Natural Resources for Human Health

eISSN: 2583-1194

Original Research

Received 29 May 2026
Revised 21 June 2026
Accepted 18 July 2026

Natural Resources for Human Health 2026, Vol. 6(9s): 1269–1282

KEYWORDS:
Radicalization, Memetic Violence, True Crime Community, Mixed Unclear Unstable (MUU) Ideology, Victimology, Criminology, Digital Grooming, Early Warning System.

From Victims to Actors: A Dual Criminological and Victimological Perspective on Youth Radicalization in Digital Subcultures

Rifqy Pratama Nugraha

Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia
Email: rifqypn@stik-ptik.ac.id

ABSTRACT: The rapid evolution of the digital landscape has fundamentally transformed the nature of modern terrorism and youth violence. This article explores the intersection of digital ecosystems, human behavior, and crime, utilizing both criminological and victimological frameworks. Through a criminological lens, the study examines the shift from traditional, coherent terrorist doctrines to "Mixed, Unclear, and Unstable" (MUU) ideologies, where personal grievances are fused with fragmented extremist narratives. It investigates the role of the True Crime Community (TCC) and the phenomenon of "memetic violence," illustrating how digital subcultures normalize and celebritize violence. These digital environments serve as echo chambers that accelerate the behavioral escalation from passive content consumption to active radicalization. Concurrently, drawing upon victimological perspectives, the article conceptualizes youths as "victims and actors". It highlights how prior victimization—such as bullying, family dysfunction, and social exclusion—creates psychological vulnerabilities that are systematically exploited by digital grooming and radical networks. Furthermore, the analysis categorizes online threats into Content, Contact, Conduct, and Contract risks, illustrating the multifaceted nature of digital victimization experienced by minors. Ultimately, this article argues that approaching youth radicalization solely through the lens of ideology or punitive law enforcement is insufficient. It advocates against early criminalization, proposing instead a macro-social, trauma-informed early warning system. By integrating family, educational, and community interventions to address the root causes of distress and alienation, the proposed framework aims to build social resilience, protect vulnerable youths, and effectively mitigate the embryonic stages of digital terrorism.

INTRODUCTION

The rapid expansion of mobile connectivity and the ubiquity of digital platforms have fundamentally altered the mechanisms of youth socialization, exposing vulnerable populations to industrialized and gamified forms of online extremism. Indonesia illustrates this dynamic with unusual clarity. Amidst massive digital immersion—where internet penetration reached 79.5 percent of the population, accounting for roughly 221.56 million users by 2024—a developmentally vulnerable demographic of children and adolescents has been increasingly exposed to predatory digital subcultures where violence is celebrated and normalized ((Prasetyo et al., 2026). Recent data from the Indonesian National Police's counter-terrorism squad, Densus 88 Antiteror, revealed that 70 children across 19 provinces were exposed to extremist ideologies through a digital network known as the True Crime Community (TCC) (Prasetyo et al., 2026). The real-world consequences of this digital exposure culminated in recent domestic terror plots, including an attempted bombing at SMAN 72 Jakarta in November 2025 and a Molotov cocktail incident at SMPN 3 Sungai Raya in February 2026 (Prasetyo et al., 2026; Smith, Cadenhead, & Broekaert, 2026).

These developments expose an analytical puzzle that conventional counter-terrorism frameworks and deterrence theories cannot adequately resolve. The Indonesian state has pursued comprehensive suppression and prevention strategies—ranging from digital takedowns by the Ministry of Communication and Digital Affairs to the implementation of the National Action Plan for Preventing and Countering Violent Extremism (RAN PE) (Peraturan Presiden Republik Indonesia Nomor 7 Tahun

2021, 2021). Yet, youth participation in targeted violence and extremist digital ecosystems persists. If these perpetrators behaved as rational, ideologically coherent actors that traditional radicalization models assume, the absence of top-down recruitment from established terror networks like Jemaah Islamiyah or ISIS should have produced widespread disengagement. It did not. Instead, radicalization mutated into an unpredictable phenomenon driven by fame-seeking behaviors, dark humor, and "memetic violence," where perpetrators mimic past mass attackers for digital clout (Prasetyo et al., 2026; Thorleifsson, 2021). Evidence from the SMPN 3 Sungai Raya case showed the 14-year-old perpetrator carrying a backpack inscribed with the hashtag "#ZERODAY" and the names of past transnational mass shooters, treating violence not as a political tool, but as a performative, symbolic language understood by community insiders (Prasetyo et al., 2026).

International and domestic scholarship has examined parts of this evolving problem, though largely in isolation. Terrorism and security studies frame this shift through the emergence of "Mixed, Unclear, and Unstable" (MUU) ideologies (Brace, Baele, & Ging, 2024; Meleagrou-Hitchens & Ayad, 2023). Modern attackers increasingly lack a single, coherent doctrine; instead, they assemble a bespoke collection of beliefs, fusing personal grievances, nihilism, misogyny, and fragmented extremist narratives to justify their actions—a phenomenon recently conceptualized as Composite Violent Extremism (CoVE) (Gartenstein-Ross et al., 2023). Criminological and media research highlights the "gamification of extremism," documenting how leaderboards, achievement systems, and the aestheticization of violence lower moral barriers (Schlegel & Kowert, 2024). This literature distinguishes between "top-down" gamification used strategically by terror groups and "bottom-up" gamification where decentralized youths utilize virtual scoreboards and "body counts" to turn mass violence into a competitive spectacle (Schlegel, 2021).

Concurrently, victimological and psychological work applies the concept of the "victim-offender overlap," demonstrating that offending and victimization are intimately linked; victims of bullying, family dysfunction, and social exclusion are at a statistically higher risk of offending as an adaptive coping mechanism (Berg & Mulford, 2017; Jennings, Piquero, & Reingle, 2012). The perpetrators in the Indonesian cases, for instance, were deeply affected by severe bullying (*perundungan*) and family pressure, highlighting that psychosocial trauma often precedes radicalization (Prasetyo et al., 2026). This is further supported by recent reviews emphasizing the role of Adverse Childhood Experiences (ACEs) and trauma in creating psychological vulnerabilities to extremism (Lewis, Marsden, Hewitt, & Peterscheck, 2024; Rousseau et al., 2019). Furthermore, public-health and child-protection research maps the demand side of this digital engagement by categorizing the online vulnerabilities of minors into Content, Contact, Conduct, and Contract risks—known as the 4Cs (Livingstone & Stoilova, 2021).

These literatures rarely speak to one another. Security studies seldom incorporate the developmental victimology of child trauma; victimological analyses rarely engage with the socio-technical affordances of gamified extremism; and public-health reporting is often disconnected from the specific ideological fluidity (MUU) that generates the supply of extremist content. The result is a fragmented evidence base that explains components of the phenomenon without modeling their interaction, often leading to a false dichotomy that treats these youths either strictly as autonomous terrorists or purely as passive victims of the internet (Corner & Gill, 2015). Indonesia-specific work compounds the gap by leaning on traditional ideological profiling rather than reconciling how localized trauma interacts with transnational digital subcultures.

This study addresses both problems by integrating the criminological and victimological disciplines. By treating the empirical data from the SMAN 72 and SMPN 3 Sungai Raya cases (Prasetyo et al., 2026) as evidence to be adjudicated rather than smoothed over, this article constructs a comprehensive model of the "victim-to-actor" pipeline. Ultimately, this article argues that countering modern youth extremism requires moving beyond punitive deterrence, proposing instead a macro-social, trauma-informed early warning system that addresses the root vulnerabilities systematically exploited by gamified digital environments.

