SOCIAL MEDIA AS A CATALYST FOR RADICALIZATION: ETIOLOGY AND MODERN TRENDS

Elena Dimovska[1], **PhD Candidate**
Faculty of Security – Skopje, University "St. Kliment Ohridski" – Bitola,
North Macedonia

ABSTRACT

Purpose: The purpose of this paper is to examine how social media platforms contribute to radicalization by exploring the mechanisms, factors, and trends that facilitate the spread of extremist content and influence contemporary crime. The paper will also analyze previous radicalization cases in North Macedonia, specifically assessing whether and how many individuals were radicalized online, and investigate if those convicted for foreign terrorist fighter (FTF) -related crimes – most of whom have already served their sentences – continue to share their ideology online.

Design/Methods/Approach: The study utilizes recent case studies and empirical research to analyze the role of platforms like Facebook, Telegram, and YouTube in disseminating extremist content. It investigates extremist tactics and psychological vulnerabilities, focusing on digital echo chambers and targeted recruitment. Additionally, the research will include a review of official documents, existing research, and online content to identify patterns of radicalization in North Macedonia, with particular attention to FTF cases and ongoing online activity by former convicts.

Findings: Social media significantly accelerates radicalization through algorithm-driven content amplification and tailored extremist strategies, especially among youth. The study identifies challenges for law enforcement in differentiating between radical expression and actual threats and underscores the impact of digital echo chambers and online propaganda in normalizing extremist views. In North Macedonia, online media are a potent mechanism for radicalization, with unregulated environments enabling the spread of extremist narratives. Preliminary findings suggest that while religious radicalization is perceived as a higher risk, online channels play a significant role in both religious and political radicalization. The analysis of FTF cases will provide insight into the prevalence of online radicalization and the extent to which former FTF convicts remain active in disseminating extremist ideologies.

Originality/Value: This paper provides a comprehensive and contemporary overview of online radicalization's etiology and phenomenology, integrating empirical evidence with case studies. By including a focused analysis of North Macedonian radicalization cases – particularly those involving FTFs and their post-release online activities – it offers valuable, context-specific insights into emerging trends and practical implications for prevention and intervention in the digital age.

Keywords: online radicalization, social media, foreign terrorist fighters.

About the author

Elena Dimovska is a teaching assistant at the Faculty of Security – Skopje, University "St. Kliment Ohrdski" – Bitola. She is a seasoned security analyst and educator with expertise in counterterrorism,

1 elena.dimovska@uklo.edu.mk

radicalization, and international security. She is currently pursuing a PhD in Criminology at the University St. Kliment Ohridski, Faculty of Security in Skopje. Her professional background includes roles such as senior security analyst and research/project coordinator. She has contributed extensively to policy development and evaluation, leading multiple research projects and co-authoring over ten publications in her field. Elena is proficient in designing research methodologies, conducting evaluations, and facilitating workshops, showcasing her strong analytical and organizational skills.

INTRODUCTION

The development of communication technologies has had an impact on shaping communication and social interaction around the world. Social media particularly has undergone a significant evolution over the past two decades, from an online networking tool to a multifaceted tool used to connect with others, share information, and even conduct business and political activities. While offering numerous benefits, social media also presents challenges related to privacy and the spread of misinformation.

A particular challenge for security services around the world is the misuse of social networks by radical groups, who use the virtual space to reach a large number of people around the world, thus spreading their radical ideology. Radicalization – the process by which individuals increasingly adopt extremist beliefs that may lead to violence – is increasingly influenced by online interactions, making social media a pivotal factor in modern radicalization trends.

Radicalization is often a hybrid process involving both online and offline influences, although fully online pathways have become more common in recent years, especially during periods of increased online engagement like the COVID-19 pandemic.

This study focuses on social media's role in radicalization with particular emphasis on North Macedonia – a region marked by ethnic diversity and strategic significance in the Balkans. The country has seen notable cases of radicalization, including foreign terrorist fighter mobilization during the Syrian conflict. By examining online radicalization mechanisms, cases of convicted foreign fighters, and their post-release online activities, this paper aims to provide context-specific insights into the evolving landscape of digital extremism.

Through a combination of theoretical frameworks and empirical case studies, the research underscores the intertwined offline and online nature of radicalization and discusses challenges related to prevention, law enforcement, and policy-making. It highlights the necessity of mutual, international approaches to counter radical content and foster resilience against digital extremism.

