HOW FIMI FUELS POLARISATION AND RADICALISATION IN THE WESTERN BALKANS

Case study



Skopje, 2026

Institute of Communication Studies

respublica

Title in Macedonian:

Како СММИ ја поттикнува поларизацијата и радикализацијата во Западен Балкан

Publisher:

Institute of Communication Studies
Jurij Gagarin Street No.17/1-1, Skopje
www.iks.edu.mk

For the publisher:

Prof. Zaneta Trajkoska PhD

Authors:

Prof. Arije Antinori PhD
Jordy Nijenhuis

Edition:

ResPublica

Layout:

Zoran Kardula

Graphic editing:

Dejan Joveski

Place and date:

Skopje, 2026

CIP - Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски“, Скопје

327.8:[316.4.063.24+316.647.7](497-15)(047.31)

ANTINORI, Arije
How fimi fuels and radicalisation in the Western Balkans
[Електронски извор] : case study / [authors Arije Antinori, Jordy Nijenhuis. - Skopje : Institute of Communication Studies, 2026. - (Edition ResPublica)

Начин на пристапување (URL): https://cdn.respublica.edu.mk/wp-content/uploads/2026/04/how-fimi-fuels-polarisation-and-radicalisation-in-the-western-balkans-en.pdf?_gl=1*qli4r9*_ga*MTk2MTg1NDAwNS4xNzY0NTQ2MTg2*_ga_H31JDGFEL3*czE3Nzc5ODE4NDQkbzI3JGcwJHQxNzc3OTgxODQ0JGo2MCRsMCRoMA...
- Превод на делото: Како СММИ ја поттикнува поларизацијата и радикализацијата во Западен Балкан.
- Текст во PDF формат, содржи 34 стр., илустр. - Наслов преземен од екранот. - Опис на изворот на ден 14.05.2026. - Фусноти кон текстот. - Библиографија кон главите

ISBN 978-608-4805-85-4

1. Nijenhuis, Jordy [автор]
а) Странски влијанија -- Поларизација -- Радикализација -- Западен Балкан -- Истражувања

COBISS.MK-ID 68802565

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

This product was prepared as part of the UK Government-funded project “TRACE: Tracking, Exposing, and Countering Hidden Foreign Manipulations and Interferences”, with support from the British Embassy in Skopje. The opinions and views expressed in this content do not necessarily reflect those of the British Government.

EXECUTIVE SUMMARY

This publication brings together two complementary analyses prepared by Prof. Dr. Arije Antinori[1] and Jordy Nijenhuis[2], to examine how Foreign Information Manipulation and Interference (FIMI) operates in contemporary information environments.

The first paper prepared by Prof. Antinori, ***Radicalisation and FIMI in the Western Balkans Cyber-Social Ecosystem***, analyses the Western Balkans as a highly contested information space in which FIMI functions through a hybrid infrastructure of digital platforms, legacy media, domestic political actors, transnational relays, and increasingly automated amplification that fuels radicalisation in the region. It shows that the region's vulnerability lies not only in foreign narratives themselves, but in the interaction between fragile media systems, polarised political contexts, platformised news consumption, and local actors capable of translating external manipulation into domestic conflict. In this sense, FIMI is presented not as an isolated messaging problem, but as an ecosystemic one.

The second paper prepared by Jordy Nijenhuis, ***Ambient Radicalisation: How FIMI Exploits Polarisation***, builds on this structural view by examining how such information environments affect audiences and societies over time. It argues that radicalisation today cannot be understood only as a process of direct ideological recruitment into extremist movements. Increasingly, it unfolds through diffuse, cumulative, and emotionally charged exposure to manipulative content that deepens distrust, sharpens divisions, and normalises more extreme interpretations of reality. The paper introduces the concept of ambient radicalisation to capture this broader process, in which the target is not only the individual at risk, but society as a whole.

Methodologically, they approach the subject from different but complementary angles. Prof. Antinori's contribution combines conceptual framing with comparative regional analysis, drawing on institutional reports, country-level media and digital indicators, platform-specific observations, and selected examples from across the Western Balkans to map the cyber-social ecosystem through which FIMI circulates, gains credibility, and fuels radicalisation. Jordy Nijenhuis's contribution, by contrast, takes a conceptual and illustrative approach, using existing research, institutional sources, and selected case studies from Europe and the Western Balkans to explore how manipulative and polarising information environments can contribute to more diffuse, cumulative processes of radicalisation over time.

