate parental monitoring that facilitated their initial vulnerability to online grooming. The progression from mainstream social media platforms to exclusive, closed communication groups highlights a highly structured recruitment pathway where initial emotional escapism rapidly evolved into deeper ideological engagement. Furthermore, the data highlights the critical necessity for early psychosocial interventions to mitigate the risks associated with unmonitored digital escapism. Ultimately, these findings underscore that online

radicalization among adolescents is not merely a product of ideological persuasion, but rather a complex response to unfulfilled emotional and social needs within their physical environments.

2. Algorithmic Curation and the Filter Bubble Mechanism

The transition from passive digital consumption to active ideological exposure was heavily mediated and accelerated by the opaque algorithmic architectures of mainstream social media platforms. The subjects initially engaged with seemingly benign content, such as religious nasheeds, historical conflict videos, and general ideological discussions, which inadvertently triggered automated recommendation systems. These machine-learning algorithms rapidly categorized their viewing histories into specific clusters, subsequently feeding them an escalating stream of radical propaganda and violence-oriented materials. This systematic curation created a digital enclosure that automatically filtered out moderate perspectives, effectively isolating the adolescents within a homogeneous ecosystem of extremist narratives. This algorithmic manipulation effectively bypassed the adolescents' critical thinking faculties, ensuring a steady diet of polarizing and extremist material. As a result, the subjects were continuously exposed to increasingly polarizing content without consciously seeking out structured terrorist organizations or formal recruitment channels.

Within this algorithmically constrained environment, virtual facilitators strategically exploited the recommendation systems to identify and intercept psychologically vulnerable adolescents who were actively seeking connection. Recruiters employed sophisticated cyber-coaching techniques, initially presenting themselves as empathetic peers or protective mentors to establish crucial emotional bonds and gain the subjects' absolute trust. During the interviews, one subject revealed the manipulative nature of this digital grooming, stating, *"They approached me gently, offering advice and brotherhood when I felt completely abandoned by my real friends."* Once this psychological attachment was securely established, the facilitators distributed encrypted invitation links, deliberately migrating the subjects away from public platforms toward exclusive, unmonitored communication channels. This directed migration served as a calculated strategy to accelerate ideological indoctrination, conceal their activities from security authorities, and immerse the adolescents entirely within controlled digital echo chambers.

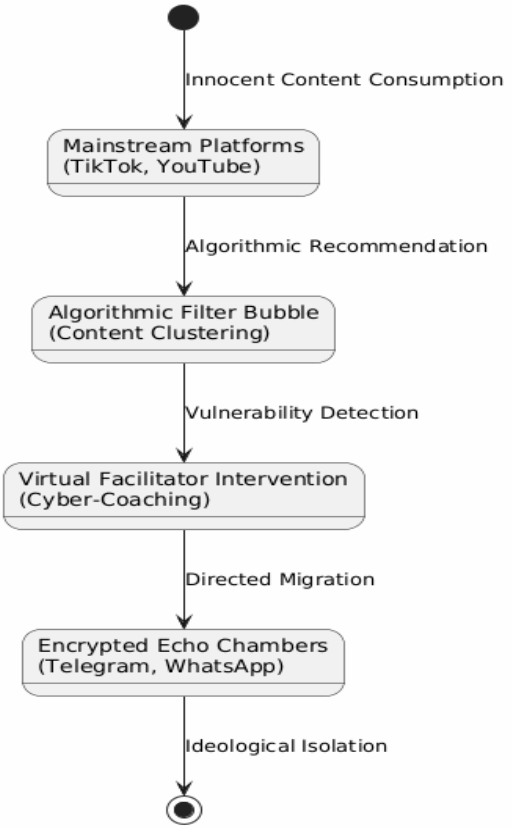

Figure 1. The Algorithmic Funnel: From Mainstream Consumption to Enclosed Extremist Ecosystems

The diagram above visually delineates the systematic progression of digital exposure, illustrating how algorithmic mechanisms inadvertently transform ordinary content consumption into a gateway for extremist recruitment. The funnel-like structure demonstrates the narrowing of cognitive diversity, where initial interactions with benign material are progressively filtered into highly specialized radical content clusters. Furthermore, it highlights the critical intervention point of virtual facilitators who actively exploit these algorithmic vulnerabilities to redirect vulnerable adolescents toward encrypted, unmonitored environments. Such technological determinism in the radicalization process necessitates urgent collaboration between platform developers and security agencies to disrupt these automated pipelines. This visual representation underscores the deceptive nature of modern digital radicalization, wherein the technology itself acts as an unwitting accomplice in the early stages of ideological manipulation and social isolation.

