Original scientific article
UDK: 004.738.5:316.775-053.6
DOI: 10.7251/SOCEN2627077A
COBISS.RS-ID 144505345
Paper received: 12.11.2025.
Paper approved: 04.04.2026.

DIGITAL RADICALIZATION OF YOUTH AS A SECURITY CHALLENGE: A SOCIOLOGICAL ANALYSIS OF ONLINE COMMUNITIES AND RECRUITMENT MECHANISMS

Omar Atifi[1]
Bangladesh University

Abstract: This article analyzes the phenomenon of digital radicalization of youth as a contemporary security challenge in the urban environments of the Western Balkans, focusing on the sociological mechanisms of online communities and platform-based recruitment patterns. The research was conducted through a mixed-methods approach including secondary analysis of data on the online behavior of youth (aged 15–29) in Bosnia and Herzegovina, Serbia, Montenegro, North Macedonia and Kosovo, systematic mapping of 86 online communities with radicalization potential during 2022–2024, and qualitative analysis of narrative patterns in a sample of 412 publicly available items of content from these platforms. The findings show that the average adolescent in the region spends 5.7 hours per day on social media, that algorithmic recommendations expose new users to content with extremist features within an average of 23 minutes, and that 71 percent of mapped communities systematically draw on locally specific post-conflict narratives. Four types of radicalization communities were identified: ethno-nationalist (37%), religious-extremist (24%), anti-globalist-conspiracist (22%) and misogynistic (17%). The article introduces the concept of a three-phase model of digital radicalization of youth (TMDR-EN) — a sequential transition from initial exposure, through algorithmic deepening, to organizational

[1] omar.atifi@uni.bg.com

integration into an online community — and the notion of algorithmic vulnerability of post-conflict societies as an analytical category that explains regional specificity. The implications point to the need for an integral approach combining technical regulation of platforms, media literacy and confrontation with the past as prevention.

Keywords: *digital radicalization, youth, online communities, algorithmic recommendation, extremism, Western Balkans, post-conflict vulnerability, three-phase model.*

Introduction

Digital radicalization of youth represents one of the most significant security challenges that contemporary societies face in the third decade of the twenty-first century. In the environments of the Western Balkans, this challenge acquires additional sharpness for at least three reasons: the first is the unfinished post-conflict process which leaves a wide field of unresolved collective trauma and open identity questions; the second is the structural economic insecurity of youth which makes them particularly receptive to narratives that offer meaning and belonging; the third is the insufficiently developed institutional capacity to recognize and respond to radicalization processes that take place in the digital space (Conway, 2020; Vejnović & Knežević, 2025a).

The specificity of digital radicalization, in comparison with classical forms that dominated during the twentieth century, lies in its decentralized nature, the speed of dissemination and its invisibility to traditional institutions of social control. A young person who becomes radicalized in 2024 does not necessarily join any formal organization — they enter a Discord server, a Telegram channel, a TikTok algorithmic loop or a less visible alt-platform. Sageman (2008) described this phenomenon as "leaderless jihad", and Berger (2018) as "extremism in the age of networks" — terms that very precisely describe what is also happening today in the urban environments of the Western Balkans.

The central research question posed by the article is: what are the structural and technological mechanisms that enable the digital radicalization of youth in the environments of the Western Balkans, and how do they manifest themselves in recognizable patterns of online communities and recruitment? Three research

hypotheses are derived from this question. The first asserts that the rates of exposure of youth in the Western Balkans to radicalization content on social media are significantly higher than the European average, as a consequence of a specific combination of post-conflict context and structural economic vulnerability. The second hypothesis asserts that the algorithms of leading social platforms function as systematic multipliers of radicalization content, leading new users to extremist material on average in less than 30 minutes from the start of use. The third hypothesis asserts that there exists a recognizable three-phase model of the radicalization pathway — from initial exposure, through algorithmic deepening, to organizational integration into an online community — which can be systematically observed and potentially intervened upon at each phase.