The aim of this publication is therefore to move beyond siloed understandings of disinformation, hate speech, polarisation, and radicalisation. Instead, it argues for a more integrated approach that recognises how these phenomena interact within the same information environment. In the Western Balkans in particular, where unresolved political tensions, fragile media markets, identity disputes, and external influence intersect, such an approach is especially important. FIMI does not create these vulnerabilities from scratch. It exploits them, organises them, and amplifies them. This publication examines both how that process works and why it matters.

1 Arije Antinori is a Professor of Criminology and Sociology of Deviance at "Sapienza" University of Rome and a member of the Interpersonal Violence Research lab (InterViRe) at the Department of Human Neurosciences. He has a PhD in "Criminology for Investigation and Security" as well as a PhD in "Communication and Media Studies." He is an EU Senior Expert on Terrorism and T.O.C. (EENeT, EUROPOL ECTC-AN, CEPOL, EFD, EUROMED, ERCOR, RAN, GIFCT) as well as a Security Consultant, Police Force Trainer, Geopolitics and OSINT Analyst/Trainer, Social Media and Stratcom Expert. He is a member of WG-EXTREME at the European Society of Criminology.

2 Jordy Nijenhuis is a trainer and consultant, and co-founder of Dare to be Grey, an award winning organisation that aims to counter polarisation, disinformation and hate. He's involved in a variety of campaigns, and trains media professionals from all over the world in (social media) campaigning, storytelling and countering radicalisation, hate speech and disinformation.

RADICALISATION AND FIMI IN THE WESTERN BALKANS CYBER-SOCIAL ECOSYSTEM

Prof. Arije Antinori PhD

1. The Western Balkans as a Semantic Framework

The concept of the "Western Balkans" (WBs) does not correspond to a neutral geographical region, but rather to a politico-institutional category constructed from the outside. In the lexicon of the European Union, it designates Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia as a transitional space oriented towards Euro-Atlantic integration and EU enlargement (Council of the European Union, 2003; EPRS, 2023). Precisely for this reason, the term does not merely describe an area: it classifies a position in relation to integrated Europe, thereby turning geography into a hierarchised space and creating an asymmetrical relationship that can be exploited by hostile states seeking to destabilise and compromise the democratic order of the Western Balkans and, indirectly, render the European Union more vulnerable. This is all the more significant given that the region should be located within a much broader strategic space - understood as a system of cross-Mediterranean phenomenological interconnections - which I refer to as "EUBalkaMENA", spanning the EU, the WBs and the Middle East and North Africa (MENA).

The concept of the WBs is useful at the diplomatic and administrative levels because it makes it possible to organise partnerships, reforms, conditionalities and regional priorities. Yet its institutional effectiveness coincides with a symbolic fragility. The category is hierarchical, because it separates a Europe that is "already complete" from a Europe that is "still waiting"; it is stigmatising, because it carries with it stereotypes of instability, corruption, fragmentation and conflict; and it is homogenising, because it flattens countries with very different histories, political systems and geopolitical trajectories into a single frame (EPRS, 2023; SEENPM/Our Media, 2025).

The EU is the actor that has most thoroughly institutionalised the term in technical and normative terms. The United States has used it primarily in a security and sanctions-related register, linking the region to corruption, post-war fragility, Euro-Atlantic security and the containment of hostile influence. Russia, by contrast, employs the category ambivalently: on the one hand, it uses it in ordinary diplomatic language; on the other, it delegitimises it as the lexicon of Euro-Atlantic expansion, increasingly pairing it with the vocabulary of multipolarity, the *Global South*, the *Global East* and the *global majority* (*EEAS, 2025; EPRS, 2023)*.

This semantic ambiguity is crucial to understanding FIMI. More precisely, the narrative weaponisation of the Western Balkans can be broken down into six analytical levels, each of which acts as a device for the selection of meaning, symbolic hierarchisation and predisposition to information manipulation:

- Geographical ambiguity: the region is presented as a frontier space rather than as a fully stabilised part of Europe, which makes it easier to portray it as an area that is intrinsically incomplete, reversible or open to contestation.
- Exclusion effect: the label signals a condition of proximity without full belonging, producing a sense of political suspension that can be narratively translated into frustration, resentment and distrust towards the Euro-Atlantic project.