3. Echo Chamber Dynamics and Digital Bai'at

Upon entering the encrypted communication groups, the adolescents were immediately submerged in intense echo chamber dynamics that systematically reinforced extremist worldviews through continuous social validation. Within these closed digital communities, radical narratives were relentlessly amplified, normalized, and celebrated by group members who shared identical ideological orientations and hostile perspectives toward out-groups. The subjects rapidly adopted exclusive linguistic markers, such as specific Arabic terminology and derogatory labels for non-believers, which served as powerful symbolic indicators of their shifting group identity. This linguistic exclusion and constant ideological affirmation fostered a profound sense of out-group antagonism, effectively severing their remaining psychological ties to mainstream societal values. This collective validation created an impenetrable psychological barrier against any external counter-narratives or moderate perspectives. The echo chamber thus functioned as a highly efficient indoctrination engine, transforming abstract extremist concepts into deeply internalized, unquestionable belief systems supported by collective consensus.

The culmination of this intensive social reinforcement was marked by the subjects' willingness to perform symbolic acts of absolute loyalty, most notably the digital pledge of allegiance or online bai'at. Traditionally requiring physical presence and organizational integration, this sacred commitment was now executed entirely through digital mediums, reflecting the profound decentralization of contemporary terrorist networks. Reflecting on this pivotal moment, one subject confessed during the psychosocial assessment, *"Recording my pledge to the leader through a video message made me feel like I was finally part of a grand, heroic struggle."* These digital pledges represented a critical threshold, signifying the definitive transition from passive ideological sympathy to active operational commitment and readiness for violent action. Consequently, the subjects had fully internalized the group's objectives, preparing themselves psychologically for the eventual execution of terrorist directives without ever meeting their commanders in person.

Table 2. Indicators of Identity Transformation and Commitment in the Exposure Phase

Subject	Initial Digital Exposure	Platform Migration	Identity Transformation
A	Conflict and jihad-related content on TikTok	WhatsApp (One Ummah)	Rejection of national symbols
B	Daulah nasheeds on YouTube and TikTok	WhatsApp → Telegram	Display of extremist slogans
C	Conflict-related videos on TikTok and YouTube	Telegram (Munasirin)	Use of exclusive terminology and propaganda

The detailed indicators presented in the table reveal a highly consistent radicalization trajectory, wherein identity transformation invariably preceded any formal operational commitment or violent planning. The subjects first manifested their ideological alignment through the adoption of exclusive linguistic codes, the public display of extremist slogans, and the outright rejection of national symbols. Only after these profound psychological and social shifts were firmly established did the subjects demonstrate tangible commitments, such as executing online pledges of allegiance to terrorist leadership. Recognizing these behavioral milestones is crucial for educators and parents aiming to intervene before ideological commitment solidifies into operational planning. This sequential progression strongly suggests that digital radicalization is fundamentally a complex process of social and psychological metamorphosis rather than a simple acquisition of extremist information.

4. Operational Escalation and DIY Terrorism Capabilities

The final stage of the radicalization trajectory was characterized by the subjects' active pursuit of operational capabilities, marking their transition into the realm of Do-It-Yourself terrorism. Operating entirely from the privacy of their bedrooms, the adolescents utilized the internet to access sophisticated technical manuals, instructional videos, and tactical guidance previously restricted to physical training camps. Subject A systematically downloaded explosive engineering documents, meticulously sketched potential targets, and conducted dangerous chemical experiments using household materials to understand blast mechanics. Similarly, Subject B engaged in rigorous physical preparation, including archery and the assembly of complex, remotely triggered explosive devices using components sourced from local markets. The seamless integration of digital learning and physical experimentation represents a terrifying evolution in how modern terrorist capabilities are acquired. These activities unequivocally demonstrate that the digital environment now serves as a fully functional operational domain, enabling adolescents to achieve lethal technical proficiency without ever leaving their homes.