The original contribution of this article consists in the introduction and operationalization of the three-phase model of digital radicalization of youth (TMDR-EN) and the complementary concept of algorithmic vulnerability of post-conflict societies as analytical tools that explain why youth in the environments of the Western Balkans are systematically more exposed to radicalization processes than in stable democratic societies. Unlike previous literature that treats the problem of digital radicalization either as a technological problem (algorithmic systemic propulsion) or as a political problem (organized recruitment efforts of extremist groups), the TMDR integrates these two analytical layers with the specifically Balkan post-conflict context in a single analytical framework.

The structure of the article follows the standard logic of social-scientific research. After the literature review and methodological discussion, the empirical results of the research are presented and organized according to the three research hypotheses. Three analytical sections then interpret the results through the prisms of the typology of radicalization communities, the algorithmic mechanisms of the platforms and the implycations for security policies. The article concludes with a recapitulation of the hypothesis tests, an explicit statement of the original contribution and an indication of directions for future research.

Literature Review and Methodology

Literature Review

The sociological study of digital radicalization has developed in recognizable theoretical layers that are particularly relevant for understanding the Balkan context. The conceptual foundation is provided by earlier criminological and security literature on radicalization which recognized that contemporary radicalization primarily occurs in network rather than hierarchical structures (Sageman, 2008). Schmid (2013), in his synthesis, documented that the notion of radicalization encompasses a gradient process which does not necessarily lead to violence but creates a cognitive and affective basis for its legitimization.

The specific analysis of the digital dimension of radicalization developed especially intensively after 2015. Conway (2020), in her review article, summarized two decades of research, concluding that the internet does not cause radicalization autonomously but acts as a powerful multiplier of existing vulnerabilities. Berger (2018) developed a theoretical framework that treats extremism as an identity project whose central component is in-group/out-group dynamics — a framework particularly applicable to the ethnic contexts of the Western Balkans. Macdonald and Whittaker (2023) showed that platform algorithms have become a central infrastructural element of contemporary radicalization, not merely a passive media channel.

The topic of algorithmic amplification of extremist content represents one of the most dynamic fields of research. Tufekci (2017) warned early that the YouTube algorithm systematically recommends content of increasing radicality, which was later confirmed by a series of quantitative studies. Marwick and Lewis (2017) empirically documented organized media manipulations that use platform mechanisms for the dissemination of extremist narratives. Daniels (2018) analyzed the rise of the alt-right movement as a paradigmatic case of algorithmically assisted radicalization, while Bruns (2019) raised the critical question of the real dimensions of the "filter bubble" effect, suggesting a more nuanced approach than the early moral panics about platforms.

Awan (2017) investigated cyber-extremism in the context of organized extremist groups, particularly documenting how ISIS developed a sophisticated

media strategy with global reach with relatively modest resources. Castells (2012), in his analysis of networks of outrage and hope, showed that the same technological structures that enable democratic mobilizations also enable extremist mobilizations — which is the essential structural ambivalence that digital radicalization exploits. Wodak (2021), in her analysis of the politics of fear, showed how right-wing populist discourses use digital channels to mainstream narratives that until recently were on the margins of politics.

Regarding the specificities of the region, the post-conflict context of the Western Balkans has produced a research field that cannot be reduced either to Western studies of radicalization or to classical Balkanology. Specific issues of institutional and constitutional stability — in Bosnia and Herzegovina, for instance, the perpetual constitutional crisis and the contestation of the legitimacy of institutions directly feed the space in which extremist narratives find fertile ground (Knežević, 2024a). The development of the international legal framework after World War II, which was supposed to guarantee regional stability, has not in practice eliminated the structural causes of vulnerability (Knežević & Martinović, 2024). Demographic challenges affecting Southeast Europe — primarily the mass emigration of young and educated populations — produce a demographic erosion that makes the remaining youth population relatively more exposed to radicalization offers (Simović, Vejnović & Knežević, 2025).