- Semantic stigma: the term evokes sedimented discursive repertoires - crisis, corruption, violence, backwardness, instability - that lower the threshold of credibility for hostile narratives and confirm pre-existing stereotypes.
- Homogenisation: the compression of distinct national trajectories into a single regional category reduces the complexity of local contexts and makes it easier to apply the same polemical or conspiratorial frames serially.
- Securitising use of the region: when the Western Balkans are interpreted primarily as a security problem, public attention shifts from social plurality to risks of destabilisation, thereby favouring emergency-driven, exceptionalist and polarising narratives.
- Opportunistic elasticity of the category: the formula is sufficiently flexible to be filled, depending on the context, with different meanings - enlargement, containment, influence, crisis, transition - and it is precisely this elasticity that makes it particularly suitable for strategic manipulation.

2. Digitalisation and the Regional Information Environment

2.1 A Highly Connected Ecosystem with Uneven Resilience

Overall, the Western Balkans today constitute a highly connected region: the most recent comparative data available place internet penetration between approximately 86.7 % in Bosnia and Herzegovina and 92.0 % in North Macedonia, with Serbia, Kosovo, Montenegro and Albania all close to or above 88 %. Social media use is also widespread, albeit with the necessary caution regarding social media identities, which do not always correspond to unique individuals (DataReportal, 2025).

Yet the decisive variable is no longer access, but the quality of the information ecosystem. Regional syntheses reveal a convergent pattern: trust in the media is generally declining; the use of social platforms as sources of news is increasing; television remains central but is no longer monopolistic; media capture persists; media literacy is low or unevenly distributed; younger users increasingly treat platforms as information sources; and ethical violations in the digital sphere recur with considerable frequency.

The media diet of the Western Balkans is therefore structurally hybrid. Television continues to occupy a strong position, especially among adult and senior audiences. Facebook remains important as a space for mass dissemination and the normalisation of frames. Instagram and TikTok are increasingly relevant for news discovery among young people and young adults. YouTube functions as a space for narrative serialisation and audiovisual memory. Messaging apps and Telegram work as environments of acceleration, community-building and relay. In this setting, content circulates along multiple trajectories: from the local portal to the television news bulletin, from the Telegram channel to the pseudo-news site, and from the television talk show to the clip on Facebook or X.

Rather than a simple inventory of dominant platforms, this distribution should be read as a pattern of functional differentiation across digital affordances. In media-studies terms, the Western Balkans take shape as a hybrid media system in which news discovery, social interaction, algorithmic recommendation and intermedial reuse operate in an interconnected manner: in Albania, a more visual and mobile-centred combination predominates, driven by TikTok, Facebook and Instagram; in Bosnia and Herzegovina, the centrality of Facebook, Instagram and YouTube points to greater integration between social networking, video clips and the recirculation of journalistic content; in Kosovo, the combined weight of Facebook, Instagram and TikTok reflects a younger information diet oriented towards rapid circulation; in Montenegro, Facebook, Instagram and X indicate a smaller environment but one with high politico-discursive density; in North Macedonia, the role of Facebook, Instagram and Linke-

dIn, alongside TikTok and Telegram, reveals the coexistence of general audiences, politicised micro-publics and professional communities; in Serbia, finally, Facebook, Instagram, YouTube, TikTok and messaging applications form the most extensive ecosystem and the one most capable of regional spillover. It follows that a platform's relevance depends not only on its numerical reach, but on the function it performs within the information ecology: discovery, emotional intensification, narrative archiving, coordination, laundering or mainstreaming.

2.2 Country Profiles: Connectivity, Media Diets and Vulnerabilities

Albania has approximately 2.45 million internet users, with penetration at around 88.4 %. The system remains strongly hybrid: television retains an important role among general audiences, while TikTok, Facebook and Instagram are gaining ground among younger publics. The most recurrent risks concern incomplete media literacy, market concentration, republishing/copy-paste practices across outlets, blurred boundaries between professional journalism and social content, as well as vulnerabilities linked to children's online safety.