SOCIAL MEDIA AS A CATALYST FOR RADICALIZATION

Violent online radicalization usually begins through selection, which can be targeted and organized, or it can be spontaneous, i.e., self-selection when someone is selected through his/her behavior (through monitoring contacts, activities on social networks, discussions in various chat rooms, etc.). For the purpose of targeted selection, some of the well-organized malicious groups and individuals have developed profiling methodologies. By scanning online activities and collecting and processing data (analyzing the behavior of the target), these groups or individuals begin a selection process. Self-radicalization can also occur when a random victim reads online literature, forums, and blogs from dubious sources or broadcasts videos, audio recordings, or songs with content that aims to violently radicalize.

Knowing about these opportunities for expanded self-radicalization, terrorist groups are increasingly present in the virtual space. For example, the terrorist organization Al-Qaeda had long published various information on its website in order to spread its ideology and recruit young fighters before the website was removed from the Internet. Today, membership is present in the online space through Al-Sahab – a media wing of Al-Qaeda responsible for producing and disseminating the group's propaganda materials (NEFA Foundation, n.d.). Al-Sahab produces and distributes videos, statements, magazines, and footage featuring Al-Qaeda leaders and operations. In addition to video messages from the leadership, martyrdom videos (suicide bombers and fighters) are also published, as well as training and operational videos and documentaries promoting al-Qaeda's ideology. While its primary output is in Arabic, many of its productions feature English subtitles to reach a global audience. Al-Sahab operates mainly on the social platform Telegram but also on private jihadist forums, the dark webs, and other private platforms.

In one of the recent videos published by the senior leader of al-Qaeda in the Arabian Peninsula (AQAP), the organization issued a direct call to lone-wolf attackers worldwide (Al Jazeera, 2025). The video, approximately 30 minutes long, was released amid Israel's ongoing war on Gaza and framed the conflict as part of a broader "crusade" against Muslims. The leader explicitly states that there are no limits to what targets are acceptable in response to the war in Gaza. It is interesting to note that the rhetoric was emotional, vengeful, and designed to resonate with frustrated individuals sympathetic to the Palestinian cause. This means that Al-Qaeda is strategically crafting its message to emotionally manipulate people, especially those already angered or disillusioned by the war in Gaza. At the same time, the group is exploiting real political and humanitarian crises (like Gaza) to legitimize extremist violence, hoping to turn sympathy into radicalization. In other words, it's weaponizing compassion and outrage for recruitment.

The messaging is tailored for individuals who feel powerless, giving them a sense of personal mission or revenge, even outside formal jihadist structures. This is a classic lone-wolf recruitment method – turning personal frustration into violent action. Rather than deep religious or ideological reasoning, the emphasis is on emotion: anger, vengeance, betrayal – which can mobilize people faster than traditional indoctrination. Thus, this suggests the message is more populist than theological.

One of the deadliest terrorist organization – ISIS – is also very present in the online space. According to Bodine-Baron et al. (2016), "Its social media prowess has quite possibly played a part in ISIS's enormous success in recruitment". Their online propaganda is one of the most aggressive and played a central role in recruitment, radicalization, and inciting lone-wolf attacks, especially during the group's peak from 2014 to 2017. Their propaganda included execution videos, battlefield success, and life in the so-called "Caliphate". In order to reach more people across the world, they are sharing content in many languages, such as Arabic, English, French, and Russian. The U.S. House Committee on Oversight and Government Reform (2015) discusses that ISIS's use of social media is resonating with vulnerable populations, particularly Muslim converts and susceptible alienated youth. As noted by Stern and Berger (2015), the Islamic State has been highly effective at using social media platforms like Twitter, Facebook, and WhatsApp to spread terrorist messaging, recruit, mobilize, and finance their operations globally. Namely, over 43,000 active pro-ISIS Twitter accounts consistently spread ISIS's messages of hatred and terror. The fact that more than 30,000 people globally have joined ISIS highlights the significant influence of social media in fueling this threat (U.S. House of Representatives, Subcommittee on National Security, 2015).

Through these channels, the group released step-by-step terrorism manuals (so-called DIY (do it yourself) guides) that instructed followers on how to make explosives, carry out stabbings, or use everyday vehicles as weapons. This online content was deliberately designed to encourage individuals,

particularly those living in Western countries, to conduct attacks independently, without needing to travel or establish direct contact with ISIS operatives. In one of the online manuals (Safety Guide for Lone Wolves, Mujahideen, and Small Cells), in a visual way, by sharing stories and advice from their "soldiers", as well as sharing the basic principles of the organization, they tried to encourage and incite disaffected people from all over the world to join them (Ryan, 2015).