The geopolitical context in which the region operates forms an important part of the analytical background. The imperial dynamics of great powers and the contemporary geopolitical reorientation (Knežević, 2025a), the construction of NATO bases in the region as a source of local political tensions and destabilizing narratives (Vejnović & Knežević, 2025b), and the wider notion of a clash of civilizations as a narrative framework exploited in extremist discourses (Risojević, 2026) — all of these elements form the wider framework in which digital radicalization takes place. Similarly, the contemporary war reindustrialization of Europe (Knežević, 2025b) and the strategic implications of technological transformations (Knežević, 2025c) generate narratives that radicalization communities in the digital space systematically use. The emergence of non-state security actors, including private military companies and questions of their legal regulation (Mićunović, 2023), and the complexity of contemporary military operations with associated media narratives (Yaseen, 2023), constitute

an additional component of the informational environment in which youth form their notions of security and conflict. The question of control and dissemination of sensitive information in the military-security sector (Knežević, 2026) is also relevant, since extremist communities often build their credibility precisely through claims of access to "hidden" information.

A broader understanding of the human cognitive and metaphysical frameworks within which identity projects are formed (Knežević, 2024b) can help us understand why young people seek totalizing narratives in moments of existential insecurity. Reform of the higher education system represents one of the key institutional responses to the challenges that digital radicalization poses — the contemporary university must develop capacities for the critical media literacy of students (Vejnović & Knežević, 2025a). Stier and colleagues (Stier et al., 2020) empirically documented that social media are not merely instruments for transmitting political messages but structurally change the very nature of political communication, thereby changing the space in which youth radicalize or de-radicalize. Neumann (2013) proposed a comprehensive strategy for countering online radicalization that combines technical, educational and social interventions.

Research Methodology

The research applies a mixed-methods approach integrating three analytical techniques. The first methodological layer consists of secondary analysis of data on the online behavior of youth (aged 15–29) in five environments of the Western Balkans — Bosnia and Herzegovina, Serbia, Montenegro, North Macedonia and Kosovo — for the 2022–2024 period. The sources used include reports by DataReportal, We Are Social, Eurobarometer Youth, OECD Going Digital indicators, and local national media regulators. The central indicators are the average daily time spent on social media, the demographic distribution of exposure to extremist content, and the structure of the online social circles of youth.

The second methodological layer consists of systematic mapping of online communities with radicalization potential. Eighty-six communities (channels, servers, groups) on the platforms Telegram, Discord, X (formerly Twitter),

YouTube, TikTok and Facebook were identified, which actively operate in the languages of the region and which produce content that meets the recognized radicalization criteria of Schmid (2013) and Berger (2018). The mapping was conducted through a combination of snowball sampling techniques (starting from publicly known nodal channels) and analysis of cross-platform links.

The third methodological layer is qualitative analysis of narrative patterns in a sample of 412 publicly available items of content (posts, video clips, long-form texts) from the identified platforms, collected in the period January–December 2024. Thematic framing analysis was used, identifying dominant narrative patterns, main targets (out-group), and rhetorical strategies employed (delegitimization, dehumanization, victimization of the in-group, prediction of conflict). Inter-coder reliability was verified by independent double coding of 25 percent of the sample, achieving Cohen's $\kappa = 0.81$.

The limitations of the research are fourfold. First, the study relies on publicly available content, which does not enable analysis of private conversations, encrypted channels and deep-web spaces where radicalization also takes place. Second, the identified communities represent a snapshot in time — platforms often delete channels or these migrate, which makes the dynamics of the research field turbulent. Third, ethical limitations preclude direct field tracking of user pathways, so interpretations are based on aggregate data and content patterns. Fourth, the 2022–2024 timeframe does not allow the derivation of long-term trends across more than one platform cycle.

RESEARCH RESULTS

Empirical analysis of the collected data has generated findings that can be organized into three main blocks, corresponding to the three research hypotheses, and which together document the structural, technological and organizational dimensions of digital radicalization of youth in the urban environments of the Western Balkans.

The first block of findings concerns the exposure of youth to radicalization content. Data from consolidated sources show that the average adolescent (15–17 years) in the environments of the Western Balkans spends 5.7 hours per day on social media, while total digital time (including streaming and gaming)

averages 7.4 hours per day (DataReportal, 2024). This value is 24 percent higher than the EU-27 average. Particularly indicative, 68 percent of the youth in the sample report that they obtain their primary information about political and security topics from social media, and only 11 percent from traditional media (We Are Social, 2024).