Bosnia and Herzegovina records around 2.72 million internet users and 2.20 million social media accounts. It is one of the most vulnerable cases: regional reports place it at the bottom of the European Media Literacy Index. Trust in the media is very low, at around 15 %, and online media have now achieved almost the same reach as television. Facebook remains the dominant platform, followed by Instagram and YouTube. This is compounded by deep political-ethnic fragmentation, the persistence of hate speech and an information environment heavily exposed to propaganda and polarisation.

Kosovo has around 1.50 million internet users and 855,000 social media accounts. Its young demographic structure has a marked effect on its information diet: television remains the most widely used source, but Facebook, Instagram and TikTok are gaining weight as spaces of news discovery and political socialisation. In terms of risk, Kosovo is one of the best documented cases concerning the vulnerability of minors: in one study of 11-16 year olds, more than 90 % remained online for between one and six hours a day, more than 90 % owned a smartphone, and YouTube and Instagram emerged as the preferred platforms; TikTok was perceived as one of the environments in which cyberbullying was most frequent. At the systemic level, Kosovo is placed in a high-vulnerability bracket for disinformation and foreign malign influence.

Montenegro records around 566,000 internet users and 445,000 social media accounts. The most relevant mainstream platforms are Facebook, Instagram and X. Here, the central issue is not only platform use, but also the link between the digital environment, media ownership and external influence. Various reports indicate Serbia's strong projection into Montenegro's media ecosystem and serious gaps in the online protection of minors. Threats against journalists are increasingly shifting into the digital realm, while media literacy has not yet been sufficiently institutionalised.

North Macedonia is the most connected country in the group, with internet penetration at around 92.0 %. The data point to a marked distrust of information quality: 71 % of respondents believe that the media provide superficial content. A significant share of the public struggles to distinguish between credible sources and manipulative campaigns. In terms of platforms, the Macedonian case is among the best mapped: Facebook, Instagram, TikTok, X and Telegram appear as vectors of coordinated campaigns, automated profiles, conspiratorial groups and echo-chamber environments.

Serbia is the quantitatively most significant case: approximately 6.13 million internet users and 4.83 million social media accounts, with very large potential adult audiences for YouTube, Instagram, Facebook and TikTok. The system nevertheless remains strongly television-centred. Television is the most widely used source of information - some segments of the population watch it for up to eight hours a day - while only around 30 % report trusting

the media and 96.7 % continue to follow television, even as 81.5 % use messaging applications. As for risk, Freedom House, the OSCE and UN/EU sources all point to a deterioration in internet freedom, intimidation campaigns against journalists and social media users, and a significant level of digital violence, especially against women and young women.

2.3 Age Clusters, Online Users and Differentiated Vulnerabilities

At least five age and exposure clusters can be identified. The first is the 11-16 age group, heavily exposed to cyberbullying, harassment, inappropriate requests, prolonged immersion in platformised environments, and the early use of smartphones, social media and online games. The second is the 15-24 cluster, which is crucial for social-first information socialisation: news discovery on Instagram, TikTok, YouTube and messaging apps, exposure to micro-videos, meme politics, influencer politics and emotionally optimised content. The third is the 25-44 segment, combining news consumption, use of messaging applications, digital labour and vulnerability to geopolitical, economic and anti-elite content. The fourth is the 45-64 group, in which television remains strong but Facebook, portals and messaging groups facilitate laundering between legacy media and the digital sphere. The fifth is the over-65 cohort, still more dependent on television, radio and hierarchical sources and therefore exposed to a specific form of vulnerability: the translation of manipulative frames into everyday information routines (Saliu et al., 2022; UNICEF Serbia, 2024/2026; UNICEF Albania, n.d.; Montenegro Media Institute, 2025; OSCE Serbia, 2023).

As regards meme culture and online gaming, the empirical base is weaker but not irrelevant. Gaming appears as a youth space characterised by high exposure and low social regulation, and it deserves attention especially in its gaming-adjacent forms - Discord, voice chats and parallel communities - although, at present, it has not yet emerged as a fully mapped vector of regional FIMI.

3. Media and Platforms Ecosystem: How FIMI Becomes Credible

In the Western Balkans, the circulation of Russian or pro-Russian narratives depends less on a single central megaphone than on an ecosystem of relays. The recurrent pathway identified is:

Russian or pro-Kremlin source → Telegram / Sputnik / RT / support sites → local portals, tabloids, television, regional politicians → further amplification on Facebook, YouTube, X and Instagram.

