

Gamified Online Radicalization and Counterterrorism Law Reform for Indonesian Adolescents

Ali Masyhar ^a , **Feddy Setio Pribadi** ^b ,
Muhammad Azil Maskur ^a , **Nadhira Madania Dimarti** ^a ,
Sunusi Dauda ^c 

^a Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

^b Faculty of Engineering, Universitas Negeri Semarang, Semarang, Indonesia

^c S.D. Attorneys, Legal Consultants and Solicitors, Kano, Nigeria

✉ corresponding email: ali_masyhar@mail.unnes.ac.id

Abstract

Indonesia's Counterterrorism Law (Law No. 5 of 2018) has not regulated one of the rapidly growing radicalization vectors: multiplayer online games, where recruitment is decentralized, extremist narratives are embedded in in-game content, and migration to encrypted platforms operates outside existing regulatory frameworks. This research addresses that normative gap by examining how extremist content is disseminated through online games played by Indonesian teenagers and identifying legal weaknesses that leave this vector unregulated. Using a normative-qualitative approach combining doctrinal analysis, literature review, and exploratory questionnaire data from 46 junior high school students (ages 12–15) in Gunungpati, Semarang, this study analyzes radicalization mechanisms—including narrative infiltration, extremist symbols, and in-game recruitment—through Moghaddam's *Staircase to Terrorism* framework and Ware's Third Generation of Radicalization. The findings

indicate significant exposure to ideological recruitment through in-game social features and psychosocial vulnerabilities among respondents, strengthening the doctrinal urgency beyond generalized statistical claims. The doctrinal analysis identified three normative gaps in Law No. 5 of 2018: the absence of due diligence obligations for game operators, the lack of detection and school-based reporting mechanisms, and the failure to recognize children vulnerable to radicalization as subjects of legal protection rather than criminal responsibility. By integrating empirical evidence with doctrinal analysis, this study provides the first legal-empirical account linking online game-based radicalization to Indonesian counterterrorism law and highlights the need to shift from a repressive to a prevention-oriented legal framework through early intervention in digital radicalization.

Keywords

Online Game Radicalization, Counterterrorism Law Reform, Normative Gap, School-Based Radicalization Prevention, Adolescent Digital Vulnerability.

HOW TO CITE:

Chicago Manual of Style Footnote:

¹ Ali Masyhar, Feddy Setio Pribadi, Muhammad Azil Maskur, Nadhira Madania Dimarti, and Sunusi Dauda, “Gamified Online Radicalization and Counterterrorism Law Reform for Indonesian Adolescents,” *Journal of Law and Legal Reform* 7, no 3 (2026): 1585–1626, <https://doi.org/10.15294/jllr.v7i3.58192>.

Chicago Manual of Style for Reference:

Masyhar, Ali, Feddy Setio Pribadi, Muhammad Azil Maskur, Nadhira Madania Dimarti, and Sunusi Dauda. “Gamified Online Radicalization and Counterterrorism Law Reform for Indonesian Adolescents.” *Journal of Law and Legal Reform* 7, no 3 (2026): 1585–1626. <https://doi.org/10.15294/jllr.v7i3.58192>.

Introduction

The development of technology has fundamentally changed social interaction patterns, especially among teenagers who grew up in a digital environment their whole lives. This generation who was born and grew up in this digital ecosystem, has faced social identity forming, group affiliation, and value orientation through a medium that is fundamentally different from the previous generation, a medium that is not bordered by geographical space or direct supervision from adults as conventional social interactions were. Online games, which at first is a form of entertainment, have now developed into a dynamic and interactive social space. Many features, such as text chat, voice chat, guild system, and the community forum, have made it possible for players to interact intensively, creating a collective identity, and building social bonds, replicating a real, offline community.¹ However, Akin's research is conducted in the context of video games in Türkiye, and it focuses on the socio-environmental communication in general, not including the ideological content mechanisms or triggering radicalization specifically, a gap that can be solved by this research in Indonesia context.

The internet penetration and online game usage level in Indonesia are among the highest in the world, with teenagers as the most active age group.² The data collected by Ameliah, Negara, and Minarto described a digital literacy scale and internet usage in Indonesia generally, but it does not reach the penetration level based on any platforms or studied the implications to the risk related to certain contents, such as radicalization in video game environments. This penetration scale makes the online gaming ecosystem as a social space of equal significance, or even in some aspects have reached beyond it, the significance of conventional social media platforms in shaping the contemporary Indonesian teenagers' social interaction landscape. However, the academic and regulative attention toward this ecosystem is

¹ Mustafa Seref Akin, "Communication With the Social Environment in Multiplayer Online Games : The Turkey Case," *International Journal of Game-Based Learning* 13, no. 1 (2023): 1–14, <https://doi.org/10.4018/IJGBL.330755>.

² Rizki Ameliah, Rangga Adi Negara, and Bahtiar Minarto, "Status Literasi Digital Di Indonesia" (Jakarta, 2023).

proportionally lower than the attention given to the social media platform.

In the context of digital security, the radicalization in digital space has become quite a prominent issue. Most of the researches in digital radicalism focused on bigger social media, such as Facebook, X, YouTube, and Telegram, as the main medium in extremist narration dissemination.³ Analysis conducted by Aminudin, Nugroho, and Sutrisno, like many similar literatures, views social media as an undifferentiated information technology category, without differentiating specific interactive and participative mechanisms on gaming platform, which according to this research operated differently than passive content-feed environments. These studies have consistently shown that conventional social media provides an algorithmic mechanism that accelerates an individual's exposure to extremist content through an optimized recommendation system for engagement, without considering ideological effects from the recommended content.⁴ Although the number of studies on digital radicalism has increased significantly, the focus tends to be limited to conventional social media, meanwhile, the online game ecosystem, which also becomes an intensive social interaction space with teenagers as the dominant users, has not received the same amount of academic attention as the risk scale.⁵

This research gap has become more worrying when considered alongside the unique characteristics of the gaming ecosystem that set it apart from social media platforms: its immersive and participatory nature, and the fact that it is often viewed as a "safe" space by parents precisely because it is framed as entertainment for children and adolescents, rather than as a social space requiring the same level of

³ Cecep Aminudin, Prastyawan Nugroho, and Andri Sutrisno, "Media Sosial Dan Radikalisme : Bagaimana Teknologi Informasi Mempengaruhi Pemikiran Ekstrem," *Journal Humaniora: Jurnal Hukum Dan Ilmu Sosial* 01, no. 04 (2023): 110–15, <https://doi.org/10.37010/hmr.v1i4.31>.

⁴ Deki Marizaldi, Muhammad Herdi Pratama, and Abipraya Guntur Sulatiasto, "From Clicks to Violence : A Study on the Role of Social Media in Radicalization and Terrorism," *Jurnal Akta* 12, no. 2 (2025): 417–33, <https://doi.org/10.30659/akta.v12i2.44872>.

⁵ Jacob Davey, "Gamers Who Hate : An Introduction to ISD ' s Gaming and Extremism Series," 2021.

supervision as social media platforms. The radicalism dissemination in online games is generally not done explicitly; instead, it is done through a subtle and implicit approach, such as the usage of symbols, narration, and sentiment framing that are integrated organically to the gaming experience.⁶ This characteristic makes online games a radicalization medium that is specifically difficult to detect compared to conventional social media, because the process happens in the frame of entertainment so that it does not raise suspicions of the user or the supervisor, including parents and teachers.

This difficulty in detecting is not only a technical issue or a parent supervision issue, instead it shows the legal response limitations in Indonesia, because the existing legal framework cannot regulate a phenomenon that is not designed yet to be identified. This problem becomes more complex when it's related to the counterterrorism framework in Indonesia. As a legal instrument that was formulated in an era when terrorist threats were still dominated by centralized and hierarchical organization structures, existing legal framework may not necessarily have the conceptual or operational capacity to address forms of radicalization that are decentralized, gamified, and operate through an ever-evolving digital ecosystem. The question of legal sufficiency becomes even more urgent, given that the global trend shows a shift from an organized terrorist act to lone-wolf terrorist acts, whose radicalization root becomes even more discovered in informal digital spaces, including the online gaming ecosystem.

Based on the description above, this research aims to analyse the pattern of radicalism dissemination in online games among teenagers, mapping the infiltration mechanisms through the theoretical framework Staircase to Terrorism and the gamification of radicalism, as well as a main contribution, identifying the normative gaps in Indonesia's counterterrorism legal framework that make this phenomenon not treated legally.

⁶ Linda Schlegel, "Jumanji Extremism? How Games and Gamification Could Facilitate Radicalization Processes," *Journal for Deradicalization* Summer 202, no. 23 (2020): 1–44, <https://journal-derad.com/index.php/jd/article/view/359>.

This research is specifically directed to answer three questions:

1. How the mechanisms of radicalism infiltration operate within the online gaming ecosystem based on empirical data from the Indonesian adolescent population;
2. To what extent the current legal framework for countering terrorism is capable of addressing these mechanisms;
3. What substantive norms are needed to fill the identified legal gaps?

This research uses a qualitative approach to analyse the radicalism dissemination pattern in online games in among teenagers, combined with normative legal analysis to identify a relevant regulation gap.⁷ A qualitative approach was picked because the studied phenomenon, an infiltration of radicalism through implicit and subtle mechanisms, needs an interpretative analysis that is not fully reduced to just quantitative data, although a Quantitative survey data continues to serve as empirical support for the normative arguments presented. Specifically the findings in the empirical survey functioned as an illustrative prove base for normative/doctrinal analysis: identified patterns in survey data used to strengthen the practical urgency from normative gaps studied in legal discussion, not as an independent statistical claim about a broader teenage population.