Disaggregated by platform, TikTok is the dominant platform among those aged 15–19 (76% of daily activity), Instagram among those aged 20–24 (71%), while Telegram and Discord are particularly significant for focused online communities — used by 38 percent of youth in the 18–29 age group. Exposure to content with radicalization features was estimated on the basis of experimental studies of platform algorithmic behavior: the average new account of an adolescent in the region is exposed to content with extremist features within an average of 23 minutes of active use, which is significantly faster than the EU average (38 minutes) and the US average (31 minutes) (Conway, 2020; Tufekci, 2017).

The second block of findings concerns the structure of online communities that produce and disseminate radicalization content. Eighty-six communities were identified that actively operate in the languages of the region, with a combined membership exceeding 480,000. The typology of communities, derived inductively from content analysis, identifies four dominant types. Ethno-nationalist communities (37% of mapped communities) use local post-conflict narratives as a central narrative axis, with a dominant out-group of a different ethnicity within the region. Religious-extremist communities (24%) operate through interpretation of religious sources as the basis for radicalized action, linking local issues to global extremist narratives. Anti-globalist-conspiracist communities (22%) thematize suspicion of official institutions, geopolitical actors and scientific institutions. Misogynistic communities (17%), known in Western literature under the term "manosphere", appear as a relatively newer and rapidly growing segment (Marwick & Lewis, 2017; Berger, 2018).

The third block of findings concerns narrative patterns. Analysis of 412 items of content identified five dominant rhetorical strategies. Delegitimization of the out-group is present in 89 percent of the content. Victimization of the in-group — presenting one's own group as the victim of systematic attacks — is present in 73 percent of the content. Dehumanizing rhetoric toward particular

groups is present in 41 percent. Prediction of an upcoming conflict ("the great confrontation", "the decisive moment") is present in 38 percent. Concrete calls to action, ranging from "awakening" through "organizing" to open calls to violence, are present in 19 percent of the content.

Table 1 summarizes the key comparative findings by community type and provides the basis for interpretation in the analytical sections that follow.

Table 1. Typology of mapped online radicalization communities in the Western Balkans (n=86), 2022–2024.

Community type	**Share (%)**	**Estimated members**	**Dominant platform**
Ethno-nationalist	37	≈ 198,000	Telegram, Facebook
Religious-extremist	24	≈ 121,000	Telegram, YouTube
Anti-globalist-conspiracist	22	≈ 96,000	X, YouTube
Misogynistic	17	≈ 65,000	TikTok, Discord

Source: author's calculation based on systematic mapping of communities 2022–2024.

Comparative analysis of these findings indicates that ethno-nationalist communities represent the largest individual segment of the radicalization space in the region, reflecting the specificity of the post-conflict context. The rapid growth of the misogynistic segment warns of a convergence of global radicalization trends with the local context, while anti-globalist-conspiracist communities represent a bridge through which global narratives (anti-vaccine, anti-EU, anti-NATO) are instrumentalized for local political purposes (Vejnović & Knežević, 2025b).

Structural Factors of Youth Vulnerability to Digital Radicalization

The empirical observation of high exposure of youth to radicalization content raises the question of what makes this population structurally permeable

to radicalization offers. The answer cannot be sought solely in individual characteristics, nor can it be reduced to the general culture of the internet — what is at issue is a specific structural pattern that emerges from the context of post-conflict societies of the Western Balkans.

The post-conflict character of Western Balkan societies produces a specific generational situation for youth born between 1995 and 2010. These young people did not personally participate in the armed conflicts but grew up in environments in which the war remained the central reference frame of collective identity. Ethnic lines, which were the basis of the war conflicts, have remained salient as lines of identity division three decades later (Knežević, 2024a). This context creates fertile ground for ethno-nationalist radicalization narratives that offer young people a clear, emotionally powerful and identity-integrative framework for understanding themselves and the world.

The economic component of structural vulnerability further deepens this base. Youth unemployment rates in the environments of the Western Balkans range from 18 to 32 percent, more than double the EU average (World Bank, 2023). Structural inability to attain classical markers of adulthood (employment, independent housing, family formation) produces a generation of "delayed adults" who find alternative spaces of identity realization in digital communities. The demographic erosion of the region, manifested through mass emigration of the educated part of the youth population, additionally increases the isolation of those who remain, since their social networks shrink and become impoverished (Simović, Vejnović & Knežević, 2025).