According to a report by Vidino, Marone, and Entenmann (2017), one of the most notorious Islamic State virtual recruiters was Rachid Kassim, a former rapper from Roanne, France. After traveling to Syria in 2015 with his family to join ISIS, Kassim began operating an influential Telegram channel called Sabre de Lumière. Through this platform, he actively directed and inspired followers in Europe to carry out attacks, often publishing weekly "target lists" that called for violence against religious leaders, media figures, entertainers, and law enforcement officers. He also appeared in official French-language propaganda videos, further solidifying his role as a key instigator of remote jihadist violence.

Considering that the majority of users of social networks are generations Z and millennials, young people are a particularly vulnerable group to online radicalization. As some studies have shown, social media use is widespread among teenagers, with up to 95% of youth ages 13–17 reporting that they use at least one platform (Office of the Surgeon General, 2023).

Having this in mind, it's important to note that according to the National Consortium for the Study of Terrorism and Responses to Terrorism (START, 2018), the internet played a primary or contributing role in the radicalization of 86% of the foreign fighters.

There is no exact time frame for how long it takes for a person to become radicalized (i.e., the time from first exposure to extremist beliefs to participation in extremist acts). However, several studies have been conducted, mainly in the United States, and according to Conway, Scrivens, and Macnair (2018), in 2016, when over 90% of U.S. foreign fighters were active on social media, the duration of radicalization was 13 months on average. On the other hand, Simonetti (2021) explains that Jensen's research found radicalization times in the U.S. have decreased dramatically (from 18 to 7 months), largely due to increased online activity. Unlike in the 1980s or '90s, when far-right extremists needed real-life connections for recruitment, the process is now much faster.

In addition to social networks, young people are often exposed to radical propaganda in video game chat rooms. On the other side of the chat group are also often young people who are already radicalized. These young people are used by the higher structures of terrorist organizations as propagandists and indoctrinators who can more easily influence their young peers because they share a common language and generational interests.

Particularly dangerous are the so-called religious preachers who are active on social networks as influencers. These self-proclaimed preachers particularly target young people, to whom they present certain theological views. They often have excellent oratory skills but are also religiously educated, so they act convincingly and easily gain trust among young people. They use open groups on social networks only for initial contact with potential followers, while avoiding sharing radical views and calls for violence in open groups, knowing that this is illegal and probably assuming that social networks are monitored by security services. The real radicalization comes later, in smaller groups in chat rooms on Telegram, Signal, or another platform, and sometimes behind closed doors in physical premises, if the people are from the same country.

Given the impact and consequences of online radical propaganda, states are taking measures, first by criminalizing the act but also by taking preventive action through identifying and closing online channels that spread radical propaganda. For instance, in the Netherlands, a man was sentenced to two years in prison by the Court of Appeal in The Hague after being convicted of involvement in a

terrorist organization, inciting terrorism, and terrorist training. He spread violent jihadist and IS-related content through various social media platforms, including managing 30 Telegram channels with pro-IS material, which had up to 1,024 followers at the time of his arrest (Europol, 2024, p. 17).

TARGETED RECRUITMENT AND PROPAGANDA TECHNIQUES

Online radicalization frequently stems from strategic psychological tactics employed by extremist groups. These groups take advantage of people's emotional weaknesses, such as loneliness, the need for connection, and the quest for purpose, to draw them in. Through advanced recruitment methods like personalized targeting and crafting compelling emotional stories, they successfully influence some individuals toward radical beliefs and motivate them to act.

Modern terrorist groups recognize that uniform recruitment tactics are ineffective. They adopt tailored messaging strategies by segmenting their audiences based on criteria such as age, gender, religion, geography, psychological characteristics, and specific grievances. This approach allows them to create customized content that strongly appeals to each distinct group.

For young men, the recruitment material often features dynamic, action-packed scenes that mimic violent video games, appealing to their sense of adventure and desire for excitement. The narratives are designed to frame involvement in the cause as both thrilling and heroic.

Meanwhile, the messaging directed toward women is entirely different. Recruiters often emphasize themes of sisterhood and belonging. They highlight the importance of marriage to fighters and the role of motherhood within the movement, casting these roles as vital contributions. This approach offers women both a sense of community and meaningful purpose.

For Western Muslims who feel alienated or discriminated against, the messaging takes on yet another tone. Here, recruiters focus on the internal struggles of identity and belonging, presenting a "pure" Islamic community as a remedy for feelings of isolation and marginalization. They suggest that joining their group will resolve identity conflicts and provide a supportive environment, making radical engagement feel like both a personal resolution and a just cause.

Regarding the narratives, extremist groups carefully shape their propaganda by using powerful ideological and emotional themes to influence their target audiences. One common approach is framing jihad as a religious obligation, portraying it as a sacred duty that every believer must fulfill. This taps into deep spiritual commitments to motivate followers.

