International Journal of Arts, Commerce and Humanities (IJACH)

eISSN:2347-694X www.journalijach.com

ONLINE GAMES, DIGITAL COMMUNITIES, AND THE RADICALIZATION OF YOUNG LONE WOLF: CYBER POLICING BASED PREVENTION MODEL IN INDONESIA

Rohiqum Noberta[1], **Dr. Supardi Hamid, M.Si.**[2]

[1,2]*Doctoral Program in Police Science, Sekolah Tinggi Ilmu Kepolisian*

Abstract: This study discusses the relationship between online games, digital communities, and the radicalization of lone wolf youth in the perspective of cyber policing in Indonesia. The digital space now functions not only as entertainment, but also as an arena for identity formation, social relations, solidarity, and the search for recognition. This research uses qualitative methods through literature studies and policy analysis. The study combines literature on online radicalization, lone actor terrorism, social identity theory, social learning theory, routine activity theory, situational action theory, algorithms, artificial intelligence, and cyber policing. The results of the study show that online games are not the direct cause of radicalism. Risks arise when the digital ecosystem is exploited by extreme actors through anonymity, closed communities, symbols of violence, recommendation algorithms, and young people's need for a sense of belonging. This study also confirms that lone wolf perpetrators can act alone, but the radicalization process is still influenced by digital communities, extreme narratives, and reference figures. Therefore, prevention needs to be directed at a preventive-collaborative cyber policing model that combines risk-based early detection, digital literacy, counter-narrative, platform cooperation, child protection, assistance to vulnerable groups, and legal accountability.

KEYWORDS: online games, digital communities, radicalization, lone wolf, cyber policing.

1. INTRODUCTION

The development of digital technology is changing the way radicalism spreads, adapts, and reaches vulnerable groups. Radicalization no longer takes place only through physical forums, closed lectures, organizational networks, or face-to-face meetings. Cyberspace is an important arena in the spread of ideology, identity formation, propaganda communication, recruitment, and mobilization of violence. The internet provides a space for like-minded individuals to find each other, discuss, build solidarity, and strengthen extreme beliefs. In this context, digital radicalism needs to be understood as an issue of security and police science that continues to develop.[1]

However, this study does not place the internet as the sole cause of radicalism. Such a view oversimplifies the problem. The internet, social media, online games, and digital communities are more appropriately understood as facilitation spaces. Such spaces can accelerate exposure, expand interactions, and reinforce extreme identities when confronted with individual vulnerability, weak digital literacy, social isolation, identity seeking, and hateful narratives. Therefore, digital radicalization needs to be read as a socio-technological process that involves individuals, platforms, algorithms, communities, and the social environment.[2]

Academic debates about the relationship between media and radicalization demonstrate the importance of a cautious attitude. Exposure to radical content online has a relationship with cognitive and behavioral radicalization, but that relationship doesn't work mechanically. Not every individual who sees extreme content will turn radical. The radicalization process is still influenced by personal, social, ideological, psychological, and situational factors. Thus, the study of digital radicalization needs to avoid conclusions that place digital media as the sole cause of extreme violence.[3]

In the context of young people, the digital space has an increasingly important meaning. Young people don't just use the internet to find information or entertainment. They also use it to build identity, seek recognition, form social networks, express views, and gain a sense of belonging. Online games, social media, streaming platforms, community forums, and private conversation channels have become part of everyday social life. This change

makes online radicalization need to be seen through the relationship between user behavior, platform algorithms, community interaction, identity needs, and social dynamics of young people.[4]

Online games and digital communities are important to study because they both provide an intensive interaction space. In the space there is anonymity, group language, community symbols, peer relations, solidarity, competition, and social recognition. Under certain conditions, the feature can be leveraged by extreme actors to insert hateful narratives, glorification of violence, conspiracy theories, anti-state sentiments, or ideological propaganda. However, this study does not state that online gaming causes radicalism. Online games are understood as a new social space that can become an arena of vulnerability when young people are in a fragile psychological, social, and ideological condition.

This phenomenon is related to the lone wolf or lone actor terrorism pattern. Lone wolf offenders are often understood as individuals who act alone without direct command from the organization. However, self-understanding does not always mean being disconnected from social influence. Many lone actors remain connected to radical environments, symbolic networks, extreme communities, ideological figures, or violent discourse currents. The relationship can take place directly or indirectly, both in the online and offline space. Therefore, lone actor radicalization is more accurately understood as a relational pathway, which is a process formed by social relations and interaction with the radical environment.[5]

The main difficulty in dealing with the lone wolf lies in its movement patterns that are not always visible in formal organizational structures. Perpetrators can move soloistically, use simple attack methods, and make preparations with a more limited footprint than group-based perpetrators. In some cases, social isolation, limited social skills, and low access to formal groups can encourage individuals to pursue violent paths independently. This condition makes early detection more complicated, especially when the radicalization process takes place in a private, anonymous, and dispersed digital space.[6]

In the Indonesian context, this issue is relevant because young people are very close to the internet and social media. Social media can be a space for spreading propaganda, forming opinions, exploiting anonymity, and reaching out to targets who are looking for identity. At the same time, filter bubbles, echo chambers, weak digital literacy, and freedom of interaction on social media can strengthen young people's vulnerability to radical narratives. Thus, young people need to be understood not only as users of technology, but also as subjects who can be in a vulnerable position to ideological influence in the digital space.[7]

The development of platform algorithms and artificial intelligence has also added to the complexity of threats. Recommendation systems can amplify exposure to extreme content on certain platforms. These risks are not always the same on every platform, but they are still worth considering because algorithms can iterate, sort, and personalize content based on user behavior. Artificial intelligence can also be used to create propaganda that is fast, personalized, and difficult to detect, including through generative content, automated bots, deepfakes, and behavioral profiling. This condition shows that digital radicalization is not only related to content, but also to the way content is produced, disseminated, amplified, and personalized.[8]

From the perspective of Police Science, this problem demands the strengthening of cyber policing. Cyber policing is not sufficiently understood as cyber patrol to find and remove radical content. Cyber policing needs to be directed at early detection, risk mapping, network analysis, digital literacy, cross-agency cooperation, platform cooperation, child protection, and supervision that remains subject to the principles of legality, accountability, privacy, and human rights. The study on Densus 88 shows that social media has been used as an intelligence gathering instrument through activity monitoring, network analysis, classification, clustering, and sentiment analysis. However, major challenges remain, especially the large volume of data, the complexity of information, the difficulty of distinguishing real threats from ordinary activities, and the need to maintain a balance between security and privacy rights.[9]

Online radicalization studies have grown rapidly, but they still leave some gaps. First, many studies have addressed social media, websites, extreme forums, or conversational apps, but not many have placed online games and digital communities as social spaces for young people. The literature has made it clear that peer-to-peer gaming, streaming, video sharing, and social media are changing the landscape of online radicalization. However, the discussion has not been much directed at Indonesia's cyber policing prevention model.[10]

Second, research on lone wolves often emphasizes individual character, psychological background, social isolation, and differences with group-based perpetrators. Studies linking lone wolves to online game ecosystems, digital communities, algorithms, and self-radicalization of young people still need to be developed.