LITERATURE REVIEW

To effectively unpack the contemporary mechanisms of youth radicalization in digital subcultures, this study integrates two traditionally separate disciplines: Criminology and Victimology. Criminology provides the framework for understanding the evolution of extremist ideologies and the sociotechnical mechanisms—such as gamification—that incentivize violent behavior1. Conversely, Victimology offers a critical lens on the psychosocial vulnerabilities and developmental traumas that push youths into these predatory digital ecosystems in the first place.

3.1. Criminological Perspectives: Ideological Fluidity and the Gamification of Violence

Traditionally, criminological and security frameworks have relied on examining violent extremism through the lens of coherent, top-down ideological doctrines propagated by established organizations, such as Al-Qaeda or formal neo-Nazi networks (Astley, 2025). However, contemporary criminology faces an epistemological crisis: the internet has catalyzed a post-organizational dynamic where hierarchical command structures have been largely supplanted by decentralized, horizontal networks (Astley, 2025; Meleagrou-Hitchens & Ayad, 2023). Within these digital ecosystems, ideology is no longer a rigid prerequisite for radicalization. Instead, it functions as a highly mutable, personalized construct. As Prasetyo, Hartono, and Prasetyo (2026) observe, the character of the terror threat has shifted fundamentally from structural command to individual activation; modern actors are often co-opted by algorithms and digital echo chambers rather than through physical indoctrination or formal pledges of allegiance (baiat). To fully comprehend this paradigm shift, it is necessary to examine how ideological fluidity intersects with the socio-technical mechanisms of the internet—specifically, how the gamification of violence lowers moral barriers and transforms mass casualties into performative, participatory acts.

Here is the revised, detailed, and critical draft of **Section 3.1: Criminological Perspectives: Ideological Fluidity and the Gamification of Violence**, fully updated to incorporate the in-text citations from the provided literature and explicitly integrating the empirical insights from your book (Prasetyo et al., 2026).

3.1. Criminological Perspectives: Ideological Fluidity and the Gamification of Violence

Traditionally, criminological and security frameworks have relied on examining violent extremism through the lens of coherent, top-down ideological doctrines propagated by established organizations, such as Al-Qaeda or formal neo-Nazi networks (Astley, 2025). However, contemporary criminology faces an epistemological crisis: the internet has catalyzed a post-organizational dynamic where hierarchical command structures have been largely supplanted by decentralized, horizontal networks (Astley, 2025; Meleagrou-Hitchens & Ayad, 2023). Within these digital ecosystems, ideology is no longer a rigid prerequisite for radicalization. Instead, it functions as a highly mutable, personalized construct. As Prasetyo, Hartono, and Prasetyo (2026) observe, the character of the terror threat has shifted fundamentally from structural command to individual activation; modern actors are often co-opted by algorithms and digital echo chambers rather than through physical indoctrination or formal pledges of allegiance (*baiat*). To fully comprehend this paradigm shift, it is necessary to examine how ideological fluidity intersects with the socio-technical mechanisms of the internet—specifically, how the gamification of violence lowers moral barriers and transforms mass casualties into performative, participatory acts.

3.1.1. The End of Ideological Purity: MUU Ideologies and Composite Violent Extremism

The contemporary threat landscape is increasingly dominated by individuals who operate without a discernible, singular political or religious manifesto. In recognition of this, counter-terrorism practitioners introduced the category of "Mixed, Unclear, and Unstable" (MUU) ideologies to classify individuals who amalgamate disparate ideological elements, shift between belief systems, or possess no coherent ideology despite posing a severe terrorism risk (Astley, 2025). Scholars characterize this era as the "Age of Incoherence," noting that modern extremists assemble a bespoke "salad bar" of beliefs that often conflict with one another, using them merely as a veneer to justify personal grievances (Meleagrou-Hitchens & Ayad, 2023).

To provide necessary conceptual clarity, Gartenstein-Ross et al. (2023) developed the Composite Violent Extremism (CoVE) framework, arguing that ideological amalgamation is not an anomaly but a distinct, categorizable threat. The CoVE framework disaggregates this phenomenon into four subtypes: ambiguous (harboring disparate prejudices without a discernible ideological framework), mixed (adhering to multiple ideologies on relatively equal footing), fused (orienting around one core ideology while expressing sentiments of another), and convergent (cooperating with differently aligned individuals for mutual interests) (Gartenstein-Ross et al., 2023).

This ideological blurring is heavily driven by the affordances of digital platforms. Brace, Baele, and Ging (2024) posit that MUU ideologies do not emerge in a vacuum but are the direct result of the technological affordance of algorithmic outlinking (or "exolinks"). In the decentralized Web 2.0, platform algorithms and user-shared hyperlinks actively cross-pollinate ideas, dragging individuals from one ideological echo chamber into another. Consequently, individuals engage in "fringe fluidity," transitioning smoothly between seemingly oppositional extremist networks, such as blending white supremacy with misogynistic "incel" narratives or neo-Nazi aesthetics with Salafi-jihadism (Gartenstein-Ross & Blackman, 2022; Meleagrou-Hitchens & Ayad, 2023; Bekti et al., 2025). Prasetyo et al. (2026) validate this socio-technical perspective in the Indonesian context, noting

that platform algorithms create an "architecture of acceleration" (*arsitektur akselerasi*) that funnels marginalized youths toward increasingly extreme, composite content. Under this framework, ideology is no longer the ultimate driver of violence; rather, it is a retroactive justification curated from a digital menu to rationalize a pre-existing desire for destruction, notoriety, or revenge (Astley, 2025).

3.1.2. Bottom-Up Gamification and Participatory Memetic Violence

As ideological canons become fragmented, the pursuit of violence itself often supersedes any strategic political goal. This shift is deeply intertwined with the "gamification of extremism," defined as the use of game-design elements in non-game contexts to facilitate behavioral change and drive sustained engagement (Schlegel, 2020). While top-down gamification involves extremist organizations strategically deploying mobile applications, badges, and reputation meters to indoctrinate recruits (e.g., ISIS's Huroof app or the Identitarian Movement's planned Patriot Peer app), contemporary youth radicalization is overwhelmingly characterized by bottom-up gamification (Schlegel, 2021).

Bottom-up gamification emerges organically within obscure message boards (e.g., 4chan, 8kun) and gaming-adjacent communication platforms like Discord and Telegram. Within these spaces, localized violence is transformed into a global, competitive spectacle. This phenomenon was epitomized by the 2019 Christchurch attack, which fundamentally altered the "cultural script" for mass violence (Lakhani & Wiedlitzka, 2022; Prasetyo et al., 2026). The attacker deliberately mirrored the aesthetic of a First-Person Shooter (FPS) game using a helmet-mounted camera and livestreamed the atrocity, mirroring the popular "Let's Play" video format (Lakhani & Wiedlitzka, 2022). Concurrently, digital audiences spectating the attack utilized virtual leaderboards to track the "body count," actively urging the perpetrator to "get the high score" (Lakhani & Wiedlitzka, 2022).

This gamification effectively lowers moral barriers by immersing users in what Thorleifsson (2021) identifies as "play frames"—environments where horrific acts are treated as simultaneously serious and non-serious, masked heavily in dark irony, memes, and subcultural slang. By treating mass murder as an interactive game, perpetrators achieve profound psychological and moral disengagement.