They also emphasize a narrative of victimhood, focusing on the suffering of Muslims in conflicts such as those in Syria (Winter, 2015, p. 23). By highlighting these injustices, they seek to evoke strong feelings of anger and empathy, which can fuel a desire for action. Another important theme centers on heroism and martyrdom. Fighters who die in battle are glorified and depicted as honorable heroes, making sacrifice appear noble and desirable. This portrayal serves both to inspire recruits and to legitimize violence.

Lastly, these groups often promote apocalyptic visions, suggesting that a final, inevitable battle or the restoration of a caliphate is forthcoming. This sense of looming, historic urgency encourages supporters to commit themselves fully, believing they are part of a grand, divine struggle. Through these carefully crafted narratives, extremist organizations manipulate emotional and religious sentiments to deepen commitment and propel individuals toward radicalization.

Terrorist recruiters have become adept at manipulating social media platforms to further their agendas. They strategically use hashtags and keywords to draw in users who are either curious or politi-

cally engaged, making it easier to spread their content to a wide audience. To amplify their reach even further, they deploy networks of fake accounts that boost the visibility of extremist material, creating an illusion of popularity and legitimacy. Moreover, these groups often encourage potential recruits to move beyond public spaces into private and encrypted messaging apps like Telegram, Zero Net, or Rocket.Chat (King, 2019). These secure platforms provide a safer environment for grooming, indoctrination, and instruction away from the scrutiny of authorities.

Once initial contact is made, recruiters typically transition to one-on-one private conversations where they work to establish trust and provide personalized spiritual guidance. In these intimate exchanges, they offer tailored advice and emotional support, fostering a sense of brotherhood and belonging. They may also guide recruits through the practicalities of radical commitment, such as instructions for hijra (migration to conflict zones) or detailed steps for planning attacks. This personalized approach allows recruiters to gradually deepen the individual's involvement and commitment to the extremist cause. For example, Junaid Hussain, a British ISIS fighter, used Surespot (an encrypted messaging program) to recruit and guide attackers, including the Garland, Texas attackers in 2015 (Regional Cooperation Council, 2018).

PATTERNS OF RADICALIZATION IN NORTH MACEDONIA

Since the early 1990s, many foreign Muslim charities, mainly Arab, have found their way into the Balkan region, and thus into Macedonia, taking advantage of the lack of political and economic stability resulting from the collapse of socialism and the period of transition, as well as the reduced capacities of the security services to monitor suspicious activities. Most of these organizations were well-intentioned and did not have radical ideologies. Unfortunately, some more radical organizations managed to hide behind this screen while strengthening their presence in the Balkans and recruiting followers. Their huge financial resources helped them reach mainly the poor communities, which were actually their target group. The lack of sovereignty of certain parts of the country was fertile ground for radical-oriented organizations to spread extremist ideas in the local and religious environment, mainly based on radical ideology.

Although such radical ideas have been spreading throughout the country's population since the late 20th century, the war in Syria was an additional opportunity for recruiters of foreign fighters to successfully mobilize around 150 Macedonian citizens. A small number of them are believed to still be on the battlefields of the Middle East, some have died fighting for the ideals of ISIS, and most have been returned to the country. Of those repatriated, some have already served or are still serving prison sentences.

Although foreign fighters are mostly male (publicly available figures suggest that men make up approximately 83% of the total number of foreign fighters from Europe (European Parliamentary Research Service, 2018, p. 33)), women are not completely excluded from this phenomenon. For example, in early 2015, an 18-year-old girl from Kumanovo went to Syria, where she allegedly married after her arrival. According to her father, shortly before leaving, she had been communicating online with a girl from Kosovo, and videos with military propaganda content were found on her computer, which her classmates said she had also watched at school. An ethnic Macedonian woman from Struga also joined ISIS and converted to Islam, while another young girl from Aracinovo was prevented by her relatives from traveling to Syria, where she had an arranged marriage with a local foreign fighter. In another case, two girls from rural Skopje also tried to leave for Syria via Pristina in early 2016 but were found and returned by their relatives (Selimi & Stojkovski, 2016). In all of these cases, radicalization occurred online. This is a clear indication that girls are not immune to extremist propaganda, and they must not be excluded from prevention programs.

Radicalization in North Macedonia takes place both online and face-to-face. Very often, young people are targeted online, with certain twisted understandings of Islam being shared with them online, and once they are hooked, they are either redirected to closed groups on Telegram or similar encrypted applications or invited to certain improvised prayer rooms, mosques, and premises of religious NGOs, where they undergo continued radicalization. This was the case with most of the young people who, after receiving radical religious ideology, left for the battlefields in Syria and Iraq in the period from 2012 to 2017.