[11] Third, cyber policing research in Indonesia has discussed the use of social media by Densus 88, but has not studied much about the digital ecosystem of young people which includes online games, streaming communities, private channels, and recommendation algorithms. [12]

Fourth, research on online radicalization prevention interventions is still not empirically strong. One systematic review found that there had not been any publications that met the main objective of public mental health interventions that specifically addressed online radicalisation. These findings demonstrate the need for a prevention model that is evidence-based, multidisciplinary, and applicable to young groups.[13]

Based on this gap, this article aims to analyze the relationship between online games, digital communities, and the radicalization of young people's lone wolf in the context of cyber policing in Indonesia. This article also formulates contextual prevention models with attention to early detection, digital literacy, platform cooperation, child protection, cross-agency collaboration, legal accountability, and privacy rights. The novelty of the article lies in the shift in focus from online radicalization based on general social media to online gaming ecosystems and digital communities as social spaces for young people. This article places the lone wolf not as a completely isolated individual, but as an actor who can be formed through digital relationships, extreme narratives, and platform distribution mechanisms.

This issue is also important because young people are in a digital environment that is constantly moving. They can move from gaming spaces to community forums, from public spaces to private channels, and from light conversations to more closed ideological spaces. The shift makes the lines between entertainment, communication, political expression, and propaganda not always easy to distinguish. In situations like this, a police approach that only seeks explicit content is no longer adequate. Authorities need to read interaction patterns, changes in communication intensity, community relations, and social context that accompany young people's digital behavior.

This article also places the protection of young people as part of the security strategy. Young people who are exposed to extreme content are not always in the position of the perpetrator. Some of them are in the vulnerable phase, confused, isolated, or looking for a reception space. Therefore, the state's response must distinguish between initial exposure, ideological sympathy, active support, and violent intent. This distinction is important so that cyber policing does not turn into overly broad surveillance, but is still able to work quickly when risk signs begin to lead to violent mobilization.

2. LITERATURE REVIEW

2.1 Social Identity Theory and Youth Digital Identity

The Social Identity Theory developed by Henri Tajfel and John C. Turner explains that individuals build self-identity through membership in a group. A person not only defines himself as an individual, but also as part of a particular group. Group membership gives us a sense of belonging, status, meaning, and boundaries that distinguish us from them. In the digital space, such identities can be formed through usernames, avatars, roles in the game, community reputation, internal symbols, and group language.[14]

This theory helps explain why young people may be drawn to digital communities that offer solidarity, status, symbols, and a sense of belonging. When young people experience social isolation, identity crisis, disrespect, or dissatisfaction with the social environment, digital communities can become a compensatory space. If the community contains a narrative of hatred, glorification of violence, or anti-state sentiment, then the process of identity formation can move in an extreme direction.

Extreme identity formation often works through a sharp distinction between in-group and out-group. The group itself is described as the righteous, oppressed, or has a moral mission. Other groups are portrayed as enemies, threats, traitors, or targets of hostility. This pattern can reinforce justifications for violence, especially when identity needs meet narratives, networks, and reference figures that provide ideological legitimacy. In the concepts of needs, narratives, and networks, radicalization moves when psychological needs gain direction through ideological stories and are strengthened by social relations.[15]

In online gaming communities, identity is not always built through direct ideological conversations. Identity can be born from roles in games, shared victories, status in groups, internal humor, and loyalty to the community. This structure provides space for young people to feel recognized. Problems arise when such confessions are associated with symbols of hatred, contempt for other groups, or loyalty to violent narratives. At that stage, digital identities can shift from ordinary social expressions to exclusive and confrontational group identities.

Social identity theory also helps explain why a counter-narrative that is merely informative is often not enough. Young people who have gained a sense of belonging from extreme communities do not only need counter information. They also need an alternative social space that gives recognition, status, and meaning. Therefore, prevention needs to build a positive community, not just refute extreme narratives. In the context of online gaming, gamer communities, schools, families, and digital platforms can be important actors to create healthy identity spaces.

2.2 Social Learning Theory, Routine Activity, and Situational Action

The Social Learning Theory from Albert Bandura explains that behaviors, attitudes, and values can be learned through observation, imitation, reinforcement, and social interaction. In the digital space, the learning process does not always happen through direct instruction. Young people can learn from videos, memes, comments, symbols, narratives, digital figures, streamers, extreme influencers, or community members who are considered influential.[16]

In the online gaming ecosystem, social learning can take place gradually. In the early stages, young people may only be exposed to dark humor, provocative symbols, hate speech, or conspiratorial narratives that are perceived as jokes. In the next stage, that exposure can turn into the normalization of violence, the acceptance of extreme narratives, and the justification of aggressive actions. When this process is reinforced by group recognition, young people can feel that extreme views confer social status in the community.

Routine Activity Theory explains that crime can occur when there are motivated perpetrators, appropriate targets, and the absence of effective guards. In the cyber context, these three elements can be translated into the relationship between extreme actors, vulnerable users, and weak digital surveillance. Motivated perpetrators can be extreme actors or radical sympathizers. Appropriate targets can be young people experiencing identity crises, social isolation, or a strong need to be accepted. The absence of effective guards can be in the form of weak family supervision, low school literacy, limited platform moderation, and suboptimal early detection by the authorities.[17]

Situational Action Theory describes the relationship between the individual and the environment in the formation of actions. Deviant actions are understood as the result of an interaction between the moral tendencies of the individual and the character of the environment in which the individual belongs. Thus, behavior is not only determined by individual character. Behavior is also influenced by social situations that provide opportunities, pressures, norms, and justification. In this study, the theory helps explain why young people in certain digital communities may experience a change in their perspective on violence.[18]

The digital space accelerates the social learning process because interactions occur repeatedly and can last indefinitely. Young people can see the community's response to certain symbols, learn which ones are being praised, and adjust their behavior to be accepted. In the long run, social validation can make hate speech, verbal violence, or the glorification of attacks seem natural. This kind of learning is not always noticed by users because it is present as part of the community culture.