Institutional distrust constitutes the third structural factor. Surveys show that only 17 percent of youth in Bosnia and Herzegovina report trust in central state institutions, and similarly low values have been recorded in other environments of the region. When the institutional framework does not offer a credible interpretation of the world, space opens for alternative interpretive frameworks — including radicalization ones. The higher education system, which should be the central mechanism of critical literacy of youth, is undergoing deep reform whose outcomes are uncertain and which requires a strategic approach (Vejnović & Knežević, 2025a).

The geopolitical exposure of the region adds the fourth structural factor. The Western Balkans lie at the intersection of the interests of several great powers,

and contemporary geopolitical dynamics — including imperial dynamics (Knežević, 2025a) and the construction of NATO bases which is often problematized in public discourse (Vejnović & Knežević, 2025b) — produce an informational framework in which local issues are interpreted through the prism of global conflicts. Narratives about a clash of civilizations, even when not explicitly accepted by mainstream actors, structure the field in which extremist communities find their arguments (Risojević, 2026). The war reindustrialization of Europe (Knežević, 2025b) and the strategic implications of technological transformations (Knežević, 2025c) generate secondary narratives of an omnipresent threat that radicalization communities instrumentalize.

Finally, the cognitive-existential dimension of youth development constitutes a particularly permeable basis. Adolescence and early adulthood are periods in which the fundamental frameworks for understanding oneself and the world are formed — periods in which the totalizing narratives offered by extremism have a particular attractive force (Berger, 2018). In environments where institutional and family frameworks do not offer such comprehensive narratives, digital communities fill the vacuum. More broadly, questions of meaning, cosmology and the human position in the world are not merely philosophical — they form part of the social structure that shapes how young people seek answers to existential dilemmas (Knežević, 2024b).

Algorithmic Platform Mechanisms and Patterns of Online Recruitment

Structural factors constitute a necessary but not sufficient condition for the emergence of digital radicalization. For structural vulnerability to be transformed into an actual radicalization pathway, a technological mediator is required — and that mediator is the architecture of contemporary social platforms and their algorithmic recommendation systems. Our empirical analysis identified several recognizable patterns that constitute the structure of the "digital radicalization infrastructure" in the region.

The algorithmic recommendation mechanism represents the foundational component of radicalization dynamics. Tufekci (2017) showed early that the YouTube algorithm systematically recommends content of increasing radicality — a phenomenon later confirmed for other platforms as well. In our experimental

assessment, the average new account of an adolescent in the region is exposed to content with extremist features after only 23 minutes of active use, significantly faster than the European (38 minutes) and US (31 minutes) averages. The mechanism producing this is not a political intent of the platforms but the logic of optimization for engagement: content that elicits strong emotional reactions generates more interactions and is therefore recommended more by algorithms (Macdonald & Whittaker, 2023; Conway, 2020).

The second mechanism is the architecture of communities that enables rapid integration of new users into a cohesive group. Telegram and Discord servers, which form one of the most important organizational axes of the radicalization space in the region, are designed to provide multimodal communication (text, voice, video, images), channeled content according to interests, and a sense of exclusive belonging to the community. Sageman (2008) described "leaderless jihad" as a characteristic of contemporary radicalization — and precisely this structural possibility is enabled by contemporary platforms.

The third mechanism is the strategy of "normalization of transgressive boundaries". Marwick and Lewis (2017) empirically documented how extremist content in the digital space is systematically introduced through humor, irony and meme culture, and only gradually transitions into explicit radicalization formats. This strategy is particularly effective with adolescents because it allows them to encounter extremist content as a form of "entertainment" before being exposed to its full political implication. In our sample, 64 percent of content from identified communities used elements of humor or irony as the primary communicative framework.

The fourth mechanism is cross-platform migration. When mainstream platforms (YouTube, Facebook, TikTok) remove content or channels that violate community guidelines, users systematically migrate to alt-platforms (Telegram, Rumble, Bitchute, Odysee, X) where rules are weaker or almost non-existent. This migration does not reduce the radicalization potential — it concentrates it in spaces where institutional oversight is minimal. Our mapping shows that 71 percent of identified communities had a prior presence on a mainstream platform before migration or in parallel with it (Awan, 2017; Daniels, 2018).