Within this circuit, local vectors are not ancillary; they are the very condition of manipulative effectiveness.

3.1 Legacy Media, Tabloids and Laundering

During the infodemic phase of 2018-2020, the backbone of diffusion was not composed solely of social media. A study based on 74 confirmed campaigns and approximately 32 million interactions concludes that Facebook was strongly present, but that television, newspapers and community/local media remained more important as channels of distribution. Newspapers and periodicals appeared in over 70 % of campaigns, local media in over 60 %, state media in roughly 45 % and private media in 82 %. The structural conclusion is clear: in the Western Balkans, the principal scale of disinformation is hybrid rather than purely social (European Parliament, 2021).

Within this architecture, Sputnik Srbija and RT Balkan function as hubs of localisation. Content produced or adapted in Serbian is easily republishable across the Bosnian-Croatian-Monte-

negrin-Serbian (BCMS) space, reducing the cost of cultural translation and increasing the volume of laundering. The key point is not only direct audience reach, but reuse. Russian or pro-Russian content enters the domestic media circuit through free republication, opaque attribution, reformulation and recontextualisation, all of which make the origin of the source less visible.

3.2 Telegram

In terms of social platforms, the most evident qualitative leap concerns Telegram. Monitoring conducted in 2023-2024 across Bosnia and Herzegovina, Kosovo and Serbia shows differentiated relevance by country: Kosovo records a very high volume on Telegram, Bosnia and Herzegovina likewise, whereas in Serbia Facebook remains very strong. In any case, Telegram emerges as a privileged space for nationalist, anti-NATO and pro-Kremlin content. Thirteen channels in Serbian and Russian have been identified with more than 230,000 subscribers in total, together with one channel with more than 54,000 followers linked to dozens of other channels, and another linked to Dejan Beric, a Serbian foreign fighter active in Donbas since 2014 who has become, within the Serbian-speaking space, a connective figure between pro-Russian militancy, volunteer recruitment, war testimony and heroic-identitarian narrative. In this context, his relevance lies not only in personal notoriety, but in the fact that he functions as a vector of symbolic authentication: he turns propaganda into lived experience, geopolitical cause into militant biography, and the pro-Russian frame into a moral repertoire.

Functionally speaking, Telegram is the platform best suited to intense radicalisation and pre-mobilisation: broadcast channels, groups, forwarding, inter-channel relay, fundraising, short clips, apocalyptic tones, identity alarmism, rapid mobilisation and an almost immediate move towards specific sites, YouTube or tabloids. In the Western Balkans, the most exposed targets are primarily Serbian-speaking publics in Serbia, northern Kosovo, Republika Srpska and Montenegro; the most recurrent topics are Kosovo, NATO 1999, the humiliation of Serbia, defence of Orthodox/Serbian identity, anti-EU, anti-NATO and the war in Ukraine read as a Russia-West confrontation (RAN, 2022; EUISS, 2023; ISD, 2024/2026).

3.3 Facebook

Facebook remains the principal mass channel of the cyber-social ecosystem. Its target audiences are broader than Telegram's: general publics, civic groups, local communities, diaspora networks, and adult and intergenerational clusters. Recurring themes on the platform include institutional crises, war memory, referendums, national identity, EU double standards, suspicions of a Western conspiracy and frames centred on the defence of traditional values. The platform works through pseudo-news pages, local groups, memes, emotionally charged posts, the recirculation of television clips, and hashtag or boycott campaigns; the Macedonian case of #Boycott / #Бојкотирам remains emblematic, since it shows how a hashtag can function as a device of discursive aggregation and protest, channelling economic discontent, political distrust and everyday indignation into a frame that is immediately shareable and easy to relay.

Facebook is less militant than Telegram but stronger in mainstreaming. It is important to highlight that mainstreaming means the process through which frames that are initially marginal, sectoral or radicalised are progressively normalised, that is, brought back within communicative forms perceived as ordinary, familiar and socially legitimate. Facebook has the capacity to turn protest into dense social networks, to lower the costs of engagement and to render organic what begins as a campaign. The risk of radicalisation is therefore medium-high, but above all cumulative: mobilisation grows when social or territorial networks already exist that can convert indignation into offline but "connective" participation.