Routine Activity Theory also provides a basis for seeing the importance of guardians in the digital space. Guardians do not always have to be state apparatus. Parents, teachers, community moderators, digital platforms, peers, and gamer communities can also serve as social guardians. When they have good digital literacy, they can recognize behavioral changes, help report risky content, or direct young people to healthier support spaces. Therefore, digital guarding needs to be understood as a distributed social work, not just a police task.

2.3 Social Embeddedness in Lone Actor Terrorism

The concept of social embeddedness is used to criticize the view that lone wolves are truly self-contained. In many cases, lone actors can indeed act without the direct command of the organization. However, the radicalization process can still be influenced by social networks, ideological communities, reference figures, extreme narratives, and movement symbols. Malthaner, O'Connor, and Lindekilde emphasized that lone actor terrorism has a social and collective dimension. They offer a relational pathway to explain that lone actor radicalization is formed by patterns of relationships, interactions, and connections to extreme environments.[19]

Schuurman and Carthy show that lone actors have different characteristics from group-based actors, especially in aspects of social isolation, social skills, and access to the group environment. This finding is important because the prevention of lone wolf is not enough to be done by looking for a formal organizational structure. Prevention should also read social, psychological, and digital signs that indicate a change in an individual's orientation toward violence. In the context of online gaming and digital communities, the perpetrator may not be

a member of a formal organization, but still absorb ideas, symbols, justifications, and inspiration of violence from the digital environment.[20]

2.4 Algorithm, Artificial Intelligence, and Digital Radicalisation

Digital radicalization is not only related to the existence of extreme content. Radicalization also has to do with the way content is discovered, repeated, recommended, personalized, and amplified by platforms. In this context, algorithms have an important role because they can determine which content appears, to whom the content is displayed, and how often it is recommended.

Whittaker, Looney, Reed, and Votta point out that recommendation systems can amplify concerns about extreme content amplification. Their research found that YouTube showed a tendency to amplify extreme and fringe content after users interacted with far-right material, while Reddit and Gab did not show the same pattern. These findings are important because they show that the impact of algorithms is contextual and cannot be generalized across all platforms.[21]

In addition to recommendation algorithms, artificial intelligence expands the complexity of digital radicalization. AI can be used for propaganda personalization, generative content creation, automated message delivery, deepfakes, bots, and behavioral profiling. Ganaie explained that extreme groups can leverage AI technology to identify vulnerable individuals, amplify ideological messages, create echo chambers, and accelerate the spread of propaganda through digital systems that are difficult to monitor conventionally.[22]

2.5 Cyber Policing and Conceptual Framework

Cyber policing in this study is understood as a function of policing in cyberspace which includes prevention, early detection, monitoring, risk analysis, enforcement, public education, and cross-actor collaboration. Cyber policing is not only oriented towards law enforcement after a violation occurs. It also needs to serve as a prevention mechanism capable of reading risk patterns before the threat develops into an act of violence.

In the context of digital terrorism, cyber policing includes extreme content mapping, network analysis, identification of communication patterns, detection of shifts to private channels, digital literacy, counter-narrative, and cooperation with platforms. The study of Densus 88 shows that social media provides a stream of data that can be used to monitor activities, see trends, and identify threats early. However, the study also points to the challenges of large volumes of data, the complexity of information, the difficulty of distinguishing real threats from ordinary content, and the need to strike a balance between security and privacy rights.[23]

The conceptual framework of this research connects five elements. First, young people as vulnerable subjects who are in the identity formation phase and need social recognition. Second, online games and digital communities as social spaces that allow interaction, solidarity, and the exchange of symbols. Third, digital radicalization mechanisms that include exposure to extreme content, community interaction, echo chambers, filter bubbles, recommendation algorithms, and the move to private channels. Fourth, lone wolves as extreme potential outputs that can act on their own, but are still influenced by the digital social environment. Fifth, cyber policing as a prevention model that combines early detection, risk analysis, digital literacy, counter-narrative, platform cooperation, child protection, and legal accountability.

Conceptually, the risk relationship can be formulated as follows: the vulnerability of young people, the online gaming ecosystem and digital community, exposure to extreme narratives, algorithms and echo chambers, and weak social surveillance can increase the risk of self-radicalization towards the lone wolf. On the other hand, preventive cyber policing, digital literacy, risk analysis, platform cooperation, child protection, and cross-agency collaboration can reduce these risks. This framework affirms that prevention must move from a content approach to an ecosystem approach.

The framework also emphasizes that cyber policing should not be solely centered on technical capabilities. Technological capabilities are important, but preventing radicalization of young people requires social sensitivity, understanding of digital culture, and the principle of protecting rights. Good early detection must be able to distinguish between crude jokes, emotional expression, passive exposure, ideological support, and indications of violent mobilization. Without that distinction, policies can produce two risks at once: failing to detect a real threat or marking a harmless individual as a threat.

In the Indonesian context, this conceptual framework needs to be placed in cross-agency work. The National Police and Densus 88 have a major role in law detection and enforcement. Indonesia's National Counter Terrorism Agency plays a role in the prevention of violent extremism. The Indonesian Child Protection

Commission needs to ensure a child protection perspective. Ministry of Communication and Digital Affairs plays a role in the governance of the platform. The school, family, and gamer community serve as the closest social guards. This division of roles is important because digital radicalization cannot be prevented by one institution alone.

3. METHOD

This research uses a qualitative method with a literature study and policy analysis approach. This method was chosen because the issue of online gaming, digital communities, the radicalization of young lone wolves, and cyber policing requires conceptual reading of the scientific literature, research reports, policy documents, and relevant open sources. The research is not directed to quantitatively examine cause-and-effect relationships, but to understand patterns, mechanisms, vulnerabilities, and models of prevention in the context of Police Science.[24]

The literature study approach is used to examine the concepts, theories, and findings of previous research related to online radicalization, lone actor terrorism, social media algorithms, artificial intelligence, digital communities, and cyber policing. The policy analysis approach is used to read how the state, police, counter-terrorism agencies, digital platforms, families, schools, and communities can be placed in a single prevention ecosystem.

Research data sources consist of three types. First, academic sources are in the form of theory books, journal articles, systematic reviews, and research reports on online radicalization, lone actor terrorism, digital media, algorithms, artificial intelligence, and cyber policing. Second, policy sources are in the form of documents related to terrorism prevention, cybersecurity, child protection, and digital platform governance. Third, open sources that can be accounted for strengthening social and technological contexts as long as they are relevant to the focus of the research.