Furthermore, this dynamic has birthed what researchers categorize as participatory memetic violence, which is highly prevalent within the True Crime Community (TCC) (Smith, Cadenhead, & Broekaert, 2026). In these layered online fandoms, past mass shooters are elevated to the status of cultural icons or "saints." Violence ceases to be a political tool and instead functions as a performative, symbolic language understood only by subcultural insiders (Smith et al., 2026). As Prasetyo et al. (2026) demonstrate empirically, when modern youths commit atrocities—such as the actors in the Indonesian SMAN 72 and SMPN 3 Sungai Raya plots—they purposefully replicate the clothing, weapon inscriptions, and selfie poses of past shooters. Their primary objective is not ideological revolution, but the exploitation of an "attention architecture" (*arsitektur atensi*) to secure validation, fame, and their own legacy on digital leaderboards among their peers (Prasetyo et al., 2026).

3.2. Victimological Perspectives: Trauma, the 4C Risks, and the Victim-Offender Overlap

While criminological frameworks elucidate the structural incentives and ideological fluidity of digital subcultures, victimology provides the necessary psychosocial lens to understand *why* youths are drawn into these predatory ecosystems. To fully conceptualize the "victim-to-actor" pipeline, it is imperative to move beyond the false dichotomy that treats youths either as autonomous terrorists or as passive targets of digital propaganda. As Prasetyo, Hartono, and Prasetyo (2026) conceptualize, the risk of child radicalization does not emerge from a single cause, but rather from the intersection of life-course experiences, personal vulnerabilities, and exposure to radicalizing digital environments. A comprehensive understanding requires analyzing the victim-offender overlap, the developmental impact of trauma, and the specific matrix of digital vulnerabilities that exploit these offline grievances.

3.2.1. The Victim-Offender Overlap and its Digital Applicability

A robust body of empirical research in victimology and criminology has consistently demonstrated that offending and victimization are not mutually exclusive categories; rather, they are deeply intertwined. The "victim-offender overlap" posits that the majority of violent offenders possess extensive histories of prior victimization, and conversely, that victims of violence face a statistically heightened risk of future offending (Berg & Mulford, 2017; Jennings et al., 2012). Historically, theoretical explanations for this overlap have relied on routine activities theory and the "code of the street," suggesting that individuals

residing in disadvantaged environments often adopt aggressive postures as an adaptive coping mechanism to prevent further victimization (Berg & Mulford, 2017).

However, traditional theories of the victim-offender overlap remain under-theorized in the context of digital radicalization. In the physical world, the overlap is largely dictated by spatial proximity to violence; in the digital realm, the overlap manifests psychologically. Prasetyo et al. (2026) emphasize that marginalized youths who suffer from offline victimization—such as severe bullying (*perundungan*), social exclusion, or familial dysfunction—often seek refuge in digital subcultures to cope with real-world strain. Toxic online environments, such as the True Crime Community (TCC), offer these victims a sense of belonging, status, and empowerment. The TCC is not merely a community of content consumers; it is a gathering place for youths seeking meaning, identity, and a shelter for their "social wounds" (Prasetyo et al., 2026). By adopting the gamified, violent norms of these digital subcultures, youths transition from being victims of offline adversity to active perpetrators (actors) of online harassment and targeted physical violence, reclaiming a sense of power that was stripped from them during their initial victimization.

3.2.2. Trauma and Adverse Childhood Experiences (ACEs) in Radicalization

The pathway into extremist subcultures is frequently paved by developmental trauma. Contemporary research emphasizes that exposure to Adverse Childhood Experiences (ACEs)—such as emotional and physical abuse, neglect, family dysfunction, and severe bullying—plays a critical role in radicalization (Lewis et al., 2024). A seminal study by Windisch et al. (2020) found that 63% of former white supremacists had experienced four or more ACEs during their formative years—a rate significantly higher than the general population and comparable only to high-risk juvenile offenders. Similarly, Simi et al. (2016) demonstrated that childhood adversity acts as a "conditioning experience" that incrementally increases a person's susceptibility to violent extremism.

Trauma creates what radicalization scholars term a "quest for significance," wherein a profound loss of personal significance motivates the individual to restore it through extreme means (Jasko et al., 2017). Prasetyo et al. (2026) contextualize this within the Indonesian setting, noting that "social crises"—such as parental divorce, parental stress, lack of emotional attention at home, and early exposure to pornography—create deep affective vacuums and psychological disorientation. Extremist digital networks weaponize this trauma. They deliberately exploit the emotional voids of vulnerable youths, reframing their personal experiences of marginalization as part of a broader, collective grievance. By providing a subculture that validates their anger, these communities effectively channel offline trauma into radicalized action.

3.2.3. The 4C Framework of Digital Vulnerability

To systematically map how offline trauma is exploited within digital ecosystems, this study utilizes the "4Cs" classification of online risk developed by Livingstone and Stoilova (2021). This framework, which is also heavily utilized by Prasetyo et al. (2026) to evaluate Indonesian youth vulnerabilities, categorizes the multifaceted nature of digital victimization:

1. **Content Risks:** This occurs when a child engages with or is passively exposed to harmful material (Livingstone & Stoilova, 2021). For traumatized youths, this involves exposure to violent, gory, or extremist content. In the context of the TCC, it involves consuming highly aestheticized edits of mass shooters, which systematically desensitize the viewer to human suffering and normalize extreme violence (Prasetyo et al., 2026).
2. **Contact Risks:** This risk arises when a child experiences or is targeted by harmful adult-initiated or peer-initiated interactions (Livingstone & Stoilova, 2021). Traumatized youths seeking validation are highly susceptible to digital grooming, ideological persuasion, and extremist recruitment via gaming-adjacent platforms, transforming their vulnerability into a pathway for exploitation (Prasetyo et al., 2026).
3. **Conduct Risks:** This manifests when the child transitions from a passive consumer to an active participant, witnessing or engaging in potentially harmful peer conduct (Livingstone & Stoilova, 2021). This includes participating in cyberbullying, coordinated "raids" against out-groups, or mimicking the transgressive, gamified behaviors celebrated by extremist subcultures. It is within this category that the victim-offender overlap explicitly materializes in the digital space.
4. **Contract Risks:** This dimension encompasses the ways in which children are exploited by the structural and transactional design of digital platforms (Livingstone & Stoilova, 2021). Through algorithmic profiling and datafication, platform recommendation systems create "filter bubbles" that continuously push vulnerable youths toward increasingly extreme content, maximizing engagement at the cost of the user's psychosocial well-being (Prasetyo et al., 2026).

By integrating the 4C framework with the victim-offender overlap, a coherent trajectory emerges. Offline trauma and ACEs render a youth psychologically vulnerable. When this youth enters the digital sphere, they are subjected to *Contract* risks (algorithmic steering) that expose them to extreme *Content*. As they engage with this material, they encounter *Contact* risks from radicalized peers who offer them validation and a sense of belonging. Finally, to secure their status within this new community, the youth partakes in *Conduct* risks, adopting extremist ideologies and engaging in memetic violence. Through this socio-technical pipeline, the victim is seamlessly transformed into an actor of terror.

METHODOLOGY

Researching modern youth radicalization presents severe methodological and epistemological challenges. Traditional studies on extremism often suffer from "dark figures"—under-reported activities or attitudes that fail to capture the full prevalence of specific behaviors among the target population (Clemmow et al., 2020). Furthermore, investigating minors in encrypted or obscure digital environments involves stringent ethical constraints and a lack of reliable baseline data, while relying exclusively on open-source media reports risks introducing editorial and selection biases (Freilich & LaFree, 2016; Lewis et al., 2024). To overcome these limitations, this study adopts a qualitative, mixed-methods research design that combines multiple case study analysis, expert interviews, and Open-Source Intelligence (OSINT).