In the last few years, there has been a notable decline in the number of foreign fighters departing from North Macedonia and the broader Balkan region to conflict zones such as Syria and Iraq. This is largely due to the territorial defeat of ISIS, enhanced international cooperation, and legal frameworks that criminalize participation in foreign conflicts. As a result, the issue of foreign fighter recruitment has diminished in urgency, although the legacies of that phenomenon, such as the return of radicalized individuals, continue to pose challenges.

With the physical caliphate dismantled, attention has increasingly turned to online radicalization, where extremist content continues to circulate across encrypted messaging platforms and social media. Individuals, especially youth, are now more vulnerable to radical ideologies spread digitally, often in isolation from traditional recruitment networks. This shift has also given rise to lone-actor threats, where individuals, radicalized online and acting without direct organizational ties, may plan or commit acts of violence. These actors are more difficult to detect and prevent through conventional counter-terrorism methods.

OVERVIEW OF DOCUMENTED CASES – CASE STUDY OPERATION "CELL"

The "Cell" case was the largest and most significant case in North Macedonia related to radicalization and recruitment of foreign terrorist fighters (FTFs). According to the investigation, the alleged mastermind behind the operation was Redzep Memishi, a self-proclaimed imam from Skopje. He was known for spreading extremist ideology to young people, both face-to-face in informal religious gatherings and online, using platforms such as Facebook and YouTube to share his preaching. In March 2016, the Basic Criminal Court in Skopje sentenced Memishi to seven years in prison for organizing and participating in a foreign paramilitary group, under Article 322-a of the Macedonian Criminal Code. Memishi pleaded guilty and reached a plea agreement with the prosecution. Five other defendants also received prison sentences (Selimi & Stojkovski, 2016). The case marked a turning point in North Macedonia's counter-terrorism efforts, drawing widespread attention to the threat of violent extremism, especially among disenfranchised youth. It highlighted the role of local radical preachers and digital platforms in facilitating recruitment and ideological indoctrination. Following this initial prosecution, Macedonian authorities launched related investigations known as "Cell 2" and "Cell 3", targeting additional extremist networks and individuals suspected of supporting terrorist organizations or planning to travel to conflict zones.

Memishi's online presence continued to be a potential recruiting tool for Macedonian extremists despite his imprisonment, as online lectures continued to circulate in the virtual space. Today, after serving his prison sentence and being released, the self-proclaimed imam is once again active on social media with his Facebook, Instagram, YouTube, and Telegram accounts.

The case of Redzep Memishi illustrates the persistent influence of ideologically motivated actors in the digital sphere, even after formal criminal sanctions have been imposed. His continued online presence

following imprisonment, and the circulation of his content during and after incarceration, demonstrate the limitations of punitive measures alone in addressing violent extremism. The reactivation of his social media profiles, coupled with a follower base of approximately 16,000 across different online platforms, points to a sustained demand for his messaging and highlights the resilience of extremist narratives in online ecosystems.

From a counter-radicalization perspective, this situation underscores the need for integrated strategies that go beyond legal prosecution to include digital monitoring, counter-messaging, and community-based interventions. The Memishi case exemplifies how offline radicalization structures can transition into enduring online influence, posing ongoing risks for ideological dissemination and potential recruitment, especially among vulnerable or previously exposed individuals. It calls for institutional coordination between judicial systems, cybersecurity agencies, and civil society to prevent recidivism and to mitigate the spread of extremist ideologies in the digital realm.

In addition to the case of Redzep Memishi, in December 2024 and January 2025, North Macedonia confronted critical developments in counter-terrorism efforts with the dismantling of terrorist cells in Gostivar and Struga. In December 2024, authorities uncovered a newly formed terrorist group engaged in recruitment and coordination primarily via digital platforms, including encrypted messaging apps and social media (Telma, 2024). Shortly after, in January 2025, the Ministry of Interior filed terrorism charges against four individuals suspected of affiliation with a terrorist organization. Investigations revealed that this group similarly relied on online communication tools to promote extremist ideologies, share radical content, and maintain contact with like-minded individuals domestically and abroad (Agency for National Security, 2025).

Together, these cases highlight the increasingly digital nature of radicalization and terrorist operations, where internet-based networks facilitate ideological influence, recruitment, and logistical support across national borders. The transnational connections observed emphasize the need for comprehensive cyber surveillance measures and intensified cross-border cooperation within the region. This evolving threat landscape challenges traditional security frameworks, underscoring the necessity of integrating advanced technological capabilities and adaptive policies to effectively counter online radicalization and disrupt terrorist activities in the digital era.