Data collection techniques are carried out through documentation and literature search. The literature was selected based on four criteria: it is relevant to the research theme, has academic or institutional credibility, makes a conceptual or empirical contribution to the understanding of digital radicalization, and can be used to build a prevention model that is appropriate to the Indonesian context. Document analysis was chosen because this research relies on a systematic reading of written sources, both in the form of scientific articles, institutional reports, and policy documents.[25]

The data analysis technique uses qualitative content analysis and thematic analysis. Content analysis is used to read the substance of the literature, especially repetitive concepts, findings, arguments, and recommendations. Thematic analysis was used to group the data into key themes, namely the vulnerability of young people, online gaming ecosystems, digital communities, self-radicalization, lone wolf, algorithms, artificial intelligence, and cyber policing. The results of the analysis are then synthesized to formulate a conceptual framework and prevention model.[26]

This research has ethical limitations. The study did not infiltrate closed extreme groups, did not collect personal data of digital users, did not analyze specific individual accounts, and did not operationally map extreme networks. The research uses only academic literature and open sources that can be accounted for. These restrictions are important so that research stays within the ethical corridor, does not expand the distribution of extreme content, and does not infringe on individual privacy.

The analysis steps are carried out through four stages. The first stage is the mapping of the main concepts from the literature, namely online radicalization, online games, digital communities, lone actors, algorithms, artificial intelligence, and cyber policing. The second stage is the grouping of arguments based on themes, such as identity, social learning, digital opportunity, lone actor relationships, and platform governance. The third stage is the synthesis between theory and the Indonesian context. The fourth stage is the preparation of a prevention model that can explain the relationship between young people's vulnerability, the digital space, and cyber policing interventions.

Conceptual validity is maintained through source triangulation. This article does not use just one type of literature. The sources used include classical theory, empirical journal articles, systematic reviews, research reports, and studies on cyber policing practices in Indonesia. In this way, the argument does not rest on one discipline alone, but combines criminology, terrorism studies, social psychology, digital media studies, and Police Science.

4. RESULT AND DISCUSSION

4.1 Online Games and Digital Communities as Youth Social Spaces

Online gaming and digital communities need to be understood as social spaces, not just entertainment spaces. Young people don't just play, compete, or fill their free time in digital platforms. They also build social relationships, display identity, seek recognition, form solidarity, and gain a sense of belonging. In this context, online games can serve as new social spaces that bring together individuals from different backgrounds through conversations, teamwork, competitions, symbols, avatars, and cross-platform communities.

This change is important because the radicalization of young people does not always start from a formal ideological forum. The initial process can arise through seemingly mundane interactions, such as in-game conversations, community chat rooms, fan forums, streaming channels, or private groups formed from game relationships. In spaces like these, young people can find groups that provide social support, recognition, and alternative identities. When communities carry narratives of hate, extreme symbols, or glorification of violence, the entertainment space can turn into a space of vulnerability.

Social Identity Theory helps explain this pattern. Young people tend to look for groups that give them a sense of security, status, and meaning. In digital communities, identities can be formed through usernames, avatars, in-game roles, community reputation, group symbols, and internal language. Such an identity can be positive when it is directed towards solidarity, creativity, and cooperation. However, identities can also shift towards exclusivity as communities build sharp boundaries between us and them. Boundaries are dangerous when outside groups are positioned as enemies, threats, or targets of hatred.

The risk does not lie in online gaming as a technology. Risks arise when online games connect with digital communities that produce violent narratives, utilize anonymity, and socially reward extreme behavior. Young people's vulnerability can arise due to identity searches, experiences of social isolation, frustration, failure to gain recognition in the real environment, weak digital literacy, and lack of family or school assistance. When these conditions meet with digital communities that offer simple answers to complex problems, young people can begin to accept extreme narratives as a source of new meaning.

Digital communities also have a distinctive social structure. There are users who are the center of attention, moderators, senior players, content creators, and new members looking for positions. Structures like this can create an informal learning process. New members learn from existing members about community norms, language styles, accepted symbols, and boundaries of behavior that are considered appropriate. If community norms are healthy, this process can strengthen cooperation and creativity. If community norms contain hatred and violence, the same process can accelerate the normalization of extremism.

On the other hand, digital communities can be a protective space. Many gaming communities actually build solidarity, cooperation, and emotional support. Therefore, this study does not see the gamer community as a threat. The focus of the analysis lies in situations when community spaces are exploited by extreme actors or when community cultures allow symbols of hate to flourish without correction. This distinction is important so that the policy does not stigmatize the gaming community, but encourages them to be part of prevention.

4.2 Mechanisms of Digital Radicalisation in Online Gaming Ecosystems

Digital radicalization in the online gaming ecosystem usually takes place gradually through exposure, interaction, reinforcement, internalization, and a move to a more closed communication space. The initial stage can be exposure to symbols, memes, videos, comments, links, or conversations that contain hate and violence. This exposure is not always immediately accepted as an ideological teaching. Most of the time, it appears in the form of humor, irony, provocation, or community language.

The next stage is interaction. Young people not only see content, but also respond, discuss, imitate, or participate in dissemination. In a digital community, social responses have a huge influence. Comments that get support, posts that get praise, or symbols that are considered bold can reinforce certain behaviors. At this point, Social Learning Theory becomes relevant because young people can learn through observation, imitation, and reinforcement from their digital environment.

The third stage is normalization. Violence is no longer seen as something deviant, but as part of a group identity. Hate narratives began to be considered as truth. Enemies are constructed repeatedly. Certain states, officials, other religious groups, certain ethnicities, or political groups can be placed as targets of hostility. In this situation, the process of radicalization moves from mere exposure to the formation of a way of view.

The fourth stage is reinforcement through the echo chamber. In echo chambers, young people are more likely to interact with people who have similar views. Different views are dismissed, considered weak, or positioned as part of the enemy. The platform's algorithm can reinforce this situation when the recommendation system continues to display content that aligns with the user's interest history. As a result, extreme narratives can come across as ordinary, dominant, or true.

The fifth stage is the move to a private channel. Early communities can form in online games, social media, or public forums. However, more ideological, technical, and closed conversations can move to private spaces such as conversation groups, closed channels, or encrypted apps. This move makes early detection difficult as communications become more limited, selective, and difficult to legally monitor.

Within the framework of Situational Action Theory, such changes can be described as the relationship between the individual and the environment. Young people in certain digital environments can experience a change in moral perception if that environment continues to provide justification, peer pressure, symbols of violence, and social support. Extreme actions do not arise simply because of individual character. It can arise when an individual is in a situation that makes violence seem right, legitimate, or necessary.

The mechanism also shows the importance of duration and intensity. Brief exposure to extreme content does not necessarily result in ideological change. The risk increases when exposure is repeated, socially reinforced, and accompanied by isolation from alternative views. In other words, radicalization depends not only on the content of the message, but also on the frequency, community context, social response, and psychological state of the message recipient.