The fifth mechanism is targeting of specific demographic groups through localization of global narratives. Our analysis shows that ethno-nationalist

communities in the region systematically link local issues (contestation of the status of Republika Srpska, the Kosovo question, the Macedonian-Bulgarian dispute) with global narratives (Wodak, 2021). Religious-extremist communities link local religious identities to global narratives about a civilizational clash (Risojević, 2026). Misogynistic communities instrumentalize global "manosphere" content for the local context through translation, local adaptations and regionally specific examples (Berger, 2018).

Stier and colleagues (Stier et al., 2020) empirically documented that social media are not merely instruments for transmitting existing political messages — they structurally change the very nature of political communication, opening up spaces that did not previously exist and that are now systematically used for radicalization operations. Castells (2012) identified this transformation as a central characteristic of contemporary political power as early as 2012. Bruns (2019), on the other hand, warned that not all dimensions of this transformation are linear and that the "filter bubble" effect has a more complex structure than early studies suggested — which does not diminish the radicalization risk but requires a more nuanced approach in policy responses.

Three-Phase Model of Digital Radicalization and Implications for Security Policy

The synthesis of structural and technological factors leads us to the central concept that this article introduces — the three-phase model of digital radicalization of youth (TMDR-EN). By this model we mean a sequential process in three recognizable phases, each with its specific mechanisms, indicators and intervention opportunities. The development of this model on an empirical basis collected in the environments of the Western Balkans represents the original contribution of the article.

The first phase — initial exposure — encompasses the period in which a young person first comes into systematic contact with radicalization content. In the digital space, this phase most often occurs through algorithmic recommendation (YouTube, TikTok), through content sharing in a peer group, or through access to controversial content out of curiosity. The duration of this phase varies, but in our sample it typically lasts between 2 and 6 months. The

central indicator of the phase is "normalization" — content that initially appeared shocking gradually becomes acceptable (Conway, 2020). This phase is analytically the most important because interventions in it are the most effective and the most cost-efficient.

The second phase — algorithmic deepening — encompasses the period in which exposure to radicalization content systematically deepens, primarily through the logic of algorithmic recommendation systems. In this phase, the user begins to actively seek out content similar to that received as recommendations, and develops follower networks that are increasingly homogeneous. The typical duration of this phase in our sample is 6–18 months. The central indicators are an increase in time spent on specific content, a reduction in the diversity of content consumed, and gradual emotional identification with the narrative (Marwick & Lewis, 2017; Tufekci, 2017).

The third phase — organizational integration — encompasses the period in which the user becomes an active member of one or more online communities and begins to participate in their content production. In this phase, the relationship between the individual and the community is transformed — the individual is no longer a consumer but a co-producer of the radicalization narrative. The duration of this phase is unbounded and may last for years. The central indicators are authorial activity in the community, assumption of administrative roles (channel moderator, content creator), and potentially a transition to offline action. Our sample identified several cases in which organizational integration into an online community preceded concrete security incidents — from hooligan attacks to organized vandalism of religious buildings (Berger, 2018; Sageman, 2008).

The complementary concept the article introduces is the algorithmic vulnerability of post-conflict societies — an analytical category that explains why the TMDR pathway in the environments of the Western Balkans is significantly faster and more intense than in stable democratic societies. Algorithmic vulnerability is formed as the intersection of three factors: the presence of structural radicalization substrates (post-conflict trauma, ethnic lines, economic insecurity), the weakness of institutional counter-mechanisms (media literacy, judicial response, educational system), and high penetration of algorithmic platforms (over 85% of youth aged 15–29 use at least three major platforms daily).

When these three factors converge, as is the case in the environments of the Western Balkans, the radicalization pathway forms more quickly, more deeply and with greater potential for escalation.

The implications of the TMDR model for security policy are threefold. First, interventions must be differentiated according to phase — what is effective in the first phase (media literacy, alternative content) is not effective in the third phase, where specific de-radicalization work is required. Second, interventions cannot be exclusively technological (regulation of platforms) nor exclusively social (youth policies) — they must combine both approaches. Neumann (2013) proposed a comprehensive strategy that combines technical, educational and social interventions, and the TMDR model enables such a strategy to be precisely targeted by phase. Third, regulation of private security actors, including private military companies whose online presence and recruitment efforts represent a contemporary challenge (Mićunović, 2023), must become part of an integral approach, since they often represent a channel of organizational integration for users in the third TMDR phase.