In addition to the aforementioned developments, it is important to recognize the significant role social media has played in the recruitment of foreign fighters for the conflict in Ukraine, despite this not directly involving the dissemination of radical religious ideology. At the onset of the war in 2022, the Ukrainian Embassy in North Macedonia issued a call via its official Twitter account, urging citizens to enlist as volunteers in the International Legion for the Defense of Ukraine (Sloboden Pecat, 2025). However, the Ministry of Foreign Affairs of North Macedonia emphasized that, under the Macedonian Criminal Code, participation in a foreign military force constitutes a criminal offense punishable by a minimum prison sentence of four years. This legal provision was enacted through amendments to the Criminal Code in 2014, following the prior mobilization of Macedonian nationals to conflict zones in Syria as part of ISIS ranks. The legislation aims to prevent extremism and deter the recruitment of Macedonian citizens for foreign conflicts.

This case highlights the complexities of foreign fighter recruitment in the digital age, demonstrating how social media can facilitate mobilization efforts while existing legal frameworks seek to mitigate associated security risks. It underscores the need for continued vigilance and adaptation of national legislation to address evolving methods of recruitment beyond traditional radicalization pathways.

CHALLENGES FOR LAW ENFORCEMENT AND POLICY

One of the primary challenges in countering online radicalization lies in the widespread use of encryption and online anonymity. End-to-end encryption technologies employed by messaging platforms such as Signal, WhatsApp, and Telegram significantly hinder the ability of law enforcement agencies to intercept and monitor communications, even with legal authorization. These platforms are increasingly utilized by extremist actors who exploit the privacy protections to disseminate propaganda, coordinate activities, and recruit followers without detection. While these technologies serve legitimate purposes in protecting privacy and freedom of expression, they simultaneously create operational blind spots for security agencies, who must navigate the tension between ensuring public safety and respecting civil liberties. The use of the dark web is another additional challenge for law enforcement. Although the main business in dark web markets remains illicit drugs (Europol, 2024), terrorists also use the dark web to provide information to fellow terrorists, to recruit and radicalize, to spread propaganda, to raise funds, and to coordinate actions and attacks (Weimann, 2016).

According to Gabriel Weimann, following the Paris attacks in November 2015, ISIS notified its supporters that its official Isdarat website – which hosts propaganda and media releases – had shifted to the Dark Web by providing a ".onion" address accessible via Tor. The group explained this move was a response to persistent efforts to take down its conventional domains and announced the launch of its site on the Dark Web to bypass these restrictions (Weimann, 2016).

A significant obstacle in countering online radicalization is the presence of jurisdictional and legal barriers that hinder timely law enforcement intervention. Radicalizing content is often hosted on servers located in foreign jurisdictions, complicating the process of investigation and content removal due to differing national laws and sovereignty issues. The global nature of the internet allows extremist groups to exploit the "safe havens" of permissive or under-regulated digital spaces, effectively evading enforcement by operating across borders (Weimann, 2016). Furthermore, inconsistencies in legal definitions of key terms such as "radicalization," "extremism," and "terrorist content" across different legal systems inhibit coordinated international responses. For instance, what may constitute hate speech or incitement in one country might be protected speech in another, leading to legal ambiguity and enforcement paralysis (UNODC, 2012). These disparities delay mutual legal assistance procedures, limit the scope of extradition or prosecution, and challenge digital evidence collection in transnational investigations. As a result, policymakers and law enforcement must continually negotiate the delicate balance between respecting national sovereignty and responding to the inherently globalized threat posed by online radicalization.

One of the core dilemmas for law enforcement in preventing violent extremism is the difficulty of identifying individuals in the early stages of radicalization. Radicalization often occurs incrementally and in private digital spaces, such as encrypted chat rooms or anonymous forums, where individuals are exposed to extremist content without outward behavioral changes. Many radicalized individuals are "self-starters" who never directly interact with terrorist organizations or known extremists, making them invisible to traditional intelligence methods. Additionally, communities may be reluctant to report early warning signs due to fear of stigmatization or distrust in authorities. On the other hand, not everyone knows how to recognize changes in the behavior of a radicalized person (withdrawal, in some cases aggression towards dissenters, growing a beard (in men)), especially if the person is young, so they often attribute such changes to puberty and the passing phase of youth. These limitations reduce the efficacy of early intervention programs and underscore the need for multi-agency collaboration involving schools, mental health services, and community leaders in identifying at-risk individuals.

Law enforcement agencies struggle to effectively combat online radicalization due to limited resources, including insufficiently trained personnel and outdated technology. The vast amount of extremist content across platforms overwhelms monitoring efforts, while extremist groups use low-cost digital tools to quickly spread propaganda. This digital capability gap highlights the need for greater investment, coordination, and international cooperation to enhance law enforcement effectiveness.