The successful development of these bomb-making capabilities among minors represents a profound escalation in contemporary security threats, blurring the traditional boundaries between virtual radicalization and physical terrorist preparation. The subjects' ability to independently fabricate functional explosive devices highlights the severe inadequacy of conventional supervision mechanisms in monitoring the lethal potential of private digital consumption. During the law enforcement interviews, investigators noted the alarming reality of this new paradigm, stating, *"We found teenagers in their bedrooms successfully building suicide vests using nothing but internet tutorials and sheer ideological obsession."* This empirical evidence confirms that the threshold for executing violent extremist activities has been drastically lowered, as cyberspace provides all necessary ideological, tactical, and technical resources. Consequently, the bedroom has effectively been transformed into a clandestine site of operational radicalization and terrorist mobilization, completely bypassing traditional organizational oversight.

Table 3. Operational Preparation and Technical Capabilities in the Terror Act Phase

Subject	Operational Preparation	Technical Capability	Intended Target/Action	Terror Act Indicator
A	Downloaded bomb-making manuals, conducted experiments	Mixed explosive materials and designed explosive devices	Church sketches and attack planning	High
B	Conducted i'dad training	Built small bombs, suicide vest bombs, and remote detonators	Successful testing of explosive devices	Very High
C	Searched for Molotov cocktail tutorials	Early-stage knowledge acquisition	No verified operational preparation	Moderate

The empirical data summarized in the table illustrates the varying degrees of operational readiness achieved by the subjects, highlighting the tangible outcomes of digitally facilitated terrorist training. Subject B demonstrates the most advanced level of threat, having successfully engineered and tested complex explosive mechanisms, while Subject A occupies an intermediate stage characterized by active material procurement and target identification. In contrast, Subject C remains in the preparatory information-gathering phase, focusing on ideological reinforcement and the acquisition of basic tactical knowledge through online searches. Ultimately, these empirical indicators provide a vital diagnostic tool for assessing the imminent threat levels posed by digitally radicalized youth. This stratification of operational capability underscores the incremental nature of digital learning environments, where access to encrypted tutorials systematically reduces the reliance on traditional terrorist infrastructures.

5. The Emergence of Virtually Directed Radicalization

Synthesizing the empirical findings across all stages of the terrorism framework reveals the emergence of a novel conceptual phenomenon termed Virtually Directed Radicalization. This concept describes a sophisticated process wherein the entire radicalization trajectory is progressively hijacked, controlled, and accelerated by anonymous online facilitators operating within encrypted digital ecosystems. Initially, the adolescents' internet consumption was

autonomous and unguided, driven primarily by psychological vulnerabilities and algorithmic serendipity within mainstream social media platforms. However, upon entering the sphere of influence of extremist networks, their digital activities became highly orchestrated through remote mentoring, emotional manipulation, and strategic cyber-coaching. This continuous virtual oversight ensures that the subjects remain ideologically pure and operationally focused until the execution of their violent directives. This paradigm shift demonstrates that contemporary lone actors are rarely entirely independent; rather, they are deeply embedded in a virtual command structure that dictates their ideological evolution and operational directives.

The implications of Virtually Directed Radicalization fundamentally challenge traditional counterterrorism paradigms that rely heavily on the disruption of physical organizational hierarchies and face-to-face training camps. Because the facilitation, indoctrination, and operational guidance occur entirely within the clandestine realms of cyberspace, security authorities face unprecedented difficulties in detecting and intercepting these covert relationships. The virtual facilitators exploit the emotional voids of the adolescents, transforming passive consumers of violent propaganda into committed operatives prepared to execute self-directed attacks. This remote guidance mechanism ensures that the ideological and tactical transmission remains continuous, adaptive, and highly resilient against conventional law enforcement interventions. Consequently, understanding the mechanics of this virtual direction is absolutely essential for developing modern, digitally informed prevention and deradicalization strategies.