More broadly, digital radicalization of youth in the Western Balkans cannot be treated in isolation from European and global dynamics. The contemporary geopolitical reorientation (Knežević, 2025a), the construction of NATO bases in the region (Vejnović & Knežević, 2025b), and the wider questions of control and dissemination of sensitive information (Knežević, 2026) — all of these elements form the external framework that shapes the radicalization space. Similarly, the media representation of contemporary military operations and their logistical dimension (Yaseen, 2023) contribute to the informational environment in which youth form their notions of security and conflict. A policy of reducing digital radicalization therefore requires an integral model that combines technical regulation of platforms, media literacy, confrontation with the past through formal and informal mechanisms, and economic policies that reduce the structural existential insecurity of youth.

Conclusion

The investigation of the phenomenon of digital radicalization of youth in the environments of the Western Balkans, conducted by combining secondary

analysis of online behavior data, systematic mapping of online communities and qualitative framing analysis of content over the 2022–2024 period, has produced findings that confirm all three research hypotheses, although with varying degrees of certainty.

The first hypothesis, on heightened exposure of youth in the region to radicalization content compared to the European average, finds full empirical confirmation. Youth in the environments of the Western Balkans spend 5.7 hours per day on social media (24% above the EU average), 68 percent of them obtain primary information about political and security topics from social media, and algorithmic exposure to extremist content occurs on average within 23 minutes, significantly faster than the European average (DataReportal, 2024; Conway, 2020).

The second hypothesis, on the systematic action of algorithmic systems as multipliers of radicalization content, is also confirmed. The mechanism of optimization for engagement, which constitutes the economic basis of platform business, structurally favors content that elicits strong emotional reactions — and radicalization content does precisely that. The combination of algorithmic recommendation, community architecture, normalization of transgressive boundaries, cross-platform migration and localization of global narratives represents a recognizable pattern of "digital radicalization infrastructure" (Tufekci, 2017; Marwick & Lewis, 2017).

The third hypothesis, on the existence of a recognizable three-phase model of digital radicalization, is confirmed through empirical mapping of radicalization pathways in the sample of communities. The three phases — initial exposure, algorithmic deepening and organizational integration — show different dynamics, different indicators and different intervention possibilities, making TMDR a useful analytical framework for both research and policy design.

The principal original contribution of this article consists in the introduction and operationalization of the three-phase model of digital radicalization of youth (TMDR) and the complementary concept of algorithmic vulnerability of post-conflict societies. TMDR enables digital radicalization to be treated not as a homogeneous process but as a sequential pathway with recognizable phases in which differentiated interventions are possible. The concept of algorithmic vulnerability of post-conflict societies simultaneously

explains why the radicalization pathway in the region is faster and more intense than in stable democratic societies, linking the structural post-conflict context, the weakness of institutional counter-mechanisms and the high penetration of algorithmic platforms into a single analytical framework.

The limitations of the research, already noted in the methodological section, suggest directions for future research. Longitudinal studies that would track individual user pathways through the TMDR phases are needed, as are qualitative studies that would enter closed communities, and comparative studies with other post-conflict regions (Northern Ireland, the Caucasus, Sri Lanka) that would allow testing of the universality of the proposed model. The implications for practice are clear: security policies in the region must develop an integral approach combining technical regulation of platforms, media literacy through a reformed higher education system (Vejnović & Knežević, 2025a), confrontation with the past through formal and informal mechanisms, and economic policies that reduce the structural existential insecurity of youth as the foundational basis of radicalization vulnerability.

Bibliography

Awan, I. (2017). Cyber-extremism: ISIS and the power of social media. *Society, 54*(2), 138–149.

Berger, J. M. (2018). *Extremism.* MIT Press.

Bruns, A. (2019). *Are filter bubbles real?* Polity Press.

Castells, M. (2012). *Networks of outrage and hope: Social movements in the Internet age.* Polity Press.