Moreover, law enforcement efforts heavily rely on cooperation from technology companies, but this collaboration is often inconsistent. While major platforms like Meta and Google actively remove extremist content, smaller platforms and encrypted services, including Telegram, have historically been less responsive due to concerns about user privacy, brand reputation, and legal risks, alongside the absence of global standards for content moderation and data disclosure (Organisation for Economic Co-operation and Development (OECD), 2024). However, the Lawfare Institute (2025) notes that, as of 2025, Telegram has markedly improved its cooperation with authorities, responding to regulatory pressure by increasing compliance with data requests and removing illicit content more promptly. Despite these advances, Telegram's encrypted and pseudonymous design still poses enforcement challenges, underscoring the need for sustained public-private partnerships that balance lawful access to information with privacy and platform accountability.

CONCLUSION

Radicalization today is often a hybrid phenomenon involving both offline and online influences, with fully online pathways notably on the rise. The internet and social media continue to play a crucial role in spreading jihadist terrorist propaganda, targeting individuals for radicalization and recruitment into terrorism and violent extremism. But it's important to note that social media is not the cause of radicalization, it's an accelerant. Key platforms for these activities include online forums, video gaming networks, decentralized platforms, and the dark web.

The recruitment process has evolved from broad public propaganda to highly personalized, often private, one-on-one interactions facilitated through encrypted messaging platforms such as Telegram, Signal, and others. These platforms allow recruiters to provide spiritual guidance, emotional support, and operational instructions securely and covertly.

Online platforms have drastically shortened the radicalization process, especially among youth, making countries more vulnerable to fast-spreading extremist ideologies. Young people's heavy social media use exposes them to manipulative content during a sensitive developmental period, increasing their risk of adopting extremist views.

The analysis of radicalization cases in North Macedonia further illustrates these dynamics, showing concrete examples of how social media and encrypted communication have facilitated recruitment and engagement, including among women – a demographic sometimes under-addressed in prevention efforts.

To address this, countries should strengthen digital literacy and critical thinking education, collaborate with tech companies to monitor and remove harmful content, provide early support for at-risk youth, and promote inclusive policies that tackle underlying social issues.

Overall, confronting the challenge of online radicalization demands a multi-faceted and adaptive approach that combines technological, socio-psychological, educational, and policy dimensions. Addressing the personalized and increasingly digital nature of radicalization processes remains pivotal to mitigating violent extremism in the modern era.

REFERENCES

Agency for National Security. (2025). Вести [News]. Retrieved July 23, 2025, from https://www.anb.gov.mk/vesti.html

Al Jazeera. (2025, June 7). Yemen's al-Qaeda leader threatens Trump, Musk over Israel's war on Gaza. Retrieved July 20, 2025 from https://www.aljazeera.com/news/2025/6/7/yemens-al-qaeda-leader-threatens-trump-musk-over-israels-war-on-gaza

Bodine-Baron, E., Helmus, T. C., Magnuson, M., & Winkelman, Z. (2016). Examining ISIS Support and Opposition Networks on Twitter. RAND Corporation. Retrieved July 27, 2025, from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1328/RAND_RR1328.pdf

Conway, M., Scrivens, R., & Macnair, L. (2018, July). Use of social media by U.S. extremists (START Research Brief). National Consortium for the Study of Terrorism and Responses to Terrorism (START), University of Maryland. Retrieved July 20, 2025 from https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

European Parliamentary Research Service. (2018). The return of foreign fighters to EU soil: Ex-post evaluation (Study No. 621811). European Parliament. Retrieved July 23, 2025, from https://www.europarl.europa.eu/RegData/etudes/STUD/2018/621811/EPRS_STU(2018)621811_EN.pdf

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union. Retrieved July 23, 2025, from https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

Europol. (2024). European Union terrorism situation and trend report 2024 (EU TE-SAT 2024). Publications Office of the European Union. Retrieved July 27, 2025, from https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf

King, P. (2019). Islamic State group's experiments with the decentralised web [Conference paper]. European Counter Terrorism Centre (ECTC) Advisory Network, Europol. Retrieved July 23, 2025, from https://www.europol.europa.eu/sites/default/files/documents/islamic_state_group_experiments_with_the_decentralised_web_-_p.king_.pdf

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). *Overview: Profiles of Individual Radicalization in the United States—Foreign Fighters (PIRUS-FF)*. U.S. Department of Homeland Security. Retrieved July 20, 2025 from https://www.dhs.gov/sites/default/files/publications/OPSR_TP_Overview-Profiles-Individual-Radicalization-US-Foreign-Fighters_508.pdf