Data were collected from a sample of 46 junior high school students in Gunungpati, Semarang, selected through purposive sampling via an existing school partnership / convenience sampling based on accessibility. This location and sample were chosen because of a prior engagement through a community service conducted previously on the same topic. The data were collected through a structured questionnaire consists of 39 items with ten indicator categories: intolerance and exclusivity, dehumanization, extreme violence glorification, in-group out-group polarization, emotional and risk influence, narrative-based infiltration, and psychosocial vulnerability. Each item is measured by a 5 point Likert scale (Strongly disagree to Strongly agree), which then recoded to a biner category (for example, Agree/Experienced vs

⁷ J.W. Cresswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (New York: SAGE, 2018).

Disagree/Not Experienced yet) to support descriptive analysis frequency.

The data in this study were analysed using qualitative descriptive methods, integrating findings from literature reviews, analyses of international case documents, and empirical survey data collected from a population of junior high school students in Gunungpati, Semarang.⁸ Literature study is used to build a theoretical framework and map the radicalism infiltration typology that has been documented in the international context; meanwhile, case document analysis is used to validate that the mapped mechanism theoretically has real manifestations in past terrorism incidents. Quantitative percentages reported in the Results & Discussion section is descriptive frequencies achieved from questionnaire answers and not intended as a finding that can be generalised statistically ; the sample size (n=46) and the limited scope in one location is the limitation in this research.

This research has high urgency because it fills and captures the radicalism infiltration phenomenon in online games, which, until now, has not been documented empirically in Indonesia, especially with its relations to the sufficiency of the positive legal framework to respond to it.⁹ The significance of this research lies in three aspects: first, empirical contribution in the form of survey data that directly measures exposure among a sample of Indonesian junior high school students in Semarang to a game-based radicalization mechanism, which is not available yet in existing Indonesian literature; second, a theoretical contribution in the mapping of radicalism gamification mechanism to the Staircase to Terrorism framework that is already established in psychopolitics literatures; and third, a normative contribution in the form of legal vacuum identification that is concrete and norm substance recommendation that is needed to fill it, a contribution that places this

⁸ Miza Nina Adlini et al., "Metode Penelitian Kualitatif Studi Pustaka," *Edumaspul : Jurnal Pendidikan* 6, no. 1 (2022): 974–80, <https://doi.org/10.33487/edumaspul.v6i1.3394>.

⁹ Syarif Saddam Rivanieparawansa, Koesrianti Koesrianti, and Toetik Rahayuningsih, "Prevention of Radicalism in the Cyberspace in Indonesia," *International Journal of Humanities Social Sciences and Education* 6, no. 7 (2019): 63–72, <https://doi.org/10.20431/2349-0381.0607007>.

research directly relevant in the law reform agenda of counterterrorism law in Indonesia.

A. The Negative Effects of Online Games and Their Manifestations in Real-Life Cases

Online games and their player communities have become a new field used by extremist groups as an informal interaction space to spread radical narration. The difference between online games and conventional social media platforms lies in how immersive and participative they are: the user is not only consuming content passively, instead, they're actively involved in the narrative world-building, interacting with other players in real-time, and building emotional investment in the progress and achievements of the games. This participative aspect is what makes online games a structurally different medium, and in more ways are more effective, to sow values compared to one-way social media content.¹⁰ Although pure radicalization seldom happens through games, the long-term effects from the online game exposure can be used as an accelerator for individuals who have previously experienced psychological or social vulnerability, accelerating the actual process rooted in factors outside of the game.

Two terrorist shooting cases became turning points in the academic understanding of the relationship between online games and radicalization are the Christchurch attack in New Zealand on March 15, 2019, and the Halle attack in Germany on October 9, 2019. The Christchurch perpetrator broadcasted his act live using languages and aesthetics that impersonate a first-person shooter games streaming style, complemented by internet meme references which are often found in online gaming communities, including the opening phrase that explicitly alludes to the meme culture before committing his act.¹¹ The official investigation report of this incident noted that the perpetrator had an extensive online activity history in forums involved with the gaming community, in which he built social network with individuals sharing

¹⁰ Rivanieparawansa, Koesrianti, and Rahayuningsih.

¹¹ Davey, "Gamers Who Hate : An Introduction to ISD ' s Gaming and Extremism Series."

similar extremist views in a significant period of time before launching his act.¹²

The Halle Shooting perpetrator showed a similar pattern of action, with intensive online activity background in forums involved with the gaming community and using gaming terminology in his manifesto.¹³ The investigative report on the Halle Shooting revealed that the perpetrator is a socially isolated individual, with a significant personal failure history, and finding validation and acknowledgement in the extremist online community, which in majority are involved with the online gaming culture.¹⁴ The two perpetrators were identified as part of a right-wing extremist network which was formed and strengthened through online interactions in spaces which culturally involved in the online gaming community, although not one of the two incidents

¹² The Royal Commission of New Zealand, "Executive Summary of the Christchurch Shootings," The Royal Commission of New Zealand, 2019, <https://christchurchattack.royalcommission.nz/the-report/executive-summary-2/executive-summary>; New Zealand Police, "2019 - Operation Deans Terrorist Attack, Ōtautahi Christchurch, 15 March," New Zealand Police, 2019, <https://www.police.govt.nz/about-us/history-and-museum/museum/exhibitions/place-many-brave-deeds/2019-operation-deans-terrorist>.

¹³ Daniel Koehler, "The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat," *CTC Sentinel* V, no. December 2018 (2019): 14–20, <https://ctc.westpoint.edu/halle-germany-synagogue-attack-evolution-far-right-terror-threat/>; Lizzie Dearden, "Stephan Balliet: The 'Loser' Neo-Nazi Suspected of Deadly Attack on German Synagogue," Independent, 2019, <https://www.independent.co.uk/news/world/europe/german-synagogue-shooting-halle-attack-latest-stephan-balliet-suspect-neo-nazi-a9150451.html#gsc.tab=0>.

¹⁴ Oliver Holmes and Philip Oltermann, "Halle Synagogue Was Fortified before Antisemitic Attack," The Guardian, 2019, <https://www.theguardian.com/world/2019/oct/11/halle-synagogue-fortified-ahead-antisemitic-attack-germany>; Jon Sheldon and Kristie Pladson, "Police Investigate Anti-Semitism Links in Halle Shootings," DW, 2019, <https://www.dw.com/en/police-investigate-anti-semitism-links-in-halle-shootings/a-50764327>; Ben Cohen, "Shock in Germany After Neo-Nazi Gunman Who Attacked Synagogue on Yom Kippur Attempts Prison Escape," The Algemeiner, 2020, <https://www.algemeiner.com/2020/06/04/shock-in-germany-after-neo-nazi-gunman-who-attacked-synagogue-on-yom-kippur-attempts-prison-escape/>.

mentioned above shows the game itself directly becoming a recruitment medium; instead, the spaces adjacent to the gaming culture become the early contact point.¹⁵

Besides the two cases mentioned above as the realest manifestations of radicalization through game, many additional incidents strengthen the argument that contemporary radicalism developing in a hybrid digital ecosystem has reached beyond the boundaries of a single platform.¹⁶ What is relevant from these additional cases is the recurring pattern, migration from gaming spaces to a more secluded ideological community, which indicates that this is not an anomaly but a structural pattern that can be predicted, and, because of that, theoretically can be intervened through the right policy. Although the Christchurch and Halle shootings happened in jurisdictions that have a terrorism typology and different gun regulations from Indonesia, the relevance lies in Indonesia's legal framework on the proven path itself, not on the jurisdictional context: those two cases stated that spaces related to online games can be used as an early communication point for radicalization, despite of the regulations around them, a path that cannot be anticipated in Indonesia counterterrorism law.

Those patterns are in harmony with the characteristics of the third generation of online radicalization, which is marked by decentralization, platform fragmentation, and user migration from an open platform to an encrypted application.¹⁷ Therefore, the role of online games needs to be understood not only as a single factor, but as a part of a broader digital ecosystem, in which many platforms are complementing each other in

¹⁵ Olivier Cauberghe, "Hate the Player, Not the Game: Exploring Extremist and Terrorist Use of Games, Gaming Platforms and Gamification Strategies for Propaganda Purposes," *Radices: Interdisciplinary Journal for the Study of Terrorism & Extremism* 4, no. 1 (2024): 90–110, <https://doi.org/10.21825/radices.94142>.

¹⁶ Simon Greipl et al., "Tracking down the Candy Crush Terrorist: The Fragile Relation between Gaming Motives and Radical Attitudes," *Frontiers in Psychology* 16, no. 1585576 (2025): 1–19, <https://doi.org/10.3389/fpsyg.2025.1585576>; Garrison Wells et al., "Right-Wing Extremism in Mainstream Games: A Review of the Literature," *Games and Culture* 19, no. 4 (2024): 469–92, <https://doi.org/10.1177/15554120231167214>.

¹⁷ Jens F Binder, Jonathan Kenyon, and Caitlin Clemmow, "Terrorism and the Internet: How Dangerous Is Online Radicalization?," *Frontiers in Psychology* 13, no. October (2022): 1–10, <https://doi.org/10.3389/fpsyg.2022.997390>.

creating a whole radicalization pathway, starting from in-game contact, to a more open discussion forum, and ending with platform migration to an encrypted community, closed off from external supervision.

Several radical-terrorist perpetrators are also identified using phrases that are often found in gaming culture, such as “achievement”, “kill-count”, and other gamified phrases to describe the violence they commit, an indication that the gaming cognitive framework has been internalized in their way to understand extreme acts.¹⁸ The use of these terminologies is not only a linguistic coincidence; it reflects how a cognitive scheme is formed through gameplay experience, in which it’s measured through scores, levels, and achievements, and transferred into a real interpretation of acts of violence, so that violence can be processed mentally through the same framework when they finish a game level.¹⁹ While the case documentation level in Indonesia on this specific pathway is still limited, similar patterns have been internationally documented, which strengthens the possibility of the existence of a radicalization vector instead of ignoring it as low risk. Considering the high level of internet and online game penetration in Indonesian teenagers, the gap in domestic documentation itself is the research gap that strengthens the empirical study urgency in this research.²⁰

¹⁸ Eka Mahatva, Yudha Pujo, and Widodo Rudy, “Strategi Badan Nasional Penanggulangan Terorisme (BNPT) Indonesia Dalam Menghadapi Ancaman Paham Radikal,” *Aurelia: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia* 4, no. 2 (2025): 2382–89, <https://doi.org/10.57235/aurelia.v4i2.5657>.