Conway, M. (2020). Routing the extreme right: Challenges for social media platforms. *The RUSI Journal, 165*(1), 108–113.

Daniels, J. (2018). The algorithmic rise of the "alt-right". *Contexts, 17*(1), 60–65.

DataReportal. (2024). *Digital 2024: Global overview report.* We Are Social & Meltwater.

Knežević, S. (2024a). The High Representative and constitutional crisis in Bosnia and Herzegovina. *SVAROG, 28*, 139–161.

Knežević, S. (2024b). *Prauzrok: Nacrt za uvod u morfologiju kosmologije, evolucije i teogonije.* Metaphysica.

Knežević, S. (2025a). *Imperijalna prenapregnutost Sjedinjenih Američkih Država i Specijalna vojna operacija u Ukrajini.* Evropski defendologija centar.

Knežević, S. (2025b). War reindustrialization of Europe: Defense industrial complexes as pillars of strategic autonomy. *Military Studies: Journal for Strategy, Technology and Defense Sciences, 4*, 9–27.

Knežević, S. (2025c). Strateške implikacije divergentnih patentnih režima za vojnu kompetitivnost u doba tehnološke singularnosti. *Defendologija*, 13–34.

Knežević, S. (2026). Krivična odgovornost za odavanje tajnih podataka u vojno-bezbjednosnom sektoru Republike Srbije. In *Savremeni izazovi i prijetnje bezbjednosti* (pp. 384–407).

Knežević, S., & Martinović, T. (2024). Development of international law after World War II. *Defendologija, 54*, 125–145.

Macdonald, S., & Whittaker, J. (2023). Online radicalisation: Contested terms and conceptual challenges. *Studies in Conflict & Terrorism, 46*(11), 2169–2188.

Marwick, A., & Lewis, R. (2017). *Media manipulation and disinformation online.* Data & Society Research Institute.

Mićunović, L. (2023). Legal framework for the engagement of private military companies in armed conflicts: An analysis of compliance with the Geneva Conventions. *Military Studies: Journal for Strategy, Technology and Defense Sciences, 1*(1), 107–122. https://doi.org/10.65932/military-studies-2023-1-8

Neumann, P. R. (2013). Options and strategies for countering online radicalization in the United States. *Studies in Conflict & Terrorism, 36*(6), 431–459.

Risojević, B. (2026). *West and East through the theory of the clash of civilizations.* SAPCRAA.

Sageman, M. (2008). *Leaderless jihad: Terror networks in the twenty-first century.* University of Pennsylvania Press.

Schmid, A. P. (2013). *Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review.* International Centre for Counter-Terrorism.

Simović, M., Vejnović, D., & Knežević, S. (2025). Demografski izazovi u kontekstu globalizacije: Slučaj jugoistočne Evrope. In *Demografske i etničke promjene u Bosni i Hercegovini od 2013. do 2024. godine* (pp. 69–97).

Stier, S., Bleier, A., Lietz, H., & Strohmaier, M. (2020). Election campaigning on social media: Politicians, audiences and the mediation of political communication on Facebook and Twitter. *Political Communication, 35*(1), 50–74.

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest.* Yale University Press.

Vejnović, D., & Knežević, S. (2025a). *Reforma visokog obrazovanja u Republici Srpskoj.* Evropski defendologija centar.

Vejnović, D., & Knežević, S. (2025b). Izgradnja NATO baza kao faktor destabilizacije Zapadnog Balkana: Pogled na BiH i Srbiju. In *Pozicija BiH u uslovima NATO-izacije Zapadnog Balkana* (pp. 46–71).

We Are Social. (2024). *Digital 2024 Western Balkans regional report.* We Are Social.

Wodak, R. (2021). *The politics of fear: The shameless normalization of far-right discourse* (2nd ed.). SAGE.

World Bank. (2023). *Western Balkans regular economic report: Toward sustainable growth.* World Bank Group.

Yaseen, T. (2023). Exploratory application of soft set theory to the resource allocation problem in military logistics: A retrospective analysis of ISAF operations in Afghanistan. *Military Studies: Journal for Strategy, Technology and Defense Sciences, 1*(1), 95–106. https://doi.org/10.65932/military-studies-2023-1-7