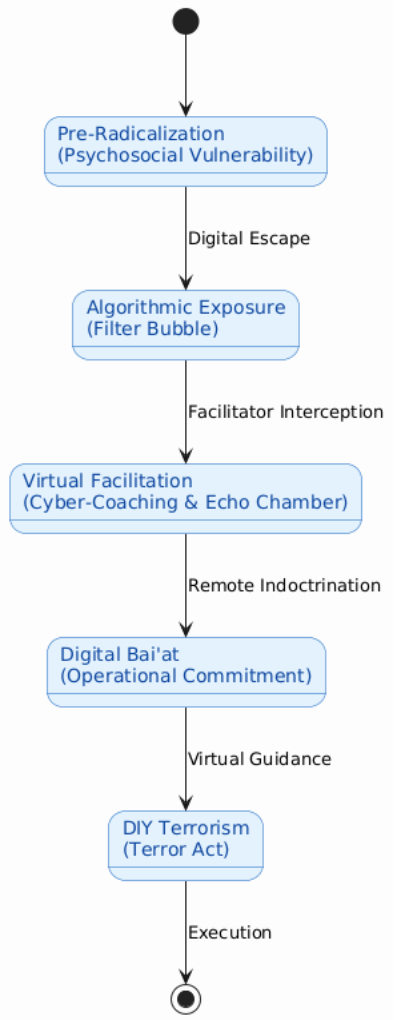

Figure 2. The Virtually Directed Radicalization (VDR) Conceptual Framework

The conceptual framework presented above maps the continuous, remote influence exerted by virtual facilitators throughout the entire radicalization lifecycle of the adolescent subjects. It visually emphasizes that the transition from initial vulnerability to lethal operational capability is

not a spontaneous act of self-radicalization, but a heavily guided process. The diagram highlights the critical nodes where online mentors intervene to exploit algorithmic exposures, deepen echo chamber isolation, and ultimately direct the subjects toward physical violence. By mapping these interconnected stages, researchers and policymakers can better identify the precise intervention points required to dismantle virtual facilitation networks. By illustrating the seamless integration of psychological manipulation and technical instruction, the framework provides a comprehensive model for analyzing how modern digital ecosystems orchestrate terrorist mobilization from a distance.

DISCUSSION

The findings of this study underscore that the pre-radicalization phase among Indonesian adolescents is fundamentally anchored in psychosocial vulnerabilities, such as chronic loneliness, social exclusion, and inadequate parental supervision. These empirical observations strongly align with recent scholarship emphasizing that digital radicalization is rarely an isolated ideological phenomenon but rather a coping mechanism for unmet emotional needs. For instance, Abbas (2024), Frissen (2021), and Harpviken (2019) demonstrated that the pursuit of online extremist materials is often intertwined with underlying psychological distress and a search for identity among young adults. Similarly, Çıtak (2025), Hollewell & Longpré (2022), and Sulfikar (2019) highlighted how self-radicalization among teenagers is frequently catalyzed by social isolation, prompting them to seek surrogate communities online. Furthermore, Byeon (2026) and Grajek et al (2026) confirmed that the interactive effects of digital isolation significantly exacerbate cognitive openings, making vulnerable youth highly receptive to extremist narratives that promise belonging and purpose. Thus, the current study corroborates these findings by illustrating how the subjects' domestic and social deficits created a psychological vacuum that virtual facilitators strategically exploited.

The transition from passive digital consumption to active ideological exposure in this study was heavily mediated by the algorithmic architectures of mainstream platforms like TikTok and YouTube. This trajectory is robustly supported by Kunst et al (2026), Liu et al (2024), Regehr et al (2025), and Yu et al (2024), whose systematic review confirmed that recommendation algorithms systematically funnel users toward increasingly problematic and extreme content based on initial benign interactions. In the context of terrorism, Shaw (2023) noted that platforms like TikTok have become critical pipelines for lone attackers, where algorithmic serendipity rapidly exposes vulnerable users to violent extremist propaganda. The present study extends these observations by demonstrating how these algorithmic filter bubbles specifically target emotionally fragile adolescents, automatically clustering their interests in religious nasheeds or conflict videos into homogeneous extremist ecosystems. Consequently, the findings validate Almeida et al (2025), Rodilosso & Rodilosso (2024), and Zabieno et al (2025) assertion that filter bubbles operate as automated radicalization accelerators, isolating youth from moderate counter-narratives before human recruiters even intervene.

Upon migrating to encrypted communication channels such as Telegram and WhatsApp, the subjects were submerged in intense echo chamber dynamics that rapidly accelerated their identity transformation and out-group antagonism. This progression resonates with Avin et al (2024), Beznosov et al (2022), and Goel et al (2023), who argued that digital echo chambers function as powerful engines for normalizing violence and fostering deep-seated hostility toward out-groups through relentless social validation. The adoption of exclusive terminology and the public display of extremist slogans by the subjects mirror the collective identity formation processes described by Mikhaeil & Baskerville (2024), Binder & Kenyon (2022), Rothut et al (2026), and Valentini et al (2020), who emphasized that online radicalization is deeply embedded in social reinforcement mechanisms rather than mere information consumption. The current study corroborates this by showing that the subjects' willingness to perform symbolic acts of defiance, such as rejecting national symbols, was a direct product of the continuous ideological affirmation received within these closed digital communities. Therefore, the echo chamber effect acts as a critical catalyst, transforming abstract online grievances into concrete, polarized group identities.