¹⁹ Marcus Schulzke, “Simulating Terrorism and Insurgency: Video Games in the War of Ideas,” *Cambridge Review of International Affairs* 27, no. 4 (2014): 627–43, <https://doi.org/10.1080/09557571.2014.960508>; Eziho Promise Ogele, “The Intersection of Gaming and Terrorism : Exploring the Role of Online Gaming in Terrorist Recruitment Methods,” *Political Observer: Portuguese Journal of Political Science* 2024, no. 22 (2024): 23–39, <https://doi.org/10.59071/2795-4765.RPCP2024.22/pp.23-39>.

²⁰ Mastina Maksin, “Strategi Pemerintah Dalam Mencegah Paham Radikalisme Di Era Penggunaan Media Sosial Di Kalangan Remaja,” *Journal of Humanity Studies* 1, no. 2 (2022): 85–94, <https://doi.org/10.22202/jhs.2022.v1i2.6495>.

B. The Radicalism Infiltration Typology in Online Games

There are several forms and typologies used by extremist groups to infiltrate online games with radical content. Understanding of these typologies is important not only as a descriptive catalogue, but because each of these typologies needs a different detection and intervention strategy, a consideration which later becomes relevant when formulating legal policy for platform operators in the legal reform part. There are at least three main typologies that can be identified from existing literature: narration and storyline, visual and linguistic symbols, and sentiment framing.

First, narration and storyline. The extremist and radical groups use a conflict demarcation line “us versus them”, in which “us” identifies their own group as the right and oppressed group, meanwhile “them” is constructed as the enemy that needs to be defeated.²¹ This narrative pattern is often inserted through the game storyline by modified content (mods) or even the game’s own default design, creating a simple yet emotionally strong moral dichotomy. What differentiates this typology from conventional propaganda is that the “us versus them” dichotomy does not serve as an argument that must be accepted cognitively, but it is faced directly through gameplay, players literally “fight” “their” group in every game session, so that the dichotomy is internalized through a recurring experience, not through an argumentative persuasion. This typology, since it operated through the core game design, instead of a separate user content, points toward a regulatory obligation for the developers themselves, not to the content moderation done after.

Second, visual and linguistic symbols. The radicalism disseminators infiltrate online games by planting war and radical ideologies visually.²² These symbols, starting from flags, logos, to character skins, functioned as a group identity signal that is recognized by all extremist group members, and also functioned as an ideology

²¹ Mahatva, Pujo, and Rudy, “Strategi Badan Nasional Penanggulangan Terorisme (BNPT) Indonesia Dalam Menghadapi Ancaman Paham Radikal.”

²² Schulzke, “Simulating Terrorism and Insurgency: Video Games in the War of Ideas.”

normalization tool through constant visual repeats. The effectiveness of this typology lies in its characteristic that looks innocent to outsiders; a symbol for ordinary players may appear to be merely an aesthetic design element can carry profound ideological significance for those who are educated about these visual codes, allowing ideological communication to take place openly without being detected by conventional content moderation systems designed to detect text rather than subtly modified visual elements. This typology shows that regulatory response cannot just depend on conventional text-based moderation content, but also on visual/symbol detection standards, specifically designed for game environments.

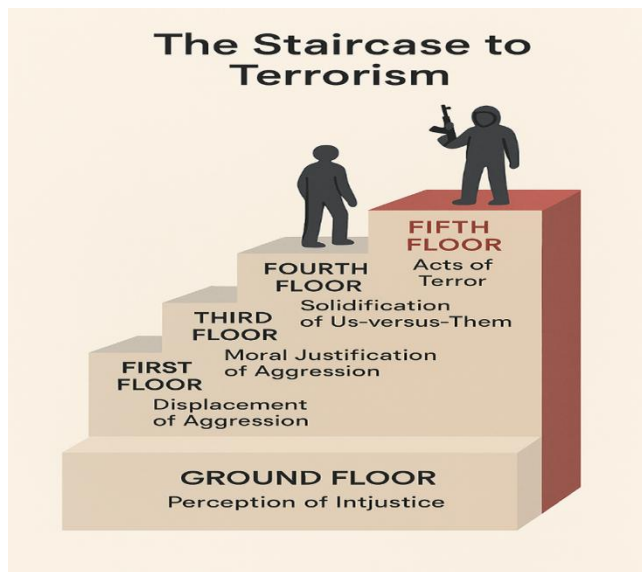
Third, Sentiment framing. Sentiment framing is used by radical groups to prioritize the glorification and heroization of violence, in which violence is framed as a heroic act that is “justified” and “necessary” to defend a group or belief.²³ This type of framing works by leveraging the reward structures inherent in the game’s design itself—actions that result in violence within the game are, by default, already positively reinforced through point systems and achievements, so that extremist sentiment framing merely needs to add a layer of ideological meaning on top of the existing reward structure, rather than building it from scratch. Since this mechanism is integrated in the achievement system architecture, not in a removable content, it indicates that the regulation standard on the level design, not content removal, which is the right intervention step.

These three typologies strengthen each other and almost never operate in isolation: narratives construct a framework of conflict that provides context for actions; symbols reinforce group identity, fostering a sense of belonging; and the framing of sentiments justifies acts of violence as a legitimate—and even noble—response to the conflict established by those narratives. The combination of these three elements produces a psychologically coherent experience—a complete narrative world with enemies, identities, and moral justifications—that is far more persuasive than if the three elements were presented separately through conventional propaganda.

²³ Maksin, “Strategi Pemerintah Dalam Mencegah Paham Radikalisme Di Era Penggunaan Media Sosial Di Kalangan Remaja.”

The process by which an individual becomes radicalized to the point of committing acts of terrorism does not occur instantly, but rather through a series of stages that unfold gradually. Fathali Moghaddam describes this process as a multi-story building or a staircase, where the higher one climbs to a higher floor, the fewer people reach that stage, yet the greater the intensity of radicalization they experience.²⁴ It is important to understand this model not as a rigid, linear description, but as an analytical framework that maps out critical points where preventive interventions are most likely to succeed—the lower the floor a person occupies, the greater the scope for intervention to prevent further progression toward acts of violence.

Figure 1. Moghaddam’s Staircase to Terrorism



Sources: Fathali M. Moghaddam “The Staircase to Terrorism” (2006)

On the ground floor, someone feels injustice that happened to them or their group, whether it is a social, economic, or political injustice. This injustice perspective does not have to be objective; it can be subjective and perceived differently by different individuals based on

²⁴ Fathali M. Moghaddam, “The Staircase to Terrorism: A Psychological Exploration,” *American Psychologist* 60, no. 2 (2005): 161–69, <https://doi.org/10.1037/0003-066X.60.2.161>.

social position, familial background, and their own personal experience. This injustice narration is then often used by radicalism disseminators as an early step to build sympathy and emotional resonance, because injustice felt personally is stronger emotionally than abstract ideological arguments.²⁵

On the first floor, individuals who feel injustice start to find a way out of their issues, but not through formal pathways, law, institution, or legal social mechanisms, thinking that it did not provide a solution, individuals began to consider alternatives outside the system.²⁶ This stage is crucial because it marks a point in which belief toward formal institutions starts to disappear, including school, the government, and the legal system, since it is not considered responsive to individual complaints, the space for alternative narratives offered by extremist groups is becoming increasingly open.

On the second floor, when individuals feel like there is no legal exit out of their issues, piling up frustration changes into displacement of aggression to targets constructed as the problem source, although the target is not always the direct source of the injustice currently being faced.²⁷ This displacement psychologically functioned as an emotional release mechanism that cannot be channelled through constructive way, and extremist groups strategically provide a clear and easy target identified as an outlet for piling up aggression.

On the third floor, individuals begin to adopt extreme or radical ideologies that justify violence as a legitimate and even necessary act. A sense of injustice that was previously personal now transforms into an

²⁵ Alessandro Orsini, "Studies in Conflict & Terrorism What Everybody Should Know about Radicalization and the DRIA Model DRIA Model," *Studies in Conflict & Terrorism* 46, no. 1 (2023): 68–100, <https://doi.org/10.1080/1057610X.2020.1738669>.

²⁶ Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism : Six Suggestions for Progressing Research," *Studies in Conflict & Terrorism* 40, no. 1 (2017): 77–98, <https://doi.org/10.1080/1057610X.2016.1157408>.

²⁷ Tereza Capelos et al., "'Today I Die like Jesus Christ': An Analysis of Ressentiment in Perceptions, Motivations and Justifications of Violent Extremist Manifestos," *Terrorism and Political Violence* 37, no. 8 (2025): 1031–47, <https://doi.org/10.1080/09546553.2024.2379043>.

ideological conviction that provides moral legitimacy for violence.²⁸ This is the critical point at which moral disengagement—the detachment from conventional moral frameworks—begins to take full effect; individuals no longer view violence as a moral transgression, but rather as a justified and even noble act within the ideological framework they have adopted.

On the fourth floor, individuals begin to join or form strong bonds with extremist groups believed to share the same goals and values, thereby strengthening their collective identity and commitment to the group.²⁹ At this stage, the individual's personal identity becomes increasingly fused with the group's identity, so that leaving the group is no longer merely a matter of severing social ties but rather a loss of the self-identity built through that affiliation—a condition that makes the deradicalization process at this stage far more difficult than in previous stages.