The move from open spaces to private channels is a very important stage for prevention. In the early stages, signs of risk may still be visible from comments, symbols, or public interactions. When conversations have moved to a closed space, monitoring becomes more difficult and must be subject to stricter legal limits. Therefore, the most effective interventions should be made before the risky conversation moves completely into a private channel.

4.3 Youth Lone Wolf as a Product of Digital Relations

Lone wolves are often understood as perpetrators who move alone, are not in an organizational network, and do not receive direct orders from terror groups. This definition is useful for distinguishing lone wolves from organization-based terror perpetrators. However, this understanding can be misleading if it is interpreted that the perpetrator is completely disconnected from social influence. In many cases, individuals can act alone, but still derive inspiration, justification, symbols, and legitimacy from a particular social environment.

The concept of social embeddedness helps explain this. Lone wolves are not always ideologically isolated. It can connect with digital communities, extreme discourses, reference figures, previous manifestations of violence, or specific movement symbols. That connectedness is not always in the form of official membership. It can take the form of content consumption, loose interactions, admiration for previous perpetrators, or involvement in communities that normalizes narratives of violence.

In the context of young people and online games, digital relationships can form new social spaces. A young person can never meet an extreme actor in person and not be a member of the organization. However, he can absorb violent narratives from digital communities, mimic extreme symbols, admire the perpetrators of previous attacks, or feel like he is part of an imaginary group that has a common enemy. At this point, the lone wolf does not grow from empty space. It grows from digital relationships that give meaning to solitary actions.

Digital relationships can also make the perpetrator feel not alone even though they are physically moving alone. Digital communities can provide moral support, provide common enemies, and create collective imaginations. In fact, an attack carried out by another perpetrator can be a signal that similar actions are possible. In lone actor studies, such dynamics can create signaling spirals, which are when previous violence sends the message that violence is a possible, effective, and replicable action.

This analysis is important for cyber policing. If the lone wolf is only understood as an isolated individual, prevention will focus too much on personal characteristics. In fact, the formation of lone wolf also needs to be seen through content consumption patterns, digital relationships, community narratives, extreme symbols, and changes in online behavior. Thus, early detection is not enough to look for organizational structure. Detection also needs to read changes in interaction patterns, digital identity, extreme content consumption intensity, and the move of communication to private spaces.

Relational reading of the lone wolf also helps to avoid excessive stereotypes. Not all young people who are alone can be considered as potential perpetrators of violence. Social isolation only becomes relevant when intersecting with the consumption of extreme narratives, violent justifications, risky digital relationships, and consistent behavior change. Therefore, a risk-based approach should be sharper than a label-based approach.

In preventive practice, relational signs need to be read carefully. An indicator worth paying attention to is not just who is being followed, but how the patterns of interaction are changing. For example, increased consumption of violent content, reinforcement of hostile language, disconnection from moderate communities, search for tactical information, or move to more closed groups. Such an indicator combination is stronger than a single mark.

4.4 Algorithms, Artificial Intelligence, and Self-Radicalisation

Digital radicalization today is not only influenced by content. It is also affected by the platform's infrastructure. The algorithm determines what content appears, how often the content is displayed, who receives the content, and how the content is prioritized. In the digital ecosystem, platforms are not just where content is stored. The platform also becomes a distribution system that regulates the user's attention.

The recommendation system has an important role. Research on recommendation systems shows that concerns against the amplification of extreme content cannot be ignored. On certain platforms, especially YouTube in the context of far-right material being tested, the recommendation system can reinforce exposure to extreme and fringe content. However, the pattern is not the same on all platforms. These findings prevent overgeneralization, but still show that platform design has consequences for exposure patterns.[27]

In the context of young people, algorithms can narrow the information space. When users frequently interact with certain content, the platform may display similar content repeatedly. If the content is hateful or extremist, users can fall into an increasingly narrow pattern of exposure. As a result, extreme views can appear ordinary, dominant, or true. This condition strengthens the echo chamber and filter bubble.

Artificial intelligence adds new complexity. AI can be used to create propaganda content that is fast, cheap, personalized, and difficult to detect. The risk of AI doesn't just lie in the ability to create content. Greater risks arise when AI is used to read user behavior, map emotions, tailor messages, and repeat narratives with different forms. Propaganda can be present as short videos, memes, automated comments, personalized messages, voice simulations, synthetic images, or narratives created according to the issue that appeals to the target group.

In the context of self-radicalization, algorithms and AI can accelerate the process from curiosity to ideological engagement. Young people who are initially looking for general information can be directed to increasingly narrow content. Users who show interest in themes of conflict, injustice, conspiracy, or violence can receive more intense content. When this process occurs in a validating digital community, self-radicalization can move faster. However, algorithms and AI are not the only actors that determine radicalization. Both work in a social context. Prevention needs to encourage algorithmic transparency, digital literacy, platform risk audits, technological cooperation, and the ability of officials to read changes in digital patterns.

Algorithmic challenges also have to do with the economic logic of the platform. Digital platforms generally place high value on user engagement, such as watch duration, number of comments, emotional responses, and sharing opportunities. Provocative content often gets more attention because it triggers anger, fear, or curiosity. In this context, extreme content can benefit not because platforms intentionally support extremism, but because engagement systems can make room for emotional content to continue circulating.

Prevention therefore requires talking about platform governance. It is not enough for the state to request the removal of content once the content is widespread. Countries, platforms, and civil society need to discuss recommendation design, reporting access, child protection, moderation transparency, and risk audit mechanisms. This approach must still be proportionate so as not to limit freedom of expression excessively.

4.5 Challenges of Cyber Policing in Early Detection

Cyber policing faces a major challenge in detecting the radicalization of lone wolf young people. The first challenge is anonymity. Young people can use pseudonyms, avatars, dual accounts, temporary chat rooms, and changing digital identities. Anonymity has a positive function in freedom of expression and privacy protection. However, anonymity can also be used to spread hatred, conduct recruitment, or build extreme communities without being easily recognized.

The second challenge is the volume of data. The digital space generates large amounts of data. Conversations, comments, uploads, videos, images, emojis, memes, and links move quickly across platforms. Not all data is relevant to the threat. A lot of content is jokes, emotional expressions, social criticism, or casual debates. Therefore, it is not enough for the authorities to rely only on keyword searches. It requires an understanding of context, interaction patterns, intensity, networking, and behavior change.

A study on Densus 88 shows that social media has been used for intelligence gathering. Techniques such as Social Network Analysis, classification, clustering, and sentiment analysis can help map relationships, segment behavior patterns, and read indications of support for extreme ideologies. However, the use of technology must be balanced with human judgment, ethical frameworks, and protection of privacy rights.[28]

The third challenge is the move of platforms. The initial interaction can occur in an open space, but more sensitive conversations can move to a closed channel. This shift makes early detection more difficult. On the one hand, the state needs to prevent threats. On the other hand, the state must still adhere to the principles of law, privacy, proportionality, and accountability. Without clear boundaries, cyber policing can be considered excessive surveillance.