4.1. Research Design

This study employs a qualitative, mixed-methods approach grounded in a constructivist epistemology (Liu & Matthews, 2005; Winner, 1993, as cited in Allchorn & Orofino, 2025). This design is particularly suited for studying "hard-to-reach" populations, such as radicalized youths operating within obscure digital ecosystems (Clemmow et al., 2022).

To capture the complex interplay between offline trauma and online gamified extremism, this study utilizes a multiple case study design. The case study method enables an in-depth, contextualized understanding of how "Mixed, Unclear, and Unstable" (MUU) ideologies and participatory memetic violence materialize in specific, real-world events. As Prasetyo, Hartono, and Prasetyo (2026) argue, understanding the "global-local" nexus of modern terrorism requires research that bridges abstract theories with actual institutional experiences and threat assessments. Therefore, this research design actively seeks to integrate digital ethnography—observing the sociotechnical affordances of platforms (Baele, Brace, & Coan, 2020)—with the traditional criminological and psychological analysis of offline criminal behavior.

4.2. Data Collection Strategies

To ensure the reliability and validity of the findings, the study employed a data triangulation strategy, combining multiple sources of evidence to mitigate the inherent biases of using a single data stream (Farmer et al., 2006; Lewis & Marsden, 2024). Data collection was divided into three primary streams:

4.2.1. Primary Data: Expert Consultations and Law Enforcement Insights

Given the closed nature of ongoing terrorism investigations involving minors, primary qualitative data were gathered through in-depth consultations and semi-structured interviews with subject matter experts. Drawing from the empirical foundation established by Prasetyo et al. (2026), these consultations included practitioners from the Directorate of Intelligence of Densus 88 Antiteror Polri, forensic psychologists, and digital media analysts (such as Drone Emprit). These interviews were critical for moving the analysis from theoretical assumptions to actual threat readings, revealing, for example, that 70 children across 19 Indonesian provinces had been exposed to extremist content and digital grooming through the True Crime Community (TCC) (Divisi Humas Polri, 2026; Prasetyo et al., 2026). This primary data stream allowed the researchers to establish the psychosocial baselines of the youths, noting prevalent factors like severe perundungan (bullying) and family dysfunction.

4.2.2. Secondary Data: Empirical Case Studies

The study focuses on two recent, high-profile cases of youth extremism in Indonesia as its primary units of analysis (Prasetyo et al., 2026):

1. **The SMAN 72 Jakarta Incident (November 2025):** An attempted bomb plot carried out by a 17-year-old student, heavily motivated by a combination of social exclusion, offline grievances, and deep immersion in TCC digital networks.
2. **The SMPN 3 Sungai Raya Incident (February 2026):** A Molotov cocktail attack plotted by a 14-**year**-old junior high school student in West Kalimantan. The perpetrator's belongings featured explicit TCC symbology, the hashtag

"#ZERODAY", and the names of past transnational mass shooters, directly illustrating the phenomenon of memetic violence.

Data for these cases were compiled using official police press releases, investigative documents, and verified national media reports. Utilizing multiple source types (e.g., cross-referencing media reports with expert police insights) helps construct a robust behavioral timeline of the perpetrators while minimizing the vagaries of media sensationalism (Gill et al., 2017; Schuurman, 2020).

4.2.3. Digital Ethnography and Open-Source Intelligence (OSINT)

To understand the digital ecosystems that influenced the perpetrators, the study employed Open-Source Intelligence (OSINT) gathering techniques. Prospective attackers frequently engage in "leakage"—the tendency to communicate violent intentions or affiliations online prior to committing an act of violence. By tracing the digital footprints of the perpetrators across platforms like TikTok, Discord, Telegram, and WhatsApp, the researchers analyzed the specific aesthetic edits, hashtags, and memetic violence scripts the youths consumed and produced (Prasetyo et al., 2026). This digital ethnographic approach is critical for observing how bottom-up gamification operates organically within dark fandoms and how the "affordances" of platforms accelerate the radicalization process (Allchorn & Orofino, 2025; Risius et al., 2024).

4.3. Data Analysis Strategy

The collected data—comprising interview transcripts, case documents, and digital artifacts—were analyzed using a reflexive thematic analysis framework (Braun & Clarke, 2006, 2022). The coding process utilized a hybrid deductive and inductive approach:

- **Deductive Coding:** The data were mapped against established theoretical frameworks. The psychosocial vulnerabilities and online experiences of the perpetrators were categorized using Livingstone and Stoilova's (2021) **4C Framework** (Content, Contact, Conduct, and Contract risks). The ideological motivations of the perpetrators were assessed using the **Composite Violent Extremism (CoVE)** typologies developed by Gartenstein-Ross et al. (2023). Furthermore, the escalation from psychological trauma to offline action was analyzed using Moghaddam's (2005) **Staircase to Terrorism** model, functioning as a diagnostic tool to read the escalation of moral disengagement (Prasetyo et al., 2026).
- **Inductive Coding:** New themes were allowed to emerge organically from the data, particularly concerning localized Indonesian socio-cultural dynamics, the specific mechanisms of digital **grooming** in gaming-adjacent platforms, and the conceptualization of the TCC as an "affective enclosure" (*ruang afektif*) where marginalized youths seek validation for their anger (Prasetyo et al., 2026).

4.4. Limitations and Ethical Considerations

Several methodological limitations must be acknowledged. First, the reliance on open-source data and media reporting introduces potential selection biases, as non-violent extremists or unsuccessful plots rarely receive equal public or academic attention (Freilich & LaFree, 2016; Gill et al., 2017). To mitigate this, the study deliberately prioritized primary data from expert consultations (Densus 88 and psychologists) to corroborate the OSINT findings.

Ethically, studying youth radicalization and TCC networks involves engaging with highly sensitive, graphic, and potentially traumatizing material, as well as handling the data of minors (British Psychological Society, 2021). All empirical data utilized in this study were strictly anonymized to protect the identities of the juvenile perpetrators and victims. Furthermore, the analysis deliberately avoids reproducing specific extremist manifestos or highly graphic imagery to prevent the inadvertent glorification, "celebrification," or memetic amplification of the attackers—a known risk when researching performative violence (Helfgott, 2015; Prasetyo et al., 2026; Schildkraut et al., 2021).

DISCUSSION

The empirical examination of the SMAN 72 Jakarta and SMPN 3 Sungai Raya cases provides critical insights into the evolving nature of youth extremism. By situating these incidents within the intersecting frameworks of Criminology and Victimology, this discussion elucidates how the digital ecosystem facilitates the transition from psychosocial victimhood to violent action. The findings necessitate a profound reassessment of traditional radicalization models, ideological categorizations, and the punitive strategies predominantly employed by state security apparatuses.

5.1. The Empirical Manifestation of Memetic Violence and the TCC

The Indonesian case studies critically validate the criminological shift away from coherent, organizationally directed terrorism toward decentralized, "participatory memetic violence" (Smith, Cadenhead, & Broekaert, 2026). Neither the 17-year-old suspect at SMAN 72 nor the 14-year-old student at SMPN 3 Sungai Raya adhered to the traditional doctrines of established regional terror networks like Jemaah Islamiyah. Instead, their actions were fundamentally intertwined with the True Crime Community (TCC).