The fifth floor is the final stage of someone's realized radicalization process in the form of terrorism act. At this stage, an individual has fully internalized violence ideology and is ready to commit the planned act.³⁰ Moghaddam stated that in this stage, the psychological mechanisms that previously held an individual back from violence act, empathy, fear of consequences, social bond with the world outside of the extremist group, is fully replaced by the ideological commitment that placed violence act as the peak of morale journey done by the individual.

If this theory is compared to radicalization happening through online games as mentioned above, it is clear that the online game ecosystem has the capacity to accelerate someone's process to walk on the floor or level on the stairs, especially from the ground floor to the second

²⁸ Saifudin Asrori and Amsal Bakhtiar, "Articulating Takfir: Ayman Al-Zawahiri and the Global Jihad Ideology," *Episteme: Jurnal Pengembangan Ilmu Keislaman* 16, no. 2 (2021): 167–87, <https://doi.org/10.21274/epis.2021.16.02.167-187>.

²⁹ Thomas James, Vaughan Williams, and Calli Tzani, "Behavioral Sciences of Terrorism and Political Aggression How Does Language Influence the Radicalisation Process? A Systematic Review of Research Exploring Online Extremist Communication and Discussion Systematic Review of Research Exploring Online Extre," *Behavioral Sciences of Terrorism and Political Aggression* 16, no. 3 (2024): 310–30, <https://doi.org/10.1080/19434472.2022.2104910>.

³⁰ Europol, "European Union Terrorism Situation and Trend Report 2021," 2021, <https://doi.org/10.2813/677724>.

floor, in which narratives of injustice, the search for alternatives outside the formal system, and the displacement of aggression can occur intensely through social interactions within the game.³¹ Online games provide a structurally ideal space for this process: they offer a sense of community and acceptance to individuals who feel alienated in the real world, provide a clear enemy target in the form of in-game opponents who can be easily mapped onto real-world ideological frameworks, and offer a sense of achievement and personal significance that may not be available to these individuals in their daily lives. Nevertheless, there are also cases in which online game content—or online content in general—can accelerate the radicalization process more rapidly than predicted by Moghaddam’s stepwise model, particularly when the individual in question already possesses significant psychosocial vulnerabilities before exposure to such content.³²

The next fundamental part is the gamification of radicalism. The gamification of radicalism is the process of psychological internalization in which the violent ideological act is wrapped and served by using game design elements, such as points, achievements, levels, and competitions, so that violence looks like a fun, competitive activity that provides a sense of personal accomplishment.³³ This gamification mechanism effectively blurs the line between games and real-world actions, as individuals who have become accustomed to interpreting achievements through a gamified framework tend to transfer that interpretive framework into the realm of real-world actions, including acts of violence. Researchers and policy institutions, including the RAND Corporation, further state that contemporary digital radicalism relies on mechanisms of emotional and participatory engagement that resemble the gaming experience, in which

³¹ Rachel Kowert, Elizabeth Kilmer, and Alex Newhouse, “Taking It to the Extreme : Prevalence and Nature of Extremist Sentiment in Games,” *Frontiers in Psychology* 15, no. August (2024): 1–7, <https://doi.org/10.3389/fpsyg.2024.1410620>.

³² Nabil F Saleh et al., “Active Inoculation Boosts Attitudinal Resistance against Extremist Persuasion Techniques : A Novel Approach towards the Prevention of Violent Extremism,” *Behavioural Public Policy* 8, no. 3 (2024): 548–71, <https://doi.org/10.1017/bpp.2020.60>.

³³ Schlegel, “Jumanji Extremism ? How Games and Gamification Could Facilitate Radicalization Processes.”

users are not merely passive consumers of content but active participants who feel they have agency within the narrative being constructed.³⁴

In games, players often identify deeply with the avatars they control. When radical recruiters infiltrate these interactive spaces, this deep identification between players and their avatars becomes an effective channel for instilling ideological values, as the boundary between a player's digital identity and personal identity becomes increasingly blurred.³⁵ This phenomenon is known in psychology as the Proteus effect, in which a person's digital representation—their avatar—gradually influences that individual's attitudes and behaviour in the real world, so that the values adopted in the digital persona slowly become part of their actual personal identity.

This process of radicalization through gamification can be broken down into three interconnected stages. The first stage is the pre-radicalization stage, which represents the initial phase of exposure. At this stage, individuals typically enter the gaming space without any ideological intent, but are gradually exposed to content, symbols, or social interactions that carry ideological messages through mechanisms that appear ordinary and unsuspecting.³⁶ The key characteristic of this stage is the individual's lack of awareness that they are part of a larger process; exposure occurs incidentally through interactions that appear normal within the context of gaming, thus failing to trigger suspicion either from the individual in question or from outsiders who might be monitoring them.

The second stage is the indoctrination stage, in which the instillation of violent values is carried out subtly through “mods”—modifications made to alter game content so that it includes more explicit ideological elements, yet remains framed as part of a legitimate gaming experience³⁷. At this stage, exposure to ideological content increases

³⁴ Ines von Behr et al., *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (Santa Monica: RAND Corporation, 2013).

³⁵ Akin, “Communication With the Social Environment in Multiplayer Online Games : The Turkey Case.”

³⁶ Kowert, Kilmer, and Newhouse, “Taking It to the Extreme : Prevalence and Nature of Extremist Sentiment in Games.”

³⁷ Linda Schlegel, Lars Wiegold, and Constantin Winkler, “Exploring the Digital Extremist Ecosystem : A Preliminary Analysis of Hateful Posts on Mod DB,”

gradually, yet it remains packaged within an entertainment framework so that the exposed individual tends not to realize they are undergoing ideological indoctrination—they simply feel they are enjoying game content that is more “challenging” or “realistic.”

The third, and most crucial, stage is the platform migration stage, or the “dark funnel.” This stage involves the movement of individuals from open or semi-open gaming spaces to more closed and encrypted communication platforms, where ideological indoctrination can take place more intensively and directly without the risk of detection by game platform moderators.³⁸ This stage is structurally the most significant from a legal perspective, as it is here that radicalization shifts from a relatively monitorable space—gaming platforms with content moderation policies—to a space that is completely closed off from any external oversight. Overall, these three stages demonstrate that radicalization within the online gaming ecosystem is a gradual and interactive process, not a single, instantaneous event, and that the most critical point for preventive intervention lies in the transition between the second and third stages—before the platform migration occurs.³⁹

This “gamification” of radicalism supports Ware’s argument, which explains how online radicalization has entered its third generation—a generation characterized by decentralization, fragmentation, and platform migration.⁴⁰ Table 1 below summarizes a comparison of the three generations of online radicalization based on time period, platforms used, impact on the radicalization process, and impact on terrorist tactics and targets.

Frontiers in Psychology, no. February (2025): 1–15,
<https://doi.org/10.3389/fpsyg.2024.1502098>.

³⁸ Jacob Ware, “The Third Generation of Online Radicalization,” *Programs on Extremism at George Washington University* 2023, no. June (2023), <https://extremism.gwu.edu/third-generation-online-radicalization>.

³⁹ Linda Schlegel and Rachel Kowert, *Gaming and Extremism: The Radicalization of Digital Playgrounds*, ed. Linda Schlegel and Rachel Kowert (New York: Routledge, 2024).

⁴⁰ Ware, “The Third Generation of Online Radicalization.”

Table 1. The Three Generations of Online Radicalization

	First Generation	Second Generation	Third Generation
Time Period	1984 to mid-2000s	Mid-2000s to late 2010s	Late 2010s to now
Platforms	Forum sites and websites (one-way)	Large social media platforms, X, Facebook, YouTube, and Instagram	End-to-end encrypted apps, WhatsApp, Telegram, far-right apps like Gab and Parler
Impact on Radicalization	Radicals networks disseminate propaganda broadly and reach new recruits	Radicals and extremists tend to gather in “echo chambers”, a space in which the same views and perspectives continuously reinforced, deepening radicalization. At the same time, content exposure is pushed by the algorithm, accelerating this development. In this context, formal organization structure becomes less centralized, meanwhile a lot of extremist ideology are often realized through violence.	Ideology itself becomes less rigid as processes of “convergence” merge elements from different traditions. At the same time, humor and meme culture play a significant role in advancing radicalization and reinforcing group cohesion. Perpetrators are increasingly likely to publish manifestos and reference online communities or previous attackers as sources of inspiration. Moreover, the phenomenon expands to broader segments of society, with women and children becoming more involved in what is often described as “mass radicalization,” alongside the influence of mental health factors and various other vulnerabilities.

Impacts on Terrorist Tactics and Targetting	Instruction and coordination can now be conducted through virtual platforms.	Violence is increasingly carried out by individuals acting alone, often with minimal training, targeting vulnerable sites, and relying on relatively simple weapons.	Almost all violence now committed by lone actors, employing even more diffuse terrorist targeting, often aimed at “accelerating” collapse. Shortened “flash-to-bang” timelines, often contributing to less effective attacks from less professional fighters. All contributes to a climate of unpredictability
--	--	--	--

Sources: Jacob Ware “The Third Generation of Online Radicalization”, George Washington University (2023)

The first generation of online radicalization, which took place roughly from 1984 to the mid-2000s, was characterized by the use of forums and one-way websites, where radical networks widely disseminated propaganda to reach new recruits. The second generation, which emerged in the mid-2000s and continued through the late 2010s, coincided with the rise of major social media platforms such as X, Facebook, YouTube, and Instagram, which allowed radical and extremist groups to gather in “echo chambers”—spaces where shared views and perspectives are constantly reinforced without challenge from differing viewpoints.⁴¹

The third generation, which has evolved from the late 2010s to the present, is defined by decentralization, fragmentation, and a shift toward encrypted apps and alternative platforms such as WhatsApp, Telegram, and far-right apps like Gab and Parler.³⁹ In this generation, the ideology itself has become less rigid due to a process of “convergence” that blends elements from various distinct ideological traditions, while—from an operational perspective—it is characterized by the prevalence of lone-actor violence, often carried out by individuals with minimal training,

⁴¹ Ware.

targeting vulnerable locations with increasingly diffuse targets and frequently aimed at “accelerating” broader social conflicts.⁴²

It is within the context of this third generation of online radicalization that the gamification of radicalism becomes particularly evident. The decentralized, user-driven nature of the third generation allows individuals to achieve a sense of accomplishment, recognition, and personal significance through participation in an ideologically framed, gamified ecosystem.⁴³ The online gaming ecosystem further reinforces these dynamics by facilitating interactive, immersive, and socially connected experiences—a combination rarely found in either first- or second-generation forms of radicalization.⁴⁴ In this sense, third-generation online radicalization represents a stage in which gamification operates most fully as a mechanism of radicalization, making online gaming ecosystems spaces that require legal attention on par with conventional social media platforms.