A critical contribution of this study is the empirical evidence of adolescents achieving operational readiness for "Do-It-Yourself" (DIY) terrorism entirely within their private bedrooms, challenging traditional assumptions about the necessity of physical training camps. The subjects' abilities to download bomb-making manuals, procure hazardous materials, and assemble functional

explosive devices align with the contemporary shift toward decentralized, digitally facilitated terrorism. Bakirov & Suleimenov (2025), Prasad et al (2025), Stockhammer (2026), and Yaacoub et al (2020) observed that modern lone actors increasingly rely on cyber-coaching and open-source technical tutorials to execute complex attacks without physical organizational support. The present study validates the *Terror Act* stage of the framework proposed by Emezue (2020), Onditi (2021), and Prindani & Syauqillah (2025), demonstrating that digital ecosystems now provide comprehensive operational blueprints that lower the threshold for lethal violence. By documenting how adolescents independently engineered suicide vests and remotely triggered detonators, this research confirms that cyberspace has evolved from a mere propaganda tool into a fully functional, remote operational domain for terrorist mobilization.

Ultimately, the synthesis of these findings necessitates a conceptual shift from the traditional paradigm of autonomous "self-radicalization" toward the framework of Virtually Directed Radicalization (VDR). While previous studies have largely focused on content consumption or operational planning (Stockhammer, 2025; Whittaker, 2022), this study's primary novelty lies in conceptualizing VDR as a comprehensive, lifecycle-spanning mechanism where anonymous virtual facilitators orchestrate the entire psychological and ideological trajectory of vulnerable adolescents. By extending the concept of Virtually Directed Attacks (VDA) from mere tactical execution to holistic identity formation, this research fills a critical gap in the literature regarding how algorithmic vulnerabilities and encrypted echo chambers interact to transform passive digital escapism into active DIY terrorism. Furthermore, it offers a new perspective by empirically demonstrating that the private bedroom has been reconfigured into a clandestine operational domain, challenging the assumption that lone actors operate in complete isolation (Conway, 2017).

The implications of these findings are multifaceted, spanning academic, practical, and policy domains. Academically, the VDR framework provides a robust theoretical lens for future terrorism studies, emphasizing the necessity of integrating algorithmic architecture analysis with psychosocial vulnerability assessments (Elsayed et al., 2025; Klein & Walton, 2024). From a practical and policy perspective, the findings underscore the urgent need for counterterrorism strategies to pivot from reactive content removal to proactive, multi-stakeholder interventions. This includes enhancing family and school-based digital literacy, implementing targeted psychosocial support systems for at-risk youth, and optimizing cyber-patrolling to dismantle virtual facilitation networks rather than merely disrupting individual accounts (Masri-zada et al., 2025). Law enforcement agencies must also develop specialized protocols for investigating DIY terrorism, as the proliferation of open-source technical tutorials drastically lowers the threshold for lethal violence.

To build upon these contributions, future research should explore the long-term efficacy of deradicalization and psychosocial rehabilitation programs specifically tailored for adolescents subjected to VDR. Additionally, comparative cross-cultural studies are recommended to examine how varying levels of internet penetration and domestic supervision influence the VDR trajectory across different geopolitical contexts. Finally, further theoretical development is needed to investigate the role of emerging technologies, such as artificial intelligence and encrypted decentralized platforms, in shaping the next generation of virtually directed extremist ecosystems (Ganaie, 2026).

CONCLUSION

This study concludes that the radicalization trajectory among adolescents has fundamentally evolved from traditional, face-to-face organizational recruitment into a highly structured, digitally mediated process. Through the lens of the *Three Stages of Terrorism Framework*, the findings reveal that psychosocial vulnerabilities—such as chronic loneliness, identity crises, and inadequate parental supervision—create a cognitive opening that drives vulnerable youth toward digital escapism. Once engaged online, algorithmic filter bubbles and encrypted echo chambers systematically isolate these adolescents, exposing them to relentless extremist propaganda and surrogate family-like communities. This digital immersion culminates in the operationalization of "Do-It-Yourself" (DIY) terrorism, where adolescents independently acquire bomb-making capabilities, conduct target planning, and execute online pledges of allegiance (*bai'at*) entirely from the privacy of their bedrooms, effectively transforming domestic spaces into clandestine sites of terrorist mobilization.