As Prasetyo, Hartono, and Prasetyo (2026) empirically demonstrate, the TCC operates as a subculture where the "celebrification of perpetrators" (selebritisasi pelaku) replaces the condemnation of violence. The perpetrators consumed and reproduced highly aestheticized edits of transnational mass shooters, utilizing violence not as a means to achieve political hegemony, but as a symbolic language to secure digital notoriety. This exemplifies what Schlegel (2021) defines as bottom-up gamification, where localized violence is transformed into a competitive spectacle.

Crucially, Prasetyo et al. (2026) argue that memetic violence is not merely mechanical imitation or a simple "copycat effect." Rather, it is the cultural transmission of violence scripts—where aesthetics, manifestos, and weapon inscriptions (such as the "#ZERODAY" tag found in the SMPN 3 Sungai Raya case) are organically imported, modified, and weaponized to express localized grievances. By cloaking extreme violence in dark humor, irony, and gamified metrics (such as "body counts" and virtual leaderboards), these platforms systematically erode moral barriers and facilitate moral disengagement, allowing youths to replicate atrocities while psychologically distancing themselves from the real-world consequences (Lakhani & Wiedlitzka, 2022; Thorleifsson, 2021).

5.2. Rethinking Radicalization: The Digital Staircase and MUU Ideologies

The phenomena observed in this study challenge the linear assumptions of classical radicalization theories, most notably Moghaddam's (2005) "Staircase to Terrorism". In traditional models, radicalization is conceptualized as a sequential climb where individuals gradually adopt rigid ideological justifications before committing acts of violence. However, Prasetyo et al. (2026) emphasize that while the psychological mechanism of the staircase—such as the narrowing of options and the dehumanization of targets—remains relevant, the digital realities of modern extremism expedite the process by removing the need for a coherent ideology.

Driven by the technological affordances of algorithmic outlinking and digital cross-pollination, modern youths exhibit "Mixed, Unclear, and Unstable" (MUU) ideologies (Brace, Baele, & Ging, 2024; Meleagrou-Hitchens & Ayad, 2023). Their belief systems are fluid composites of personal grievances, nihilism, and varying extremist tropes curated from a digital "salad bar" (Gartenstein-Ross et al., 2023). Because ideological purity is no longer a prerequisite for violence in subcultures like the TCC, the traditional radicalization staircase is effectively compressed. A youth can rapidly escalate from passive consumption of gore content to active attack preparation simply to gain clout among digital peers, bypassing the deep ideological indoctrination historically required by top-down terror networks (Prasetyo et al., 2026).

5.3. Validating the Victim-Offender Overlap in the Digital Sphere

While criminological analysis explains the mechanisms of gamified violence, victimological frameworks are essential for understanding the psychosocial vulnerabilities that initiate this trajectory. The empirical data strongly support the applicability of the victim-offender overlap within the digital radicalization pipeline (Berg & Mulford, 2017; Jennings, Piquero, & Reingle, 2012).

The perpetrators in both Indonesian cases possessed extensive histories of prior offline victimization, characterized by severe peer bullying (perundungan), social exclusion, and familial dysfunction. According to general strain theory, such Adverse Childhood Experiences (ACEs) create profound psychological voids and a loss of significance (Jasko, LaFree, & Kruglanski, 2017). Finding no protective offline environment, these youths sought refuge in the digital sphere, where they were immediately subjected to the 4C risks: Content, Contact, Conduct, and Contract risks (Livingstone & Stoilova, 2021; Prasetyo et al., 2026).

Prasetyo et al. (2026) aptly conceptualize the TCC as an "affective enclosure" (ruang afektif) that weaponizes this trauma. By offering a supportive—albeit toxic—community that validates their anger and celebrates retribution, these digital networks provide a maladaptive coping mechanism. The youths transition from being victims of offline marginalization to actors of online and offline terror, adopting the violent norms of their new digital in-group to reclaim a sense of agency. This confirms

that modern youth extremism cannot be fully understood or mitigated without first acknowledging the foundational trauma of the perpetrator.

5.4. Critiquing Punitive Frameworks and Deterrence Theory

The integration of the MUU phenomenon and the victim-offender overlap exposes significant flaws in conventional, punitive counter-terrorism frameworks. Deterrence theory relies on the assumption that actors are rational and will alter their behavior in response to the threat of legal sanctions. However, traumatized adolescents operating within gamified echo chambers do not behave as rational, information-responsive actors.

For these youths, the threat of law enforcement intervention or societal condemnation is frequently outweighed by the immediate psychosocial rewards of peer validation and digital infamy. In some instances, the prospect of notoriety or "martyrdom" within the TCC actively incentivizes the violence (Smith et al., 2026). Consequently, relying primarily on aggressive suppression strategies, early criminalization, or internet blocking is fundamentally insufficient. As Prasetyo et al. (2026) argue, treating traumatized, indoctrinated minors strictly through the lens of the criminal justice system ignores their developmental immaturity and fundamental victimhood. It risks further alienating them, reinforcing their anti-social narratives, and exacerbating the very grievances that drove them to extremism. Instead, the manifestation of MUU ideologies and memetic violence must be treated concurrently as a public health and child protection crisis (Lewis, Marsden, Stefaniak, & Hewitt, 2025).

5.5. Theoretical Tensions and Counterarguments

While the synthesis of Criminology and Victimology provides a compelling framework to understand modern youth radicalization—particularly in cases like the SMAN 72 Jakarta and SMPN 3 Sungai Raya incidents—it is imperative to address the theoretical tensions inherent in this approach. Scholars have raised rigorous critiques regarding technological determinism, the risk of depoliticizing extremist actors by over-emphasizing psychological trauma, and the empirical validity and ethical implications of Preventative/Countering Violent Extremism (P/CVE) interventions. Addressing these counterarguments is essential for constructing a robust and deeply critical understanding of the phenomenon.

5.5.1. The Limits of Technological Determinism: Gaming vs. Radicalization

A primary critique of the current digital radicalization discourse is its tendency to overstate the causal power of the internet and gamification. Critics argue that linking video games, gaming-adjacent platforms (e.g., Discord, Twitch), or gamified mechanics directly to violent extremism risks falling into technological determinism. There is a significant absence of empirical evidence to substantiate a definitive causal relationship between exposure to video games—even violent ones—and adverse effects such as radicalization or real-world aggression. The American Psychological Association explicitly concluded that attributing societal violence to video gaming is scientifically unsound and draws attention away from more complex, intersecting psychosocial factors.

Furthermore, scholars caution that gamification is not a "magic bullet" capable of unilaterally altering behavior simply by introducing virtual points, badges, or leaderboards. Treating "online radicalization" as an isolated process creates a false dichotomy that ignores the primacy of offline interactions. Empirical databases of convicted terrorists demonstrate that radicalization is rarely exclusively digital; the internet acts as an "enabler" or "facilitator" that complements, rather than substitutes, face-to-face interactions and offline grievances. Internet philosophers increasingly describe this dynamic as the "Onlife" continuum, arguing that digital and physical milieus are seamlessly integrated and cannot be demarcated into entirely separate domains of radicalization.

While acknowledging these critiques, this study posits that gamification does not cause terrorism ex nihilo. Instead, the gamified infrastructure of subcultures like the True Crime Community (TCC) provides a potent "cultural script" and performative language. Extremists often use gaming platforms organically rather than strategically, leveraging their immense pop-cultural appeal to reach target demographics where they already congregate. In the empirical cases examined by Prasetyo et al. (2026), digital platforms did not create the perpetrators' underlying grievances; rather, they provided an "attention architecture" (*arsitektur atensi*) that weaponized their pre-existing offline vulnerabilities, offering notoriety as a reward for transgressive action.