The fourth challenge is the ambiguity of the indicators. Not all users who see extreme content will be radical. Not all harsh comments indicate violent intent. Not all provocative symbols imply support for terrorism. Misreading indicators can give birth to false positives, which are when harmless individuals are considered a threat. Conversely, reading indicators too loosely can result in false negatives, i.e. when a real threat is not detected.

The fifth challenge is child protection. If the subject being monitored is a young person, the security approach should be more careful. Young people can be in the phase of identity exploration, role seeking, and peer group influence. Overly repressive responses can exacerbate alienation. Therefore, prevention needs to prioritize education, mentoring, counseling, and strengthening the social environment before entering law enforcement.

Another challenge is the limitation of human capacity. Digital data can be processed by the system, but the final assessment still requires analysts who understand the social context, culture, local language, symbols, and community dynamics. Without human judgment, the system can misread satirism, jokes, news quotes, or academic discussions as threats. On the other hand, without the help of technology, humans will have difficulty reading huge volumes of data.

Therefore, cyber policing needs to combine a technological approach and a human approach. Technology can help filter data, find patterns, and provide early warnings. Human analysts provide context, assess the level of risk, and determine proportionate measures. This combination is important so that prevention doesn't get stuck on context-blind automation or manual monitoring that is too slow.

4.6 Preventive-Collaborative Cyber Policing Model

Based on the previous discussion, the model of preventing the radicalization of young people must move from a content approach to an ecosystem approach. The content approach focuses only on the removal of extreme material. This approach remains important, but not enough. Content can be removed, but young people's communities, narratives, symbols, algorithms, and vulnerabilities can still survive. Therefore, prevention models need to look at the entire digital ecosystem.

The prevention model offered in this study can be referred to as the Preventive-Collaborative Cyber Policing Model. This model places the National Police as an important actor, but not the only actor. Preventing the radicalization of young people requires joint work between the National Police, Densus 88, Indonesia's National Counter Terrorism Agency, The Indonesian Child Protection Commission, Ministry of Communication and Digital Affairs, schools, families, digital platforms, academics, community organizations, and the gamer community.

The first component is digital risk-based early detection. Early detection should not be based solely on keywords. Detection needs to read broader patterns, such as changes in interaction intensity, extreme content consumption, involvement in closed communities, glorification of violence, search for tactical information, and expressions of violent justification. Schumann, Kenyon, and Binder show that types of internet use have different levels of risk. Learning about ideology alone is not the same as seeking tactical and ideological information at the same time. The search for tactical information combined with ideological consumption has a higher relevance to the possibility of planning or executing an attack.[29]

The second component is community-based digital literacy. Young people need to be equipped with the ability to recognize propaganda, algorithm manipulation, hoaxes, conspiracy theories, hate speech, and extreme recruitment techniques. Digital literacy is not enough in the form of general campaigns. Literacy must enter the spaces that young people use, including schools, campuses, gaming communities, streaming platforms, and digital forums. The language used must be in accordance with the digital culture of young people so that it does not feel patronizing.

The third component is counter-narrative and alternative narratives. The counter-narrative does not only refute extreme propaganda. It also needs to offer a positive identity, a sense of belonging, and a healthy space for participation. Young people who are looking for meaning are not enough to be forbidden. They need to have space to be recognized, discuss, create, and be involved in productive communities. The gamer community can be an important partner because a healthy community can reject hate symbols, report harmful content, and build an inclusive digital culture.

The fourth component is digital platform cooperation. The platform has a huge role in the moderation, recommendations, and design of the ecosystem. Cooperation with platforms needs to include content reporting, responses to risky accounts, algorithmic audits, child protection, and transparency mechanisms. Regulations that focus solely on content removal are not enough to address the problem of amplification. Content distribution and recommendations also need to be considered.[30]

The fifth component is assistance to vulnerable young people. Not all young people who are exposed to extreme content should be treated as perpetrators. Many of them are more accurately understood as vulnerable individuals who need assistance. This approach can involve counselors, teachers, families, psychologists, social workers, community leaders, and child protection agencies. Mentoring is important so that interventions not only stop exposure, but also improve social conditions that make young people vulnerable to extreme narratives.

The sixth component is legal accountability and privacy protection. Cyber policing must run within the corridor of the law. Early detection, monitoring, and data analysis must have a legal basis, limits of authority, supervisory mechanisms, and protection of personal data. Without accountability, cyber policing can lose public legitimacy. In the issue of young people, the principle of child protection must be the main concern. Prevention must distinguish between curiosity, early exposure, ideological support, and violent intent.

This model can be formulated in a flow: the vulnerability of young people to exposure to digital communities, the reinforcement of extreme narratives, the move to private spaces, the potential for self-radicalization, and preventive cyber policing interventions. Interventions are not placed at the end of the process alone. Interventions need to be present from the early stages through literacy, risk mapping, community engagement, and platform cooperation. The earlier the intervention is carried out, the greater the chance of preventing radicalization from moving towards violence.

The preventive-collaborative model also requires an evaluation mechanism. Each literacy, early detection, and platform cooperation program needs to be evaluated to see if it lowers risk, increases reporting, strengthens youth resilience, or creates fear. Evaluation needs to involve security indicators and rights protection indicators. Thus, the success of prevention is measured not only by the amount of content removed, but also by the increasing social resilience of the digital community.

The application of this model demands a change in perspective. Cyber policing should not only be understood as a response to threats that have already emerged. It must be a risk management strategy that works from the upstream. The upstream includes literacy, family, school, community, platform design, and dialogue spaces. When upstream is strengthened, the authorities have a greater chance of preventing radicalization before it develops into violent intent.

5. CONCLUSION

This research shows that online gaming and digital communities have become part of the social space of young people. The space serves not only as a means of entertainment, but also as a place for the formation of identity, social relations, group solidarity, and the search for recognition. Under certain conditions, the digital space can become an arena of vulnerability when young people experience social isolation, weak digital literacy, identity crises, and repeated exposure to narratives of hatred and violence.

The main findings of the study confirm that online gaming cannot be positioned as a direct cause of radicalism. Risks arise when the online gaming ecosystem and digital community are exploited by extreme actors through anonymity, closed communities, violent symbols, recommendation algorithms, and young people's need for a sense of belonging. Thus, the main problem lies not in games as a technology, but in the digital ecosystem that allows extreme narratives to be produced, disseminated, amplified, and normalized.