Building upon these empirical findings, this research conceptualizes the phenomenon of *Virtually Directed Radicalization* (VDR), challenging the conventional notion of autonomous "self-radicalization." VDR illustrates how the entire radicalization lifecycle is progressively hijacked and orchestrated by anonymous virtual facilitators who exploit emotional voids to guide adolescents from passive content consumption to binding operational commitments. Consequently, contemporary counterterrorism and prevention strategies require a comprehensive paradigm shift that extends beyond mere digital content removal. It is imperative to implement holistic, multi-stakeholder interventions that prioritize early psychosocial support, enhance family and school-based digital literacy, and optimize proactive cyber-patrolling to dismantle the virtual facilitation networks that remotely engineer youth extremism.

REFERENCES

Abbas, A. I. (2024). Modernitas, Globalisasi, dan Realisme Sosial: Perspektif Anthony Giddens Terhadap Perubahan Sosial. *Al-Musthalah: Jurnal Riset Dan Penelitian Multi Disiplin*, *2*. https://doi.org/10.31958/lathaif.v1i1.5926

Abdalla Mikhaeil, C., & Baskerville, R. L. (2024). Explaining online conspiracy theory radicalization: A second-order affordance for identity-driven escalation. *Information Systems Journal*, *34*(3), 711–735. https://doi.org/10.1111/ISJ.12427

Almeida, L. G., Garcia, A. C. B., & Simões, J. E. (2025). Polarisation, filter bubbles and radicalisation on YouTube: a systematic literature review. *International Journal of Web Based Communities*, *21*(4), 324–347. https://doi.org/10.1504/IJWBC.2025.149347

Areeb, Q. M., Nadeem, M., Sohail, S. S., Imam, R., Doctor, F., Himeur, Y., Hussain, A., & Amira, A. (2023). Filter bubbles in recommender systems: Fact or fallacy—A systematic review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *13*(6), e1512. https://doi.org/10.1002/WIDM.1512;WEBSITE:WEBSITE:WIRES;ISSUE:ISSUE:DOI

Avin, C., Daltrophe, H., & Lotker, Z. (2024). On the impossibility of breaking the echo chamber effect in social media using regulation. *Scientific Reports*, *14*(1), 1107. https://doi.org/10.1038/S41598-023-50850-6

Bakirov, A., & Suleimenov, I. (2025). Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare. *Computers 2025, Vol. 14, Page 410*, *14*(10), 410. https://doi.org/10.3390/COMPUTERS14100410

Beznosov, M. A., Анатольевич, Б. М., Golikov, A. S., & Сергеевич, Г. А. (2022). Digital Echo Chambers as Phenomenon of Political Space. *RUDN Journal of Political Science*, *24*(3), 499–516. https://doi.org/10.22363/2313-1438-2022-24-3-499-516

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

Byeon, H. (2026). The impact of social isolation and digital exclusion on mental and physical health in older adults: A meta-analysis. *Medicine*, *105*(4), e46010. https://doi.org/10.1097/MD.0000000000046010

Çıtak, E. (2025). Not that lonely! assessing the “socialization” role of online environment in the radicalization process of lone wolves. *EDPACS*, *70*(10), 14–32. https://doi.org/10.1080/07366981.2025.2492982

Conway, M. (2017). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism*, *40*(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

Elsayed, S., Elsayed, S., Salah, A., Elhenawy, I., & Abdellah, M. (2025). Predicting stock prices using ensemble learning techniques. *International Journal of Electrical and Computer Engineering (IJECE)*, *15*(2), 1783–1792. https://doi.org/10.11591/ijece.v15i2.pp1783-1792

Emezue, C. (2020). Digital or Digitally Delivered Responses to Domestic and Intimate Partner Violence During COVID-19. *JMIR Public Health and Surveillance*, *6*(3), e19831. https://doi.org/10.2196/19831

Frissen, T. (2021). Internet, the Great Radicalizer? Exploring Relationships between Seeking for Online Extremist Materials and Cognitive Radicalization in Young Adults. *Computers in Human Behavior*, *114*, 106549. https://doi.org/10.1016/j.chb.2020.106549

Ganaie, N. A. (2026). The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: deconstructing violent extremism and reimagining counterterrorism in

contemporary digital ecosystems. *Frontiers in Political Science*, *7*, 1718396. https://doi.org/10.3389/FPOS.2025.1718396/TEXT