5.5.2. Trauma, Mental Health, and the Risk of Depoliticization

A second major theoretical tension challenges the reliance on trauma, mental health, and the victim-offender overlap to explain violent extremism. Criminological and epidemiological research notes that trauma or Adverse Childhood Experiences (ACEs)

alone offer an insufficient explanation for radicalization, as the vast majority of individuals exposed to trauma or abuse do not suffer from long-term toxic stress, and even fewer progress to violent extremism. Furthermore, extensive forensic analyses have repeatedly shown that terrorists operating within group structures rarely exhibit higher rates of diagnosed mental illness than the general population, although mental health disorders do appear more prevalently among lone-actor terrorists.

Moreover, critical terrorism scholars argue that overly relying on psychological trauma, individual vulnerabilities, and "resilience-building" has a profoundly "depoliticizing effect". By treating radicalized youths strictly as traumatized victims who require therapeutic adaptation to fit the existing social order, this framework risks stripping them of their political agency. It conveniently relieves the state of its responsibility to address systemic injustices, socio-economic marginalization, or discriminatory policies (such as anti-Muslim foreign policy or institutional racism) that may be the genuine root causes of their grievances.

However, integrating the victim-offender overlap does not absolve the actor of agency, nor does it dismiss the systemic dimensions of their actions. Rather, trauma functions as a "conditioning experience" that initiates a "quest for significance," making the individual highly susceptible to alternative, extreme narratives that offer empowerment, belonging, and a clear target for their anger. Acknowledging victimhood is not about pathologizing the actor; it is about understanding the precise psychosocial voids that extremist subcultures exploit to reframe personal alienation into collective, violent action.

5.5.3. The Securitization of Care and the Efficacy of P/CVE

Finally, the advocacy for non-punitive, Preventative/Countering Violent Extremism (P/CVE) and trauma-informed interventions faces intense methodological and sociological scrutiny. Methodologically, the P/CVE field has long struggled with a profound lack of rigorous, independent evaluation standards. Measuring the success of preventative programs fundamentally relies on "measuring a negative"—assessing whether an act of violent extremism was successfully averted because of the intervention. Because terrorism has an extremely low base rate, distinguishing between genuine intervention success and individuals who naturally desisted is highly problematic.

Sociologically, the P/CVE agenda has been fiercely criticized for expanding the security apparatus into the realms of education, social work, and healthcare. Critics argue that preventative policies deployed by the state often result in pre-oppressive measures, termed "prepression," which can inadvertently stigmatize marginalized groups. In the UK, for instance, the Prevent strategy has been repeatedly criticized for creating a "suspect community" dynamic, disproportionately securitizing Muslim populations, and blurring the lines between safeguarding and state surveillance. When social cohesion or mental health services are co-opted under a counter-terrorism umbrella, individuals experiencing trauma or alienation may avoid seeking help out of fear of criminalization.

These valid concerns underscore precisely why traditional, securitized P/CVE models must be fundamentally reformed. Interventions aimed at minors entangled in MUU ideologies must be genuinely trauma-informed and strictly decoupled from punitive law enforcement frameworks. As advocated by Prasetyo et al. (2026), the state must adopt "precautionary protection" (precautionary protection)—a principle that prioritizes public health, educational resilience, and restorative justice. By addressing the root causes of distress outside the purview of the criminal justice system, society can build resilience and mitigate the allure of gamified extremism without preemptively criminalizing vulnerable adolescents.

CONTRIBUTION

By synthesizing the realities of digital youth extremism with robust interdisciplinary frameworks, this study offers significant advancements to the academic literature and practical policy design. The findings challenge the siloed nature of contemporary extremism research and provide an actionable, multi-layered blueprint for reforming Preventative and Countering Violent Extremism (P/CVE) strategies. The contributions of this study are delineated across four distinct domains: theoretical, empirical, methodological, and practical.

6.1. Theoretical Contribution: Bridging Criminology and Victimology

The primary theoretical contribution of this article is the successful integration of criminological and victimological paradigms to explain the modern "victim-to-actor" radicalization pipeline. Historically, terrorism studies and criminology have faced an epistemological crisis when attempting to categorize youths who engage in violence without coherent organizational or ideological backing (Gartenstein-Ross et al., 2023; Meleagrou-Hitchens & Ayad, 2023).

This study resolves this theoretical tension by demonstrating that "Mixed, Unclear, and Unstable" (MUU) ideologies and participatory memetic violence—such as those prevalent in the True Crime Community (TCC)—cannot be fully understood without incorporating the victimological concept of the victim-offender overlap (Berg & Felson, 2016; Jennings et al., 2012). By mapping Livingstone and Stoilova's (2021) 4C digital risk framework (Content, Contact, Conduct, and Contract risks) onto the radicalization trajectories of traumatized youths, this study establishes a new, integrated theoretical model. It posits that radicalization in the digital age is fundamentally a socio-technical exploitation of offline psychosocial trauma. In doing so, it reinforces the theoretical postulations of Prasetyo, Hartono, and Prasetyo (2026), who argue that digital extremism functions as an "affective enclosure" (*ruang afektif*) that weaponizes offline vulnerabilities. Consequently, this research enriches general strain theory by proving its high applicability to the mechanics of algorithmic radicalization, demonstrating how offline victimization creates the "cognitive openings" necessary for extremist digital grooming (Jasko et al., 2017; Prasetyo et al., 2026).

6.2. Empirical Contribution: Localizing Transnational Memetic Violence

Empirically, this study addresses a significant geographical bias in the existing literature. The vast majority of research on the TCC, bottom-up gamification, and MUU ideologies is heavily Western-centric, focusing primarily on North American and European case studies (Brace, Baele, & Ging, 2024; Smith, Cadenhead, & Broekaert, 2026). This article provides critical, rare empirical evidence from the Global South by analyzing high-profile youth terror plots in Indonesia, specifically the SMAN 72 Jakarta and SMPN 3 Sungai Raya incidents (Prasetyo et al., 2026).

By bringing these localized cases into the global academic discourse, this study empirically validates the transnational reach of memetic violence. It proves that the "cultural scripts" of mass violence—such as the aestheticization of transnational attackers or the use of the "#ZERODAY" hashtag—are not confined by geography or language. Instead, they are organically imported, modified, and weaponized by Indonesian youths to express localized grievances (Prasetyo et al., 2026). Furthermore, by utilizing primary data from Densus 88 Antiteror Polri regarding the 70 Indonesian children exposed to the TCC across 19 provinces, this study provides a crucial empirical baseline that confirms the scale of the threat among minors in developing nations with high internet penetration.

6.3. Methodological Contribution: Capturing the "Onlife" Continuum

Researching modern youth radicalization presents severe methodological challenges, particularly due to the "dark figures" of unreported activities and the ethical constraints of studying minors in encrypted digital environments (Clemmow et al., 2020; Lewis et al., 2024). This study makes a distinct methodological contribution by combining Open-Source Intelligence (OSINT) and digital ethnography with privileged, primary qualitative data from law enforcement (Densus 88) and forensic psychologists, as modeled by Prasetyo et al. (2026).