Wave’s third generation directly becomes the foundation for empirical instrument design and the following legal analysis. Methodologically, whether or not the respondents have been invited to a private group chat in WhatsApp, Telegram, or Discord that talk about ideology outside of the game itself, designed to operate the migration dynamic platform identified by Ware as the characteristic of third generation digital radicalization. Analytically, this same dynamic explains why legal reform that will be proposed in the next section prioritizes institutional detection at the early stage: when radicalization moves from the gaming platform to a closed, private, encrypted communication channel, radicalization will move beyond practical and juridical reach of the platform operator obligation or any content moderation system. Therefore, legal intervention point identified by this study as the most urgent is not the migration itself, but the preceding moment, right where Ware’s model places the third generation’s structural vulnerability to supervision.

⁴² Ware.

⁴³ Akin, “Communication With the Social Environment in Multiplayer Online Games : The Turkey Case.”

⁴⁴ Schlegel and Kowert, *Gaming and Extremism : The Radicalization of Digital Playgrounds*.

C. Legal Reform: Rectifying Normative Gaps Regarding Radical and Extremist Content in Online Games

The previous discussion has stated that the online game ecosystem functioned as a supporting media for the third generation of digital radicalization, marked by decentralization, gamification, and platform migration, which operates through three main mechanisms: visual and narration infiltration, recruitment through the social features of the game, and the development of a psychosocial profile that serves as a prerequisite for lone-wolf attacks. This discussion has also stated that the three mechanisms are not hypothetical: the empirical data collected from 46 junior high school students in Gunungpati, Semarang has shown that these mechanisms operate in reality, measured, and consistent with the theoretical patterns described above, rather than a nationally representative finding. .

The question that now urgently needs to be answered is no longer whether this phenomenon exists, but whether the applicable laws can address it. The answer to this question has to be formulated normatively, not based on speculation: by dissecting the existing provisions, identifying their reach, and stating the norm's substance needed to fill the unaddressed gaps. This is what is called as legal reform in the context of this paper, not only a policy recommendation, but also identifying the normative gap, which arguably needs rectifying and filling by concrete legal instruments.

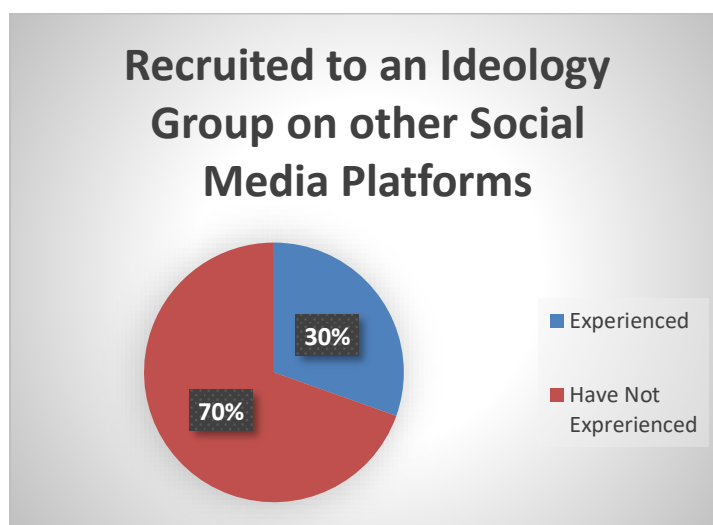
The Likert scale responses in the survey instrument (STS for "Sangat Tidak Setuju" or "Very Disagree" to SS for "Sangat Setuju" or "Very Agree) were re-coded into a binary scale: STS and TS were categorized as "Never" or "Not Exposed," while RR, S, and SS were categorized as 'Ever' or "Exposed." The inclusion for the neutral or hesitant (RR) response in the "Exposed" or "Experienced" is based on the uncertainty principle in the sensitive item for teenager surveys reflecting proto-consciousness without an institutional infrastructure: children have suffered something and their moral intuition has given

them danger signals, but they don't have the conceptual vocabulary or a safe reporting channel to confirm it.⁴⁵

1) First Normative Gap: The Absence of Legal Obligations for Gaming Platform Operators Regarding Social Features as Channels for Ideological Recruitment

As mentioned above, a questionnaire regarding junior high schools' habits and opinions on extreme content in online games was conducted as a way to collect data. One of the questions were whether or not the respondents had been invited to a private group chat (WhatsApp, Telegram, or Discord), which talk about ideologies outside of the context of the game, but still uses game as its entryway. As shown on Figure 2, about 30.4% respondents reported about facing such recruitment method.

Figure 2. Proportion of Respondents Who Have Been Recruited into External Ideological Communication Groups Through Social Features in Online Games (n=46)



Sources: Authors' Analysis (2026)

⁴⁵ Ivar Krumpal, "Determinants of Social Desirability Bias in Sensitive Surveys : A Literature Review," *Quality and Quantity* 47, no. 2013 (2025): 2025–47, <https://doi.org/10.1007/s11135-011-9640-9>.

This number is not an abstract indicator. It shows that almost 1 out of 3 junior high school students in Gunungpati, Semarang had faced what was identified by the Institute for Strategic Dialogue as game-based extremist recruitment resea: the transition from a gaming space to a closed, ideologically charged communication group, which constitutes a platform migration phase or “dark funnel” in the process of gamifying radicalism.⁴⁶ The legal statement is not “Is this dangerous?”, instead it’s “Are there any legal provisions that obligated anyone to prevent or respond it?”

The answer to the question above is, none. Law No. 5 of 2018 regulates the crime of recruitment in Article 12A and 12B, however those two articles require two conditions that are not met in this context: first, a relationship with an identified terrorist organization; and second, a proven or planned terrorist criminal act. Ideological recruitment via in-game chat features that are not linked to any terrorist organization and have not resulted in any criminal acts is not covered by these two articles. The Information and Technology Law as amended with Law No. 19 of 2016 obligated the removal of content that violates the law, but this obligation is content-centric and reactive, operating after reports are received; meanwhile, the social feature in games are not removable content, instead, it’s an in-game infrastructure that makes recruitment possible.⁴⁷ Government Regulations (PP) No. 71 of 2019 gives the Ministry of Communication and Information Affairs the authority to block electronic system that violates the provisions, but does not impose an obligation on platform operators to proactively monitor the use of community features for the purpose of ideological recruitment.

This gap is structural, not interpretative. No norms can be interpreted extensively to reach the obligation of game platform

⁴⁶ Davey, “Gamers Who Hate : An Introduction to ISD ‘ s Gaming and Extremism Series”; Schlegel, “Jumanji Extremism ? How Games and Gamification Could Facilitate Radicalization Processes.”

⁴⁷ William Allchorn and Elisa Orofino, “Policing Extremism on Gaming-Adjacent Platforms : Awful but Lawful ?,” *Frontiers in Psychology* 16, no. July (2025): 1–16, <https://doi.org/10.3389/fpsyg.2025.1537460>.

operator in supervising and reporting the ideological recruitment pattern through their social features. This gap filling and rectifying needs a new norm.

The norm needed is a norm that orders a digital due diligence for game platform operator as part of the counterterrorism architecture. The norm substance needs to at least fulfil three elements: first, proactive supervision by operator on in-platform or in-game social features, including voice chat, guild system, and group making mechanism, to detect communication pattern that indicates ideological recruitment; second, an obligation of reporting to the National Counterterrorism Agency when the recruitment indicator reaches beyond the established threshold by technical regulations; and third, the obligation to provide a reporting mechanism accessible for young users so that they can report a recruitment method faced without legal risk or social stigma. The most relevant comparative reference are assessment obligation and systemic risk mitigation as regulated in the Europe Union Digital Services Act, Article 34-35 for large scale online platform, can be adapted into Indonesian legal framework as scope extension of PP No. 71 of 2019 or the addition of a special chapter in Law No. 5 of 2018. Based on Article 34-35 of the Europe Union Digital Services Act, large-scale online platforms are obligated to do an annual systemic risk assessment, which includes fundamental rights risk and civic discourse, also implementing relevant mitigation steps that need to be audited independently. Adapting this model into the gaming platform context in Indonesia does not require Digital Service Act's infrastructure audit replication as a whole; on the contrary, this proposed a tailored framework in which gaming platform operators exceeding a certain user threshold conduct periodic risk assessments specific to in-game social features, with reporting obligations to the BNPT scaled to the platform's size and risk profile, thereby avoiding a one-size-fits-all compliance burden that would be disproportionate for smaller Indonesian game developers compared to global platforms.⁴⁸ A similar model can be found in

⁴⁸ Allchorn and Orofino.

the UK Online Safety Act 2023, which shifts platform obligations from reactive measures, such as content removal, to proactive risk management: service providers likely to be accessed by children are required to conduct “adequate and appropriate” child-related risk assessments, update them as services evolve, and take proportionate steps to mitigate identified risk, with enforcement by Ofcom involving sanctions of up to £18 million or 10% of global turnover. This “duty-of-care” obligation structure offers valuable lessons for the Indonesian context because it explicitly links the scope of platform obligations to a platform’s specific risk profile and user base, rather than imposing a uniform standard; this provides a practical framework for tailoring obligations to various entities, ranging from small-scale domestic game developers in Indonesia to large-scale international platforms. Australia’s Online Safety Act 2021 arguably offers the most directly relevant precedent, given that its “Basic Online Safety Expectations” framework explicitly encompasses gaming services; furthermore, the eSafety Commissioner has issued formal transparency notices to major gaming platforms—including Roblox, Minecraft, Fortnite, and Steam—requiring them to report on measures taken to protect users from various harms, such as extremist and violent content. This underscores that treating online gaming platforms as entities subject to regulation on par with social media—rather than viewing them as a category that is unregulated by default—is not a novel proposal, but rather an approach already implemented in comparable jurisdictions, thereby providing a practical precedent for the reforms proposed in this study for Indonesia.