Goel, V., Sahnan, D., Dutta, S., Bandhakavi, A., & Chakraborty, T. (2023). Hatemongers ride on echo chambers to escalate hate speech diffusion. *PNAS Nexus*, *2*(3), pgad041. https://doi.org/10.1093/PNASNEXUS/PGAD041

Grajek, M., Wagner-Tomaszewska, T., & Jurys, T. (2026). Digital Isolation: The Impact of Social Media and Emerging Technologies on Mental Health. *Healthcare 2026, Vol. 14, Page 1701*, *14*(12), 1701. https://doi.org/10.3390/HEALTHCARE14121701

Harpviken, A. N. (2019). Psychological Vulnerabilities and Extremism Among Western Youth: A Literature Review. *Adolescent Research Review 2019 5:1*, *5*(1), 1–26. https://doi.org/10.1007/S40894-019-00108-Y

Hollewell, G. F., & Longpré, N. (2022). Radicalization in the Social Media Era: Understanding the Relationship between Self-Radicalization and the Internet. *International Journal of Offender Therapy and Comparative Criminology*, *66*(8), 896–913. https://doi.org/10.1177/0306624X211028771;WEBSITE:WEBSITE:SAGE;ISSUE:ISSUE:DOI

Keijzer, M. A., & Mäs, M. (2022). The complex link between filter bubbles and opinion polarization. *Data Science*, *5*(2), 139–166. https://doi.org/10.3233/DS-220054;WEBSITE:WEBSITE:SAGE;REQUESTEDJOURNAL:JOURNAL:DSCA;WGROUP:STRING:PUBLICATION

Klein, E., & Walton, J. (2024). Mapping future work skills in the bachelor of arts: findings from an Australian study. *Higher Education Research and Development*, *43*(1), 104–118. https://doi.org/10.1080/07294360.2023.2228218

Kunst, J. R., Obaidi, M., Gollwitzer, A., Brandtzæg, P. B., Hinrichs, Y., Saini, N., & Schroeder, D. T. (2026). Intelligent Systems, Vulnerable Minds: A Framework for Radicalization to Violence in the Age of AI. *Personality and Social Psychology Review*. https://doi.org/10.1177/10888683261430089;WGROUP:STRING:PUBLICATION

Liu, M., Zhang, H., Liu, M., Chen, D., Zhuang, Z., Wang, X., Zhang, L., Peng, D., & Wang, Q. (2024). Randomizing Human Brain Function Representation for Brain Disease Diagnosis. *IEEE Transactions on Medical Imaging*, *43*(7), 2537–2546. https://doi.org/10.1109/TMI.2024.3368064

Masri-zada, T., Martirosyan, S., Abdou, A., Barbar, R., Kades, S., Makki, H., Haley, G., & Agrawal, D. K. (2025). The Impact of Social Media & Technology on Child and Adolescent Mental Health. *Journal of Psychiatry and Psychiatric Disorders*, *9*(2), 111. https://doi.org/10.26502/jppd.2572-519x0242

Mohiuddin, A. (2023). Islamism in the Digital Age: The Role of Cyberspace in Transforming Religious Authority. *Navigating Religious Authority in Muslim Societies*, 203–236. https://doi.org/10.1007/978-3-031-44825-6_6

Onditi, F. (2021). New Possibilities for a Peaceful Digital Society in Violence Prevalent Geographies. *Journal of Peacebuilding and Development*, *16*(2), 162–178. https://doi.org/10.1177/1542316620958673;PAGE:STRING:ARTICLE/CHAPTER

Polri, D. H. (2026). *Rakernis Densus 88 Soroti Ancaman Ekstremisme Digital Terhadap Anak*.