This mixed-methods triangulation successfully overcomes the artificial separation of offline and online research domains. Internet philosophers and terrorism scholars increasingly argue that we exist in a state of "Onlife," where digital and physical milieus are seamlessly integrated (Valentini, Lorusso, & Stephan, 2020). By tracing the digital footprints of the perpetrators (e.g., manifestos, weapon inscriptions, and chat logs) and corroborating them with offline psychological histories (e.g., records of bullying and family dysfunction), this methodology captures the entirety of the radicalization continuum. This approach serves as a robust methodological template for future researchers attempting to study hard-to-reach extremist populations while mitigating the biases inherent in relying solely on open-source media reporting (Freilich & LaFree, 2016; Prasetyo et al., 2026).

6.4. Practical and Policy Contribution: A Paradigm Shift in P/CVE

Practically, this study advocates for a paradigm shift away from traditional, securitized counter-terrorism approaches toward a public health and child-protection model (Bhui et al., 2012; Weine et al., 2020). The empirical evidence demonstrating that radicalized youths are often victims of Adverse Childhood Experiences (ACEs) necessitates that interventions occur outside the punitive criminal justice system wherever possible, avoiding early criminalization that exacerbates trauma and anti-social identities (Lewis et al., 2025; Prasetyo et al., 2026).

This study offers direct, actionable contributions to the formulation and implementation of Indonesia's National Action Plan for Preventing and Countering Violent Extremism (RAN PE). While Presidential Regulation No. 7 of 2021 laid the foundational framework for a "soft approach," the evolving threat landscape demands that future iterations—specifically the Draft R-Perpres RAN PE 2025-2029—explicitly incorporate the dynamics of gamified violence and MUU ideologies. To operationalize this,

the study draws upon the recommendations of Prasetyo et al. (2026) to propose a **Trauma-Informed, Macro-Social Early Warning System**, structured across three pillars:

1. **Primary Prevention (Needs-Based Prevention):** Focusing on building socio-emotional resilience in families and schools to address the root causes of distress (e.g., severe bullying and social isolation) before cognitive openings are exploited by extremists. This requires a "protective routing system" (*sistem rujukan perlindungan*) connecting schools, parents, and community workers (Prasetyo et al., 2026).
2. **Secondary Prevention (Ecological Digital Moderation):** Assisting platforms and the Ministry of Communication and Digital Affairs (Komdigi) in implementing "algorithmic friction" to interrupt the automated recommendation of extreme TCC and gore content, directly mitigating the Contract and Content risks identified in the 4C framework (Livingstone & Stoilova, 2021; Prasetyo et al., 2026).
3. **Tertiary Prevention (Integrated Case Management):** Developing multi-agency case management systems that prioritize therapeutic recovery, disengagement, and reintegration over immediate incarceration. This treats the radicalized minor primarily as a victim of digital exploitation who requires restorative justice and psychological rehabilitation (Lewis et al., 2024; Prasetyo et al., 2026).

Ultimately, this macro-social policy framework recognizes that because the gamification of violence exploits multiple facets of a youth's life, the state's solution must be equally multifaceted, collaborative, and deeply humane.

CONCLUSION

The digital era has fundamentally disrupted traditional paradigms of terrorism and youth radicalization. As this study has demonstrated, the contemporary threat landscape is no longer exclusively defined by coherent, top-down extremist organizations relying on rigorous ideological indoctrination. Instead, a new, decentralized paradigm has emerged, characterized by "Mixed, Unclear, and Unstable" (MUU) ideologies and Composite Violent Extremism (CoVE) (Astley, 2025; Gartenstein-Ross et al., 2023; Meleagrou-Hitchens & Ayad, 2023). Within predatory digital subcultures like the True Crime Community (TCC), violence has been stripped of its political utility and transformed into "participatory memetic violence"—a gamified, performative act utilized by youths to achieve notoriety and status among their digital peers (Schlegel, 2021; Smith, Cadenhead, & Broekaert, 2026).

However, understanding the sociotechnical mechanics of gamified extremism is only half the equation. The central thesis of this article is that the journey into digital extremism cannot be fully comprehended without acknowledging the psychological victimhood that precedes it. By integrating criminological theories of extremism with the victimological concept of the victim-offender overlap, this study elucidates the "victim-to-actor" pipeline (Berg & Mulford, 2017; Jennings et al., 2012). The empirical realities of the Indonesian case studies—specifically the attempted attacks at SMAN 72 Jakarta and SMPN 3 Sungai Raya—confirm that the youths drawn into these dark fandoms are frequently victims of severe offline trauma, including chronic peer bullying (perundungan), social exclusion, and family dysfunction (Lewis, Marsden, Hewitt, & Peterscheck, 2024; Prasetyo, Hartono, & Prasetyo, 2026).

When these marginalized youths seek refuge online, they are exposed to a matrix of digital vulnerabilities, accurately mapped by Livingstone and Stoilova's (2021) 4C framework: Content, Contact, Conduct, and Contract risks. Algorithmic "outlinking" and digital grooming weaponize their pre-existing trauma, offering a toxic sense of belonging while systematically eroding their moral barriers through dark humor and violent aesthetics (Brace, Baele, & Ging, 2024; Thorleifsson, 2022). As Prasetyo et al. (2026) compellingly argue, the TCC functions as an "affective enclosure" (ruang afektif), exploiting an "attention architecture" (arsitektur atensi) that provides validation to broken youths. Ultimately, violent offending in the digital age often functions as a maladaptive coping mechanism—a tragic attempt by a traumatized youth to reclaim agency and significance in a world where they feel powerless.

The implications of this synthesis are profound. The localization of transnational memetic violence in Indonesia proves that this is not merely a Western phenomenon, but a global crisis operating in the "Onlife" continuum (Valentini, Lorusso, & Stephan, 2020). Consequently, state responses that rely primarily on traditional deterrence theory, punitive law enforcement, and early criminalization are fundamentally misaligned with the nature of the threat. Treating traumatized, indoctrinated minors strictly as autonomous terrorists ignores their developmental vulnerabilities, risks exacerbating their trauma, and ultimately fails to dismantle the digital ecosystems that recruited them (Lewis, Marsden, Stefaniak, & Hewitt, 2025; Prasetyo et al., 2026).

To effectively combat the embryonic stages of digital terrorism, governments and civil society must implement a paradigm shift in Preventative and Countering Violent Extremism (P/CVE) strategies. As proposed in this study's Trauma-Informed, Macro-Social Early Warning System—and aligned with the evolving objectives of Indonesia's Draft RAN PE 2025-2029—interventions must operate on a continuum of care rather than a continuum of punishment. This requires strengthening primary prevention in schools to address the root causes of psychosocial distress, enforcing algorithmic friction at the platform level to disrupt the gamification of violence, and utilizing multi-disciplinary case management to rehabilitate rather than incarcerate at-risk youths (Bhui et al., 2012; Prasetyo et al., 2026).

In closing, the gamification of violence within digital subcultures represents one of the most complex security and public health challenges of the modern era. To break the cycle of memetic violence, society must stop viewing these adolescents exclusively through the lens of the threat they pose, and begin addressing the vulnerabilities they suffer. By bridging the disciplines of Criminology and Victimology, stakeholders can build trauma-informed interventions that do not merely punish the actor, but successfully rescue the victim.

REFERENCES

[1] Allchorn, W., & Orofino, E. (2025). Policing extremism on gaming-adjacent platforms: Awful but lawful? *Frontiers in Psychology*, *16*, 1537460. https://doi.org/10.3389/fpsyg.2025.1537460

[2] Astley, J. (2025). Ideological idiosyncrasies and individual-level radicalisation pathways: Unpacking the mutating dynamics of contemporary extremism. Journal of Policing, Intelligence and Counter Terrorism, 20(3), 380–398. https://doi.org/10.1080/18335330.2025.2502580

[3] Baele, S. J., Brace, L., & Coan, T. G. (2021). Variations on a theme? Comparing 4chan, 8kun, and other chans' far-right "/pol" boards. Perspectives on Terrorism, 15(1), 65–80.