The radicalization of young lone wolves cannot be explained through a single factor. The process is formed through relationships between individuals, digital communities, extreme narratives, platform algorithms, social experiences, and private communication spaces. Young people can move from initial exposure to ideological engagement through a gradual process, from content consumption, community interaction, group validation, to justification of violence. Perpetrators can act alone, but the radicalization process can still be influenced by digital communities, reference figures, or violent narratives circulating in cyberspace.[31]

The development of algorithms and artificial intelligence magnifies the challenge of prevention. Algorithms can amplify exposure through recommendations and content personalization. Artificial intelligence can be used to produce propaganda that is fast, personalized, and difficult to detect. Technology does not automatically create radicalism, but can accelerate the exposure process if it is not balanced with digital literacy, platform governance, and adequate early detection.[32]

Theoretically, this study expands the study of digital radicalization in Police Science. The focus of research shifted from general social media to online gaming ecosystems and digital communities as a social space for young people. This research also reinforces the view that online and offline boundaries cannot be rigidly separated. Digital radicalization needs to be read as a hybrid process that brings together identity, social learning, community relations, algorithms, and social conditions in the real world.

Practically, the National Police and Densus 88 need to strengthen the capacity of digital risk-based early detection. Detection shouldn't rely solely on keywords or the presence of extreme content. The analysis needs to pay attention to interaction patterns, communication intensity, involvement in closed communities, glorification of violence, search for tactical information, and changes in ideological orientation. The use of Social Network Analysis, clustering, sentiment analysis, and data mining can help with this process, but it must be accompanied by human validation and clear legal boundaries.[33]

Prevention also needs to involve actors outside the security forces. Indonesia's National Counter Terrorism Agency, The Indonesian Child Protection Commission, Ministry of Communication and Digital Affairs, schools, campuses, families, psychologists, gamer communities, digital platforms, academics, and civil society need to be placed as part of the prevention ecosystem. The National Police play a role in law detection and enforcement. Indonesia's National Counter Terrorism Agency strengthens the prevention of violent extremism. The Indonesian Child Protection Commission maintains a child protection perspective. The Ministry of Communication and Digital Affairs encourages platform governance. Schools, families, and gamer communities reinforce literacy and healthy social supervision.

This research has limitations because it uses a qualitative approach based on literature studies and policy analysis. This study has not presented direct field data from online gaming communities, law enforcement officials, young people, families, schools, or digital platforms. The study also did not observe closed digital groups for ethical, security, privacy, and risk of expanding exposure to extreme content. Follow-up studies need to use interviews, ethical limited observations, or policy studies with officials, teachers, psychologists, gamer communities, digital literacy activists, and cybersecurity analysts.

Thus, the prevention of the radicalization of young people's lone wolf in the digital space cannot be built only through a security approach. Prevention must combine cyber policing, child protection, digital literacy, platform governance, and social collaboration to be able to close the space for extremism exploitation without ignoring the rights of citizens.

The policy direction born from this research emphasizes balance. The state must be able to be present to prevent the exploitation of extremism in the digital space. At the same time, the state needs to maintain public trust by ensuring that monitoring does not violate the right to privacy and does not stigmatize young people or the gamer community. This balance is a prerequisite for strong and socially legitimate cyber policing.

The main contribution of this article is to offer a way to read the radicalization of young lone wolves as an ecosystem process. That process is not born from one content, one platform, or one psychological factor. It is formed from the meeting of identity, relationships, technology, algorithms, communities, and social surveillance. Therefore, prevention must be done as a sustained cross-actor agenda, not as a response immediately after a threat has emerged.

ENDNOTE

Heather Wolbers, Christopher Dowling, Timothy Cubitt, and Chante Kuhn, "Understanding and Preventing Internet-Facilitated Radicalisation," Trends & Issues in Crime and Criminal Justice, no. 673 (2023): 1.

Rosamund Mutton, James Lewis, and Sarah Marsden, Online Radicalisation: A Rapid Review of the Literature (CREST, 2023), 4.

Michael Wolfowicz, Badi Hasisi, and David Weisburd, "What Are the Effects of Different Elements of Media on Radicalization Outcomes? A Systematic Review," Campbell Systematic Reviews 18, no. 2 (2022): e1244.

Rabya Mughal, Valerie DeMarinis, Maria Nordendahl, Hassan Lone, Veronica Phillips, and Eolene Boyd-MacMillan, "Public Mental Health Approaches to Online Radicalisation: An Empty Systematic Review," International Journal of Environmental Research and Public Health 20, no. 16 (2023): Article 6586, 1-3.

Stefan Malthaner, Francis O'Connor, and Lasse Lindekilde, "Scattered Attacks: The Collective Dynamics of Lone-Actor Terrorism," Perspectives on Politics 22, no. 2 (2024): 463-464.

Bart Schuurman and Sarah L. Carthy, "Who Commits Terrorism Alone? Comparing the Biographical Backgrounds and Radicalization Dynamics of Lone-Actor and Group-Based Terrorists," Crime & Delinquency 71, no. 6-7 (2025): 2092-2095.

Hana Abshari, "Threat Analysis of Social Media Use on the Tendency of College Student Radicalism," Security Intelligence Terrorism Journal 2, no. 1 (2025): 84-94.

Joe Whittaker, Seán Looney, Alastair Reed, and Fabio Votta, "Recommender Systems and the Amplification of Extremist Content," Internet Policy Review 10, no. 2 (2021); Nasir Ahmad Ganaie, "The Role of Artificial Intelligence in Radicalisation, Recruitment and Terrorist Propaganda," Frontiers in Political Science 7 (2026): Article 1718396.

Aliviqo Pandu Virgantara, Surya Nita, and Didik Novi Rahmanto, "The Role of Social Media in Supporting Information and Intelligence Gathering by Densus 88," Security Intelligence Terrorism Journal 1, no. 2 (2024): 92-100.

Mughal et al., "Public Mental Health Approaches to Online Radicalisation," 2-3.

Malthaner, O'Connor, and Lindekilde, "Scattered Attacks," 463-465.

Virgantara, Nita, and Rahmanto, "The Role of Social Media in Supporting Information and Intelligence Gathering by Densus 88," 92-100.

Mughal et al., "Public Mental Health Approaches to Online Radicalisation," 1.

Henri Tajfel and John C. Turner, "The Social Identity Theory of Intergroup Behavior," in Psychology of Intergroup Relations, ed. Stephen Worchel and William G. Austin (Chicago: Nelson-Hall, 1986), 7-24.

Arie W. Kruglanski, Jocelyn J. Bélanger, and Rohan Gunaratna, The Three Pillars of Radicalization: Needs, Narratives, and Networks (Oxford: Oxford University Press, 2019).