Prasad, N., Diro, A., Warren, M., & Fernando, M. (2025). A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security*, *157*, 104606. https://doi.org/10.1016/J.COSE.2025.104606

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

Regehr, K., Shaughnessy, C., Zhao, M., Cambazoglu, I., Turner, A., & Shaughnessy, N. (2025). Normalizing toxicity: the role of recommender algorithms for young people's mental health and social wellbeing. *Frontiers in Psychology*, *16*, 1523649. https://doi.org/10.3389/FPSYG.2025.1523649/TEXT

Reyna, C., Bellovary, A., & Harris, K. (2022). The Psychology of White Nationalism: Ambivalence Towards a Changing America. *Social Issues and Policy Review*, *16*(1), 79–124. https://doi.org/10.1111/SIPR.12081;REQUESTEDJOURNAL:JOURNAL:17512409;WGROUP:STRING:PUBLICATION

Rodilosso, E., & Rodilosso, E. (2024). Filter Bubbles and the Unfeeling: How AI for Social Media Can Foster Extremism and Polarization. *Philosophy & Technology 2024 37:2*, *37*(2), 71-. https://doi.org/10.1007/S13347-024-00758-4

Rothut, S., Schulze, H., Hohner, J., Greipl, S., & Rieger, D. (2026). Radicalization and the internet: 25 years of (online) radicalization research. *The Communication Review*. https://doi.org/10.1080/10714421.2026.2658935

Shaw, A. (2023). Social media, extremism, and radicalization. *Science Advances*, *9*(35), eadk2031. https://doi.org/10.1126/SCIADV.ADK2031

Sholehoddin, Azkiya, M. A. Al, Kaloko, I. F., & Chairil, A. (2025). The Dynamics of Transnational Religious Movements on the Resilience of the Pancasila Ideology. *Jurnal Pelita Raya*, *1*(3), 198–214. https://doi.org/10.65586/JPR.V1I3.33

SinPo.id. (2025). *BNPT Temukan 21.199 Konten Radikalisme dan Terorisme Sepanjang 2025*.

Stockhammer, N. (2025). From TikTok to Terrorism? The Online Radicalization of European Lone Attackers since October 7, 2023. *CTC Sentinel*, *18*(7), 16–28.

Stockhammer, N. (2026). *Seven Key Trends of Transnational Terrorism: The Current Threat Matrix for Europe*. 395–422. https://doi.org/10.1007/978-3-658-50490-8_19

Sulfikar, A. (2019). Swa-radikalisasi Melalui Media Sosial di Indonesia. *Jurnal Jurnalisa*, *4*(1). https://doi.org/10.24252/jurnalisa.v4i1.5622

Valentini, D., Lorusso, A. M., & Stephan, A. (2020). Onlife Extremism: Dynamic Integration of Digital and Physical Spaces in Radicalization. *Frontiers in Psychology*, *11*, 481289. https://doi.org/10.3389/FPSYG.2020.00524/TEXT

Walther, S., & Rice, S. (2024). Out-Group Antagonism and Radicalization in Digital Echo Chambers. *Journal of Cyber Extremism*, *12*(2), 45–62.

Whittaker, J. (2022). Rethinking Online Radicalization. *Perspectives on Terrorism*, *16*(4), 27–40.

Widiarni, F., Pratiwi, I., Muda, Y., & Islam Negeri Sultan Syarif Kasim Riau, U. (2024). Dinamika Radikalisme di Dunia Maya: Analisis Tren dan Strategi Pencegahan. *Journal of Education Research*, *5*(3), 3346–3352. https://doi.org/10.37985/JER.V5I3.1274

Windsor, L. (2020). The Language of Radicalization: Female Internet Recruitment to Participation in ISIS Activities. *Terrorism and Political Violence*, *32*(3), 506–538. https://doi.org/10.1080/09546553.2017.1385457

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Examining the Interactive Effects of the Filter Bubble and the Echo Chamber on Radicalization. *Journal of Experimental Criminology*, *19*(1), 119–141. https://doi.org/10.1007/s11292-021-09471-0

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, *77*, 103201. https://doi.org/10.1016/J.MICPRO.2020.103201

Yesilada, M., & Lewandowsky, S. (2022). Systematic Review: YouTube Recommendations and Problematic Content. *Internet Policy Review*, *11*(1), 1–22. https://doi.org/10.14763/2022.1.1652

Yu, X., Haroon, M., Menchen-Trevino, E., & Wojcieszak, M. (2024). Nudging recommendation algorithms increases news consumption and diversity on YouTube. *PNAS Nexus*, *3*(12), pgae518. https://doi.org/10.1093/PNASNEXUS/PGAE518

Zabieno, A. S., Damayanti, D., & Abdullah, A. Z. (2025). The Role of AI, Filter Bubbles, and Echo Chambers in Political and Religious Polarization on Social Media. *Dinamika Penelitian: Media Komunikasi Penelitian Sosial Keagamaan*, *25*(2), 102–118. https://doi.org/10.21274/DINAMIKA.2025.25.2.102-118