[4] Berg, M. T. (2012). The overlap of violent offending and violent victimization: Assessing the evidence and explanations. In M. DeLisi & P. J. Conis (Eds.), Violent offenders: Theory, research, policy, and practice (pp. 17–38). Jones & Bartlett Learning.

[5] Berg, M. T., & Mulford, C. F. (2017). Reappraising and redirecting research on the victim–offender overlap. Trauma, Violence, & Abuse, 21(1), 16–30. https://doi.org/10.1177/1524838017735925

[6] Bekti, H., Pancasilawan, R., Komara, S. R., & Achmad, W. (2025). Integrating Policy, Public Opinion, and Sundanese Values for Effective Public Leadership and Good Governance. International Journal of Law and Society, 4(2), 219-233. https://doi.org/10.59683/ijls.v4i2.288

[7] Brace, L., Baele, S. J., & Ging, D. (2024). Where do 'mixed, unclear, and unstable' ideologies come from? A data-driven answer centred on the incelosphere. Journal of Policing, Intelligence and Counter Terrorism, 19(2), 103–124. https://doi.org/10.1080/18335330.2023.2226667

[8] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

[9] British Psychological Society. (2021). BPS code of human research ethics (4th ed.). British Psychological Society.

[10] Clemmow, C., Schumann, S., Salman, N. L., & Gill, P. (2020). The base rate study: Developing base rates for risk factors and indicators for engagement in violent extremism. Journal of Forensic Sciences, 65(3), 865–881.

[11] Corner, E., & Gill, P. (2015). A false dichotomy? Mental illness and lone-actor terrorism. Law and Human Behavior, 39(1), 23–34. https://doi.org/10.1037/lhb0000102

[12] Gartenstein-Ross, D., & Blackman, M. (2022). Fluidity of the fringes: Prior extremist involvement as a radicalization pathway. Studies in Conflict & Terrorism, 45(7), 555–578. https://doi.org/10.1080/1057610X.2018.1531545

[13] Gartenstein-Ross, D., Zammit, A., Chace-Donahue, E., & Urban, M. (2023). Composite violent extremism: Conceptualizing attackers who increasingly challenge traditional categories of terrorism. Studies in Conflict & Terrorism, 48(12), 1343–1369.

[14] Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. Criminology & Public Policy, 16(1), 99–117. https://doi.org/10.1111/1745-9133.12249

[15] Helfgott, J. B. (2015). Criminal behavior and the copycat effect: Literature review and theoretical framework for empirical investigation. Aggression and Violent Behavior, 22, 46–64. https://doi.org/10.1016/j.avb.2015.02.002

[16] Jasko, K., LaFree, G., & Kruglanski, A. (2017). Quest for significance and violent extremism: The case of domestic radicalization. Political Psychology, 38(5), 815–831.

[17] Jennings, W. G., Piquero, A. R., & Reingle, J. M. (2012). On the overlap between victimization and offending: A review of the literature. Aggression and Violent Behavior, 17(1), 16–26. https://doi.org/10.1016/j.avb.2011.09.003
[18] Lakhani, S., & Wiedlitzka, S. (2022). "Press F to Pay Respects": An empirical exploration of the mechanics of gamification in relation to the Christchurch attack. Terrorism and Political Violence, 34, 1–18. https://doi.org/10.1080/09546553.2022.2064746
[19] Lewis, J., & Marsden, S. (2021). Countering violent extremism interventions: Contemporary research. Centre for Research and Evidence on Security Threats (CREST).
[20] Lewis, J., Marsden, S., & Copeland, S. (2020). Evaluating programmes to prevent and counter extremism. Centre for Research and Evidence on Security Threats (CREST).
[21] Lewis, J., Marsden, S., Hewitt, J., & Peterscheck, A. (2024). Trauma, adversity and violent extremism (TAVE): A systematic review. Centre for Research and Evidence on Security Threats (CREST).
[22] Lewis, J., Marsden, S., Stefaniak, A., & Hewitt, J. (2025). Non-criminal justice interventions for countering cognitive and behavioural radicalisation amongst children and adolescents: A systematic review of effectiveness and implementation. Campbell Systematic Reviews, 21(1), e70020. https://doi.org/10.1002/cl2.70079
[23] Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. (CO:RE Short Report Series on Key Topics). Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI). https://doi.org/10.21241/ssoar.71817
[24] McCauley, C., & Moskalenko, S. (2017). Understanding political radicalization: The two-pyramids model. American Psychologist, 72(3), 205–216.
[25] Meleagrou-Hitchens, A., & Ayad, M. (2023). The age of incoherence? Understanding mixed and unclear ideology extremism. Program on Extremism at George Washington University.
[26] 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
[27] Norris, J. T. (2020). Idiosyncratic terrorism: Disaggregating an undertheorized concept. Perspectives on Terrorism, 14(3), 2–18.
[28] Peraturan Presiden Republik Indonesia Nomor 7 Tahun 2021. (2021). Rencana Aksi Nasional Pencegahan dan Penanggulangan Ekstremisme Berbasis Kekerasan yang Mengarah pada Terorisme Tahun 2021-2024.
[29] Piquero, A. R., MacDonald, J. M., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-control, violent offending, and homicide victimization: Assessing the general theory of crime. Journal of Quantitative Criminology, 21(1), 55–71.
[30] Prasetyo, D., Hartono, E., & Prasetyo, S. (2026). Gamifikasi kekerasan dalam teror modern di era digital.
[31] Rencana Aksi Nasional Pencegahan dan Penanggulangan Ekstremisme Berbasis Kekerasan. (2024). Draf R-Perpres RAN PE 2025-2029.
[32] Schlegel, L. (2020). Jumanji extremism? How games and gamification could facilitate radicalization processes. Journal for Deradicalization, 23, 50–92.
[33] Schlegel, L. (2021). The role of gamification in radicalization processes (Working Paper 1/2021). Modus|zad.
[34] Schlegel, L., & Kowert, R. (Eds.). (2024). Gaming and extremism: The radicalization of digital playgrounds. Routledge.
[35] Simi, P., Sporer, K., & Bubolz, B. F. (2016). Narratives of childhood adversity and adolescent marginalization among white supremacists. Terrorism and Political Violence, 28(4), 715–731.
[36] Smith, P., Cadenhead, C., & Broekaert, C. (2026). True crime community: Understanding the depths of digital fandom and performative violence. CTC Sentinel, 19(2), 17–26.
[37] Thorleifsson, C. (2021). From cyberfascism to terrorism: On 4Chan/Pol/culture and the transnational production of memetic violence. Nations and Nationalism, 28(1), 286–301. https://doi.org/10.1111/nana.12780
[38] Valentini, D., Lorusso, A. M., & Stephan, A. (2020). Onlife extremism: Dynamic integration of digital and physical spaces in radicalization. Frontiers in Psychology, 11, 524. https://doi.org/10.3389/fpsyg.2020.00524
[39] Windisch, S., Simi, P., Blee, K., & DeMichele, M. (2020). Measuring the extent and nature of adverse childhood experiences (ACE) among former white supremacists. Terrorism and Political Violence, 34(6), 1184–1204.