2) Second Normative Gap: The Lack of an Institutional Bridge Between Children’s Awareness of the Dangers of Digital Radicalization and the State’s Response

Another question asked in the questionnaire was “Do respondents think the games that they play need strict supervision for provocative content?”. About 45.7% respondents, almost half of the number of the sample, gave signals of agreement on the question. This finding is not about content exposure, it’s about

awareness, instead: almost half of the teenagers surveyed have independently identify the need of institutional supervision on the digital environment that they live in, before adults or any institution who asks them to do it.

This finding opens a different legal issue from the first gap. If in the first gap's question is on who has the obligation to prevent, then in this one is on whether or not teenagers have realized the danger and the will to report it, to whom they need to report, and whether or not there is a norm that regulates the reporting mechanism.

The answer is once again: none or non-existent. The National Counterterrorism Agency deradicalization mandate in Article 43D of Law No. 5 of 2018 is intended for individuals who are proven and identified to be involved in a terrorist criminal act, not to children who have not done anything but have identified that their digital environment is dangerous. The Children Protection Act ordered collective responsibility in children protection in Article 20 of Law No. 35 of 2014, but it does not state any specific mechanism to detect or respond to digital radicalization exposure as a threat to children protection. The National Education System mandated character development and national identity in Article 3 of Law No. 20 of 2003, but it does not give an instrument to educational unit, including guidance counselors, to detect digital radicalization indicators and report it to the authority. As a result, guidance counselors who know or suspect an exposure of digital radicalization on their students do not have mandates, procedures, or legal protection to act.

This gap resulted in an institutional paradox: teenagers realize a dangerous situation, but the system that is supposed to protect them does not have a mechanism to receive and respond to the awareness. Schlegel and Kowert showed that the radicalism gamification process works in stages and results in cognitive dissonance at the early stage of exposure, before the full internalization happens.⁴⁹ This dissonance stage, as reflected in the

⁴⁹ Schlegel and Kowert, *Gaming and Extremism: The Radicalization of Digital Playgrounds*.

RR or hesitant response on sensitive items, which theoretically is the most responsive toward intervention. However, the institutional paradox above assures that the intervention window can pass without any institutional response.

The regulations needed to fill this gap are those that build an institutional bridge between children's awareness and the state's response. The substance of these regulations must include three inseparable components: first, designating guidance counselors as mandated reporters for indicators of digital radicalization—a status that transforms reporting from a voluntary act into a legal obligation; second, a standardized detection tool that provides Guidance Counselors with an operational framework for identifying indicators of digital radicalization among students, including adapting survey instruments such as those used in this study as an initial screening tool; and third, explicit legal protection for Guidance Counselors who report in good faith, so that the reporting obligation does not result in legal exposure for the reporter. The most appropriate legal instrument to incorporate these three components is a joint regulation between the Ministry of Education, Culture, Research, and Technology (Kemendikbudristek) and the National Counterterrorism Agency (BNPT), which operationalizes the BNPT's prevention mandate within the formal education system as the first line of early detection. The legal basis for such a joint regulation is found in Article 43D of Law No. 5 of 2018, which grants the BNPT a sufficiently broad prevention mandate to encompass interministerial coordination, combined with the Ministry of Education, Culture, Research, and Technology's general regulatory authority over the formal education system under Law No. 20 of 2003. Joint regulations issued by ministries and agencies are recognized instruments within Indonesia's legal and regulatory hierarchy for this type of cross-sectoral mandate; thus, there is no need for a comprehensive amendment to the law, yet such regulations still possess legally binding force for both institutions. As a ministry-level legal instrument, this joint regulation authorizes to regulate the reporting and supervisory obligations as mentioned above. Since this would be an administrative regulation, the form

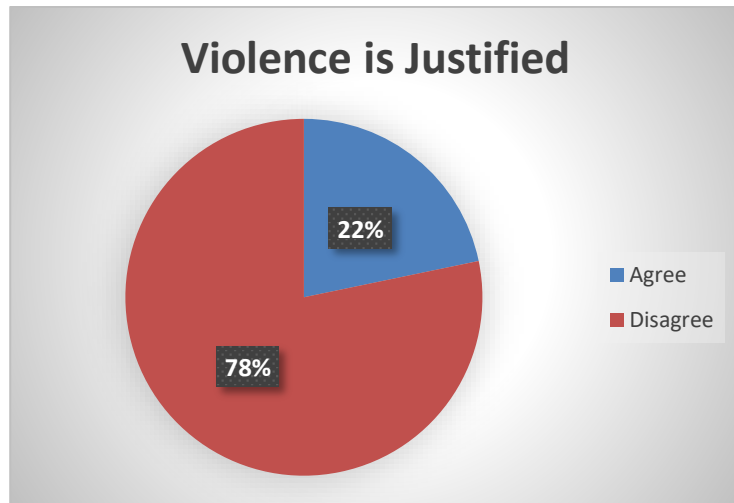
of punishments if the game developers don't do their due diligence in help preventing radicalization through their platform would be, formal warning, administrative fine, and suspension of operating license under the Government Regulation No. 71 of 2019 authority. However, this regulation does not have the authority to establish criminal sanctions, because this regulation requires that related obligations need to be codified in Law No. 5 of 2018 first through an amendment if a criminal law enforcement is needed. This approach aligns with the findings of the Global Network on Extremism and Technology that interventions based on formal education are the most effective means of intercepting the radicalization process at an early stage.⁵⁰

3) Third Normative Gap: The Lack of a Legal Category for Children in the Radicalization Process as Subjects of Protection, Not Subjects of Criminal Prosecution

Two questions in the questionnaire formed the empirical foundation for the most fundamental normative gaps. The first question in this is whether or not after playing the games, respondents feel that violence is a normal thing in fighting for their beliefs. As shown in Figure 3, about 21.8% of respondents gave signals of agreement to this question.

⁵⁰ Galen Englund and Luxinaree Bunmathong, "Understanding the Game: Bridging Research Gaps at the Nexus of Gaming and Extremism," Global Network on Extremism and Technology, 2022, [https://gnet-research.org/2022/03/09/understanding-the-game-bridging-research-gaps-at-the-nexus-of-gaming-and-extremism/#:~:text=In 2021%2C we developed a,inform areas of possible studies.](https://gnet-research.org/2022/03/09/understanding-the-game-bridging-research-gaps-at-the-nexus-of-gaming-and-extremism/#:~:text=In%202021%2C%20we%20developed%20a%2Cinformal%20areas%20of%20possible%20studies.)

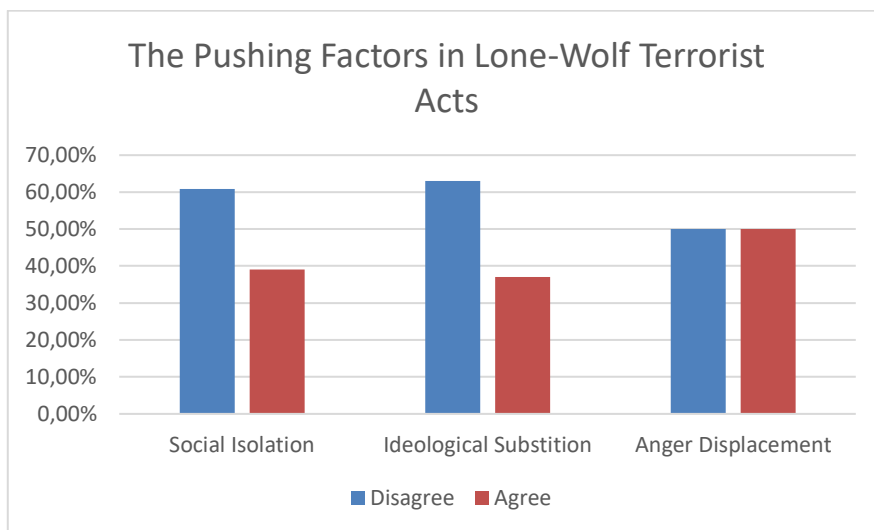
Figure 3. Proportion of Respondents Who Believe Violence Is Acceptable After Playing Video Games (I1) — Agree vs. Disagree (n=46)



Sources: Authors' Analysis

This finding shows that game content exposure does not stop at the consumption level; it results in measured value erosion. This is not a theoretical claim; this is actual empirical data that shows that for some junior high school students, the interaction with game content has shifted the perception of violence legitimacy. Moreover, the three questions below created the psychosocial profile that in contemporary terrorism literature are identified as prerequisites for lone-wolf activities. As shown on Figure 4 below, social isolation (39.1% exposure signal) reflected the dependency in game due to the feeling of not being understood in the real world; ideological substitute (37%) reflected a condition in which the game fills the function that is supposed to be filled by a value system and a healthy social community; and anger displacement (50%) reflected the condition in which game becomes the only outlet for social anger that is not channeled constructively.