Albert Bandura, Social Learning Theory (Englewood Cliffs: Prentice Hall, 1977); Albert Bandura, Social Foundations of Thought and Action: A Social Cognitive Theory (Englewood Cliffs: Prentice Hall, 1986).

Lawrence E. Cohen and Marcus Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," American Sociological Review 44, no. 4 (1979): 588-608.

Per-Olof H. Wikström and Noémie Bouhana, "Analyzing Radicalization and Terrorism: A Situational Action Theory," in The Handbook of the Criminology of Terrorism, ed. Gary LaFree and Joshua D. Freilich (Hoboken: Wiley, 2017), 175-186; Joe Whittaker, "Rethinking Online Radicalization," Perspectives on Terrorism 16, no. 4 (2022): 71-84.

Malthaner, O'Connor, and Lindekilde, "Scattered Attacks," 463-480.

Schuurman and Carthy, "Who Commits Terrorism Alone?" 2092-2117.

Whittaker, Looney, Reed, and Votta, "Recommender Systems and the Amplification of Extremist Content."

Ganaie, "The Role of Artificial Intelligence in Radicalisation, Recruitment and Terrorist Propaganda."

Virgantara, Nita, and Rahmanto, "The Role of Social Media in Supporting Information and Intelligence Gathering by Densus 88," 92-100.

John W. Creswell and Cheryl N. Poth, Qualitative Inquiry and Research Design: Choosing Among Five Approaches, 4th ed. (Thousand Oaks: SAGE Publications, 2018).

Glenn A. Bowen, "Document Analysis as a Qualitative Research Method," Qualitative Research Journal 9, no. 2 (2009): 27-40.

Virginia Braun and Victoria Clarke, "Using Thematic Analysis in Psychology," Qualitative Research in Psychology 3, no. 2 (2006): 77-101; Klaus Krippendorff, Content Analysis: An Introduction to Its Methodology, 4th ed. (Thousand Oaks: SAGE Publications, 2019).

Whittaker, Looney, Reed, and Votta, "Recommender Systems and the Amplification of Extremist Content."
Virgantara, Nita, and Rahmanto, "The Role of Social Media in Supporting Information and Intelligence Gathering by Densus 88," 92-100.
Sandy Schumann, Jonathan Kenyon, and Jens Binder, "Identifying Distinct Types of Internet Use That Predict the Likelihood of Planning or Committing a Terrorist Attack: Findings from an Analysis of Individuals Convicted on Terrorism-Related Charges in England and Wales," Computers in Human Behavior 168 (2025): Article 108646.
Whittaker, Looney, Reed, and Votta, "Recommender Systems and the Amplification of Extremist Content."
Malthaner, O'Connor, and Lindekilde, "Scattered Attacks," 463-480.
Whittaker, Looney, Reed, and Votta, "Recommender Systems and the Amplification of Extremist Content"; Ganaie, "The Role of Artificial Intelligence in Radicalisation, Recruitment and Terrorist Propaganda."
Virgantara, Nita, and Rahmanto, "The Role of Social Media in Supporting Information and Intelligence Gathering by Densus 88," 92-100.

REFERENCES

1. Abshari, H. (2025). Threat analysis of social media use on the tendency of college student radicalism. Security Intelligence Terrorism Journal, 2(1), 84-94. https://doi.org/10.70710/sitj.v2i1.35
2. Bandura, A. (1977). Social learning theory. Prentice Hall.
3. Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice Hall.
4. Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27-40.
5. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.
6. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.
7. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications.
8. Ganaie, N. A. (2026). The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: Deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems. Frontiers in Political Science, 7, Article 1718396. https://doi.org/10.3389/fpos.2025.1718396
9. Krippendorff, K. (2019). Content analysis: An introduction to its methodology (4th ed.). SAGE Publications.
10. Kruglanski, A. W., Bélanger, J. J., & Gunaratna, R. (2019). The three pillars of radicalization: Needs, narratives, and networks. Oxford University Press.
11. Malthaner, S., O'Connor, F., & Lindekilde, L. (2024). Scattered attacks: The collective dynamics of lone-actor terrorism. Perspectives on Politics, 22(2), 463-480. https://doi.org/10.1017/S1537592723002852
12. Mughal, R., DeMarinis, V., Nordendahl, M., Lone, H., Phillips, V., & Boyd-MacMillan, E. (2023). Public mental health approaches to online radicalisation: An empty systematic review. International Journal of Environmental Research and Public Health, 20(16), Article 6586. https://doi.org/10.3390/ijerph20166586
13. Mutton, R., Lewis, J., & Marsden, S. (2023). Online radicalisation: A rapid review of the literature. Centre for Research and Evidence on Security Threats.
14. Schumann, S., Kenyon, J., & Binder, J. (2025). Identifying distinct types of internet use that predict the likelihood of planning or committing a terrorist attack: Findings from an analysis of individuals convicted on terrorism-related charges in England and Wales. Computers in Human Behavior, 168, Article 108646. https://doi.org/10.1016/j.chb.2025.108646
15. Schuurman, B., & Carthy, S. L. (2025). Who commits terrorism alone? Comparing the biographical backgrounds and radicalization dynamics of lone-actor and group-based terrorists. Crime & Delinquency, 71(6-7), 2092-2117. https://doi.org/10.1177/00111287231180126
16. Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W. G. Austin (Eds.), Psychology of intergroup relations (pp. 7-24). Nelson-Hall.
17. Virgantara, A. P., Nita, S., & Rahmanto, D. N. (2024). The role of social media in supporting information and intelligence gathering by Densus 88. Security Intelligence Terrorism Journal, 1(2), 92-100. https://doi.org/10.70710/sitj.v1i2.10
18. Whittaker, J. (2022). Rethinking online radicalization. Perspectives on Terrorism, 16(4), 71-84.
19. Whittaker, J., Looney, S., Reed, A., & Votta, F. (2021). Recommender systems and the amplification of extremist content. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1565
20. Wikström, P.-O. H., & Bouhana, N. (2017). Analyzing radicalization and terrorism: A situational action theory. In G. LaFree & J. D. Freilich (Eds.), The handbook of the criminology of terrorism (pp. 175-186). Wiley.

21. Wolbers, H., Dowling, C., Cubitt, T., & Kuhn, C. (2023). Understanding and preventing internet-facilitated radicalisation. Trends & Issues in Crime and Criminal Justice, 673, 1-17. https://doi.org/10.52922/ti77024
22. Wolfowicz, M., Hasisi, B., & Weisburd, D. (2022). What are the effects of different elements of media on radicalization outcomes? A systematic review. Campbell Systematic Reviews, 18(2), Article e1244. https://doi.org/10.1002/cl2.1244