NEFA Foundation. (n.d.). As-Sahab is the official media wing of Al-Qaida's core leadership [CIA Abbottabad compound documents]. Retrieved July 23, 2025, from https://www.cia.gov/library/abbottabad-compound/F3/F3C107E83E79035F79728F26322A1B25_nefajihadmedia0309.pdf

Organisation for Economic Co-operation and Development (OECD). (2024). Transparency reporting on terrorist and violent extremist content online (4th ed., OECD Digital Economy Papers, No. 367). OECD Publishing. Retrieved July 23, 2025, from https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/transparency-reporting-on-terrorist-and-violent-extremist-content-online_3f72a170/901cb8cf-en.pdf

Regional Cooperation Council. (2018, November 22). Inside the hunt for the world's most dangerous terrorist – How a British hacker joined ISIS's top ranks and launched a deadly global cyber plot. Retrieved July 24, 2025, from https://www.rcc.int/swp/news/159/inside-the-hunt-for-the-worlds-most-dangerous-terrorist--how-a-british-hacker-joined-isiss-top-ranks-and-launched-a-deadly-global-cyber-plot

Ryan, M. W. S. (2015). Hot issue: How DAESH's lone wolf guidance increases the group's threat to the United States. The Jamestown Foundation. Retrieved July 28, 2025, from https://jamestown.org/program/hot-issue-how-daeshs-lone-wolf-guidance-increases-the-groups-threat-to-the-united-states/

Selimi, K., & Stojkovski, F. (2016). Assessment of Macedonia's efforts in countering violent extremism: View from civil society. Analytica. Retrieved July 23, 2025, from https://www.analyticamk.org/images/Files/extremisim-mk-updated-FINAL-UPDATED-web_b30f9.pdf

Simonetti, R. (2021, February 11). The problem isn't just one insurrection. It's mass radicalization. Politico. Retrieved July 23, 2025, from https://www.politico.com/news/magazine/2021/02/11/mass-radicalization-trump-insurrection-468746

Stern, J., & Berger, J. M. (2015). ISIS: The state of terror. HarperCollins.

Telma. (2024, December 15). Уапсена терористичка ќелија во Гостивар и Струга – регрутирале жители за свои активности [A terrorist cell arrested in Gostivar and Struga – recruited locals for their activities]. Retrieved July 23, 2025, from https://telma.com.mk/2024/12/15/uapsena-teroristichka-kelija-vo-gostivar-i-struga-regrutirale-zhiteli-za-svoi-aktivnosti/ Ask ChatGPT

The Lawfare Institute. (2025, May 23). Telegram Is Cooperating with Authorities, for Now. Lawfare. Retrieved July 23, 2025, from https://www.lawfaremedia.org/article/telegram-is-cooperating-with-authorities--for-now

United Nations Office on Drugs and Crime. (2012). The use of the Internet for terrorist purposes. United Nations. Retrieved July 23, 2025, from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

U.S. House Committee on Oversight and Government Reform. (2015, October 28). Radicalization: Social media and the rise of terrorism (Hearing before the Subcommittee on National Security, 114th Congress, Serial No. 114-57). U.S. Government Publishing Office. Retrieved July 20, 2025 from https://www.govinfo.gov/content/pkg/CHRG-114hhrg97977/html/CHRG-114hhrg97977.htm

U.S. House of Representatives, Subcommittee on National Security, Committee on Oversight and Government Reform. (2015, October 28). *Radicalization: Social media and the rise of terrorism* [Hearing transcript]. U.S. Government Publishing Office. Retrieved July 23, 2025, from https://www.govinfo.gov/content/pkg/CHRG-114hhrg97977/html/CHRG-114hhrg97977.htm

Vidino, L., Marone, F., & Entenmann, E. (2017). Fear Thy Neighbor: Radicalization and Jihadist Attacks in the West. Ledizioni LediPublishing. Retrieved July 24, 2025, from https://icct.nl/sites/default/files/import/publication/FearThyNeighbor-RadicalizationandJihadistAttacksintheWest.pdf

Weimann, G. (2016). Terrorist Migration to the Dark Web. Perspectives on Terrorism, 10(3), 40–44. Retrieved July 23, 2025, from https://www.jstor.org/stable/26297596

Winter, C. (2015, October). Documenting the virtual 'caliphate'. Quilliam. Retrieved July 23, 2025, from https://core.ac.uk/download/pdf/30670971.pdf

Слободен Печат. (2025, April 17). Украина бара воени доброволци од Македонија, но за тоа кај нас се оди во затвор пет години. Слободен Печат. Retrieved July 23, 2025, from https://www.slobodenpecat.mk/ukraina-bara-voeni-dobrovolci-od-makedonija-no-za-toa-kaj-nas-se-odi-vo-zatvor-pet-godini/