Figure 4. Psychosocial Vulnerabilities as Prerequisites for Lone-Wolf Radicalization: Social Isolation, Ideological Substitution, and Displacement of Anger Among Junior High School Online Gamers (n=46)



Sources: Authors' Analysis

These three indicators formed what Moghaddam identified as a ground floor level to the second floor level in Staircase to Terrorism: the feeling of injustice, the failure to find a way out through a formal system, and the transfer of aggression toward a constructed enemy.⁵¹ This data does not show children who have already turned into terrorists, instead it shows children who are in the early stages of a process that, if left unchecked, could lead to acts of terrorism—particularly in the form of “lone-wolf” attacks, which Ware has identified as the dominant form of third-generation online radicalization, characterized by an increasingly short “flash-to-bang” trajectory.⁵²

The legal question is: Does Indonesian law have the means to reach these children, not to punish them, but to protect them from the proceedings they are currently facing?

⁵¹ Moghaddam, “The Staircase to Terrorism: A Psychological Exploration.”

⁵² Ware, “The Third Generation of Online Radicalization.”

The answer is no, and this gap is the most dangerous. Law No. 5 of 2018 does not regulate pre-criminal intervention based on a psychosocial risk profile. The National Counterterrorism Agency's deradicalization mandate under Article 43D applies only to individuals who have been identified as involved in terrorism. The Child Protection Law provides for the protection of children from violence, exploitation, and neglect, but does not conceptualize children undergoing a process of radicalization as subjects requiring special protection—this category is normatively distinct because the child is not a victim of violence perpetrated by others, but is being shaped into a perpetrator by an environment beyond their control. Juvenile criminal law under Law No. 11 of 2012 on the Juvenile Criminal Justice System can only apply to children after a criminal act has been committed. Thus, there is no third legal category: between ordinary citizens who receive no specific protection from radicalization and suspects or convicted offenders who receive deradicalization interventions, there is a gap occupied by children—whose presence, as the data in this study show, is significant in number.

Filling this gap requires the creation of a new legal category that explicitly recognizes children with a profile of psychosocial vulnerability to radicalization as subjects entitled to state intervention before a criminal act occurs. This category—which could be termed “Child Vulnerability to Radicalization”—must include three non-negotiable normative elements: first, an operational definition of what is meant by a child's vulnerability to radicalization, which can be formulated based on a combination of measurable psychosocial indicators such as those used in this research instrument; second, the establishment that children identified as meeting this definition are subjects of protection—not subjects of criminal punishment—so that the interventions provided take the form of psychosocial support, counter-narrative programs, and family counseling, rather than criminal legal proceedings; and third, the establishment of the state's obligation to provide these interventions as a child's right, not as a discretionary policy. In terms of implementation, this category could be integrated into the Child Protection Law as a form of

special protection in a separate chapter, or included as a chapter on individual-based prevention in the revision of Law No. 5 of 2018. What cannot be sustained is the current situation, in which children whose profiles match the data in Figures 2 and 3 have no legal status whatsoever to protect them from the processes that are shaping them. Concretely, it could be applicated through the addition of new chapter in Law No. 35 of 2014 about Child Protection which basically acknowledges children who fit under certain psychosocial vulnerability requirement as a protection subject that are entitled to psychosocial intervention, also states that the vulnerability condition does not constitute grounds for criminal investigation. Alternatively, these provisions could be incorporated into a dedicated individual-focused prevention chapter in a future amendment to Law No. 5 of 2018.

4) The Direction of Reform: From Counterterrorism Law to Terrorism Prevention Law

The three normative gaps identified below share the same denomination: Law No. 5 of 2018 in its current form, it is an instrument for countering terrorism, not for preventing it. It is designed to reach terrorism after it has happened, to define it punish it, and rehabilitate the perpetrators. It is not designed to reach the conditions that enable terrorism to occur, particularly those that have now emerged within the digital ecosystem, conditions that had no historical precedent when this law was first enacted.

The data presented in this study illustrate a reality that the legal framework for countering such threats cannot address: nearly one in three junior high school students has been subjected to ideological recruitment through video games, with no operator obligated to prevent it; nearly half of students are aware that their digital environment is dangerous, yet no institution has a mandate to address this awareness; and psychosocial profiles consistent with the prerequisites for lone-wolf actions are measurably present in a population that is entirely beyond the reach of any existing preventive norms. Most crucially, it must be understood that this situation is not an administrative loophole that can be filled with

circulars or technical policies. It is a normative void that requires legally binding norms, at both the statutory level and in subordinate regulations—that provide clear mandates, authorities, and obligations to the relevant actors.

The legal reform needed, therefore, is not the piecemeal addition of provisions to the existing Law No. 5 of 2018, but rather a paradigm shift in the way Indonesian law conceptualizes counterterrorism: from a post-incident response toward pre-incident prevention that encompasses three layers, platform operators as the infrastructure layer, educational institutions as the early detection layer, and child protection as the individual intervention layer. These three layers cannot function in isolation; their effectiveness depends on their integration within a single normative framework that explicitly recognizes that third-generation digital radicalization is a threat that cannot be addressed with first-generation legal instruments.

Conclusion

This research shows that the online gaming ecosystem functioned as the third arena for radicalization, which operates through a different qualitative mechanism from previous online extremism forms: narrative infiltration, symbol internalization, and recruitment through the in-game social features. The empirical data is gathered from 46 junior high school students in Gunungpati, Semarang, giving an explorative local evidence on the phenomenon that is usually analysed through Western case study; meanwhile the normative analysis on Law No. 5 of 2018, The Information, Technology, and Electronics Law, Government Regulation No. 71 of 2019, Child Protection Law, and National Education System Law has identified three normative gaps that are related to each other: the lack of due diligence for gaming platform operator, the lack of institutional bridge that connects child's awareness to state's response, also the none existing legal protection category for children who are currently facing radicalization process instead of punishing them.

This research has given the contribution in three aspects: theoretically, this research broadens the “Staircase to Terrorism” theory by Moghaddam and the third generation of radicalization by Ware into online game environment that still has a small number of researches; empirically, this research serves the first specific survey data on Indonesia context that connects the gaming behaviour in teenagers to radicalization indicators; and normatively, this research has identified the normative gaps in Indonesia’s counterterrorism framework also proposed specific norms to overcome them.

This finding indicated that the gamification functioned as the accelerator of the Staircase model, especially on the early stages, also supported Ware’s arguments that the third digital radicalization generation requires an analytical framework accounting for decentralized, platform-specific mechanisms, rather than the centralized organizational assumptions underpinning earlier models. Legal implications. Indonesia’s counter-terrorism framework remains oriented toward post-incident responses rather than pre-incident prevention. The reforms proposed in this study—including mandatory digital due diligence for platform operators, institutional detection mandates for schools, and legal protection categories for at-risk children, necessitate a paradigm shift from merely combating terrorism to actively preventing it. Limitations. The study’s findings are subject to limitations arising from a small sample size ($n=46$), a single geographic location, and a cross-sectional design that fails to capture the evolution of radicalization risk over time. Consequently, these findings should be viewed as exploratory and illustrative rather than statistically generalizable. Future research. Future studies would benefit from larger-scale surveys covering various regions of Indonesia to assess geographic and demographic variations, longitudinal designs that monitor psychosocial risk indicators over time, and comparative legal research examining the practical application of due diligence regimes for platform operators in other jurisdictions. Recommendations. For lawmakers: incorporate the three proposed normative provisions into amendments to Law No. 5/2018 or into the implementing government regulations. For the National Counterterrorism Agency: establish technical thresholds and reporting mechanisms for platform operators and schools within the framework of the proposed joint regulation. For the Ministry of Education and

Culture: pilot a model designating school counselors as mandated reporters and conduct training on the use of detection tools in schools. For gaming platform operators: begin voluntarily implementing monitoring and reporting practices for social features ahead of formal regulation. For schools: integrate awareness regarding digital radicalization into existing character education curricula as an immediate, non-legislative initial step.

References

- Adlini, Miza Nina, Anisya Hanifa Dinda, Sarah Yulinda, and Octavia Chotimah. "Metode Penelitian Kualitatif Studi Pustaka." *Edumaspul: Jurnal Pendidikan* 6, no. 1 (2022): 974–80. <https://doi.org/10.33487/edumaspul.v6i1.3394>.
- Akin, Mustafa Seref. "Communication With the Social Environment in Multiplayer Online Games: The Turkey Case." *International Journal of Game-Based Learning* 13, no. 1 (2023): 1–14. <https://doi.org/10.4018/IJGBL.330755>.
- Allchorn, William, and Elisa Orofino. "Policing Extremism on Gaming-Adjacent Platforms: Awful but Lawful?" *Frontiers in Psychology* 16, no. July (2025): 1–16. <https://doi.org/10.3389/fpsyg.2025.1537460>.
- Ameliah, Rizki, Rangga Adi Negara, and Bahtiar Minarto. "Status Literasi Digital Di Indonesia." Jakarta, 2023.
- Aminudin, Cecep, Prastyawan Nugroho, and Andri Sutrisno. "Media Sosial Dan Radikalisme: Bagaimana Teknologi Informasi Mempengaruhi Pemikiran Ekstrem." *Journal Humaniora: Jurnal Hukum Dan Ilmu Sosial* 01, no. 04 (2023): 110–15. <https://doi.org/10.37010/hmr.v1i4.31>.
- Asrori, Saifudin, and Amsal Bakhtiar. "Articulating Takfir: Ayman Al-Zawahiri and the Global Jihad Ideology." *Episteme: Jurnal Pengembangan Ilmu Keislaman* 16, no. 2 (2021): 167–87. <https://doi.org/10.21274/epis.2021.16.02.167-187>.
- Behr, Ines von, Anais Reding, Charlie Edwards, and Luke Gribbon. *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*. Santa Monica: RAND Corporation, 2013.

- Binder, Jens F, Jonathan Kenyon, and Caitlin Clemmow. "Terrorism and the Internet : How Dangerous Is Online Radicalization ?" *Frontiers in Psychology* 13, no. October (2022): 1–10. <https://doi.org/10.3389/fpsyg.2022.997390>.
- Capelos, Tereza, Kaitlyn Davisio, Mikko Salmela, and Kaitlyn Davisio. "“ Today I Die like Jesus Christ ‘: An Analysis of Ressentiment in Perceptions , Motivations and Justifications of Violent Extremist Manifestos.” *Terrorism and Political Violence* 37, no. 8 (2025): 1031–47. <https://doi.org/10.1080/09546553.2024.2379043>.
- Cauberghs, Olivier. "Hate the Player, Not the Game: Exploring Extremist and Terrorist Use of Games, Gaming Platforms and Gamification Strategies for Propaganda Purposes." *Radices: Interdisciplinary Journal for the Study of Terrorism & Extremism* 4, no. 1 (2024): 90–110. <https://doi.org/10.21825/radices.94142>.
- Cohen, Ben. "Shock in Germany After Neo-Nazi Gunman Who Attacked Synagogue on Yom Kippur Attempts Prison Escap." *The Algemeiner*, 2020. <https://www.algemeiner.com/2020/06/04/shock-in-germany-after-neo-nazi-gunman-who-attacked-synagogue-on-yom-kippur-attempts-prison-escape/>.
- Conway, Maura. "Determining the Role of the Internet in Violent Extremism and Terrorism : Six Suggestions for Progressing Research." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 77–98. <https://doi.org/10.1080/1057610X.2016.1157408>.
- Cresswell, J.W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. New York: SAGE, 2018.
- Davey, Jacob. "Gamers Who Hate : An Introduction to ISD ‘ s Gaming and Extremism Series," 2021.
- Dearden, Lizzie. "Stephan Balliet: The ‘Loser’ Neo-Nazi Suspected of Deadly Attack on German Synagogue." *Independent*, 2019. <https://www.independent.co.uk/news/world/europe/german-synagogue-shooting-halle-attack-latest-stephan-balliet-suspect-neo-nazi-a9150451.html#gsc.tab=0>.
- Englund, Galen, and Luxinaree Bunmathong. "Understanding the Game: Bridging Research Gaps at the Nexus of Gaming and Extremism." *Global Network on Extremism and Technology*, 2022. <https://gnet-research.org/2022/03/09/understanding-the>

game-bridging-research-gaps-at-the-nexus-of-gaming-and-extremism/#:~:text=In 2021%2C we developed a,inform areas of possible studies.

Europol. "European Union Terrorism Situation and Trend Report 2021," 2021. <https://doi.org/10.2813/677724>.

Greipl, Simon, Maximilian Lechner, Jannik Fischer, Heidi Schulze, Julian Hohner, and Diana Rieger. "Tracking down the Candy Crush Terrorist : The Fragile Relation between Gaming Motives and Radical Attitudes." *Frontiers in Psychology* 16, no. 1585576 (2025): 1–19. <https://doi.org/10.3389/fpsyg.2025.1585576>.

Holmes, Oliver, and Philip Oltermann. "Halle Synagogue Was Fortified before Antisemitic Attack." *The Guardian*, 2019. <https://www.theguardian.com/world/2019/oct/11/halle-synagogue-fortified-ahead-antisemitic-attack-germany>.

James, Thomas, Vaughan Williams, and Calli Tzani. "Behavioral Sciences of Terrorism and Political Aggression How Does Language Influence the Radicalisation Process ? A Systematic Review of Research Exploring Online Extremist Communication and Discussion Systematic Review of Research Exploring Online Extre." *Behavioral Sciences of Terrorism and Political Aggression* 16, no. 3 (2024): 310–30. <https://doi.org/10.1080/19434472.2022.2104910>.

Koehler, Daniel. "The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat." *CTC Sentinel* V, no. December 2018 (2019): 14–20. <https://ctc.westpoint.edu/halle-germany-synagogue-attack-evolution-far-right-terror-threat/>.

Kowert, Rachel, Elizabeth Kilmer, and Alex Newhouse. "Taking It to the Extreme : Prevalence and Nature of Extremist Sentiment in Games." *Frontiers in Psychology* 15, no. August (2024): 1–7. <https://doi.org/10.3389/fpsyg.2024.1410620>.

Krumpal, Ivar. "Determinants of Social Desirability Bias in Sensitive Surveys : A Literature Review." *Quality and Quantity* 47, no. 2013 (2025): 2025–47. <https://doi.org/10.1007/s11135-011-9640-9>.

Mahatva, Eka, Yudha Pujo, and Widodo Rudy. "Strategi Badan Nasional Penanggulangan Terorisme (BNPT) Indonesia Dalam Menghadapi Ancaman Paham Radikal." *Aurelia: Jurnal*

- Penelitian Dan Pengabdian Masyarakat Indonesia* 4, no. 2 (2025): 2382–89. <https://doi.org/10.57235/aurelia.v4i2.5657>.
- Maksin, Mastina. “Strategi Pemerintah Dalam Mencegah Paham Radikalisme Di Era Penggunaan Media Sosial Di Kalangan Remaja.” *Journal of Humanity Studies* 1, no. 2 (2022): 85–94. <https://doi.org/10.22202/jhs.2022.v1i2.6495>.
- Marizaldi, Deki, Muhammad Herdi Pratama, and Abipraya Guntur Sulatiasto. “From Clicks to Violence : A Study on the Role of Social Media in Radicalization and Terrorism.” *Jurnal Akta* 12, no. 2 (2025): 417–33. <https://doi.org/10.30659/akta.v12i2.44872>.
- Moghaddam, Fathali M. “The Staircase to Terrorism: A Psychological Exploration.” *American Psychologist* 60, no. 2 (2005): 161–69. <https://doi.org/10.1037/0003-066X.60.2.161>.
- New Zealand Police. “2019 - Operation Deans Terrorist Attack, Ōtautahi Christchurch, 15 March.” New Zealand Police, 2019. <https://www.police.govt.nz/about-us/history-and-museum/museum/exhibitions/place-many-brave-deeds/2019-operation-deans-terrorist>.
- Ogele, Eziho Promise. “The Intersection of Gaming and Terrorism : Exploring the Role of Online Gaming in Terrorist Recruitment Methods.” *Political Observer: Portuguese Journal of Political Science* 2024, no. 22 (2024): 23–39. <https://doi.org/10.59071/2795-4765.RPCP2024.22/pp.23-39>.
- Orsini, Alessandro. “Studies in Conflict & Terrorism What Everybody Should Know about Radicalization and the DRIA Model DRIA Model.” *Studies in Conflict & Terrorism* 46, no. 1 (2023): 68–100. <https://doi.org/10.1080/1057610X.2020.1738669>.
- Rivanieparawansa, Syarif Saddam, Koesrianti Koesrianti, and Toetik Rahayuningsih. “Prevention of Radicalism in the Cyberspace in Indonesia.” *International Journal of Humanities Social Sciences and Education* 6, no. 7 (2019): 63–72. <https://doi.org/10.20431/2349-0381.0607007>.
- Salah, Nabil F, Jon Roozenbeek, Fadi A Makki, William P Mcclanahan, and Sander Van Der Linden. “Active Inoculation Boosts Attitudinal Resistance against Extremist Persuasion Techniques : A Novel Approach towards the Prevention of Violent

- Extremism.” *Behavioural Public Policy* 8, no. 3 (2024): 548–71. <https://doi.org/10.1017/bpp.2020.60>.
- Schlegel, Linda. “Jumanji Extremism ? How Games and Gamification Could Facilitate Radicalization Processes.” *Journal for Deradicalization* Summer 202, no. 23 (2020): 1–44. <https://journal-derad.com/index.php/jd/article/view/359>.
- Schlegel, Linda, and Rachel Kowert. *Gaming and Extremism : The Radicalization of Digital Playgrounds*. Edited by Linda Schlegel and Rachel Kowert. New York: Routledge, 2024.
- Schlegel, Linda, Lars Wiegold, and Constantin Winkler. “Exploring the Digital Extremist Ecosystem : A Preliminary Analysis of Hateful Posts on Mod DB.” *Frontiers in Psychology*, no. February (2025): 1–15. <https://doi.org/10.3389/fpsyg.2024.1502098>.
- Schulzke, Marcus. “Simulating Terrorism and Insurgency: Video Games in the War of Ideas.” *Cambridge Review of International Affairs* 27, no. 4 (2014): 627–43. <https://doi.org/10.1080/09557571.2014.960508>.
- Sheldon, Jon, and Kristie Pladson. “Police Investigate Anti-Semitism Links in Halle Shootings.” DW, 2019. <https://www.dw.com/en/police-investigate-anti-semitism-links-in-halle-shootings/a-50764327>.
- The Royal Commission of New Zealand. “Executive Summary of the Christchurch Shootings.” The Royal Commission of New Zealand, 2019. <https://christchurchattack.royalcommission.nz/the-report/executive-summary-2/executive-summary>.
- Ware, Jacob. “The Third Generation of Online Radicalization.” *Programs on Extremism at George Washington University* 2023, no. June (2023). <https://extremism.gwu.edu/third-generation-online-radicalization>.
- Wells, Garrison, Agnes Romhanyi, Jason G Reitman, Reginald Gardner, Kurt Squire, and Constance Steinkuehler. “Right-Wing Extremism in Mainstream Games : A Review of the Literature.” *Games and Culture* 19, no. 4 (2024): 469–92. <https://doi.org/10.1177/15554120231167214>.

Acknowledgment

None.

Funding Information

None.

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement

None.