3.4 YouTube

YouTube matters less for rapid coordination than for narrative depth, perceived authority, political memory and the serialisation of frames, as shown by monitoring conducted on more than 70 hours of content from 13 channels with over 2.9 million followers in total. This makes the platform particularly effective for Kosovo, 1999, NATO, Serbian historical victimhood, the idea of Russia as a natural ally, the decadence of the West and European betrayal.

The risk of radicalisation on YouTube is medium-high, but it occurs primarily through reiteration and long-form narrative. Weaponisation operates through clip extraction, the circulation of talk shows, the reuse of television programmes and intersection with legacy media. More precisely, YouTube weaponises narrative when it allows a complex political story to be broken down into short audiovisual units, easy to recontextualise and highly reusable, which can then be recirculated on other platforms as proof, confession, debunking or memorial artefacts. The text also recalls the role of Happy TV and of other channels that re-propose political and commemorative content to an already predisposed audience. In this sense, YouTube is not the platform that mobilises most rapidly, but the one that constructs the interpretive horizon within which future mobilisation becomes legitimate, morally justifiable and narratively coherent.

3.5 X

X has more limited mass penetration, but considerable weight in agenda-setting among elites, journalists, politicians, activists and diasporas. It is used to launch hashtags, turn anniversaries or incidents into political frames, provide material to journalists and accelerate the visibility of the most divisive framings in the first hours of a crisis. Its impact is less community-driven than Telegram's and less sedimentary than Facebook's, but very strong in terms of frame-setting speed and intermedial chains of relay.[3]

3.6 Automated Sites, Pseudo-News and Laundering Networks

Another central component of the scenario mapped here is the emergence of automated sites and content-laundering networks. From a FIMI perspective, this is one of the most efficient infrastructures. The RFE/RL investigation into the "Pravda / Portal Kombat" network documents that, between March and July 2024, four sites in Serbian, Bosnian, Macedonian and Albanian published more than 70,000 articles, with more than 67,000 items on the Serbian site alone. The passage from Telegram to the sites took place within 3 to 12 minutes, using tools such as VK Video and Yandex for translation, production and distribution (Viginum, 2024; RFE/RL, 2024; EEAS, 2025).

These sites have a lower capacity for direct radicalisation than Telegram, but a very high weaponisation potential: they offer persistence, indexability, volume, false pluralism of sources, deniability and SEO. They are ideal for turning content born on a propagandistic channel into an "article" that other portals, pages and commentators can subsequently cite as ordinary information.

[3] IKS (2025), cit.

Table 1. Platforms, Functions and FIMI Utility

PLATFORM	INFRASTRUCTURE / LOGIC	RADICALISATION	WEAPONISATION	MOBILISATION	FIMI UTILITY
Telegram	Channels, groups, forwarding, cross-platform relay	High: dense communities, antagonistic identities, emotional escalation	High: coordination, fundraising, initial laundering, network continuity	Medium-high: preparation and coordination more than mass outreach	Very high
Facebook	Pages, groups, local communities, diaspora	Medium: sedimentation rather than shock	Medium-high: social targeting and normalisation	High: logistical coordination and frame dissemination	High
YouTube	Talk shows, clips, seriality, audiovisual memory	Medium-high: narrative depth and perceived authority	Medium: reuse, clip extraction, long duration	Medium: legitimises and prepares more than it coordinates	Medium-high
X / Twitter	Agenda-setting, hashtags, elites, journalists	Medium: discursive hardening among politicised publics	High for rapid frames and crises	Medium: strong among elites, lower among the wider public	Medium
Automated sites / pseudo-news	Translation, duplication, indexing, laundering	Low-medium direct effect	Very high: volume, persistence, deniability	Low direct, high indirect	Very high
TV / tabloids / mainstream portals	Mass reach, apparent reputation, domestic relay	Medium-high: construction of common sense	High: domestication and legitimisation	Medium-high: enables political effects and protests	Very high

4. FIMI, Radicalisation and State/Platform Analysis

4.1 Regional Overview and Operational Model

The combination most functional to FIMI in the Western Balkans is the one that links Telegram with automated sites/portals, then with local media/tabloids/television, and finally with localisation hubs such as Sputnik/RT, with Facebook and YouTube playing a complementary role of normalisation and narrative depth, and X functioning as a crisis accelerator. This architecture generates three distinct but interdependent processes:

X. **Radicalisation**: a process of cognitive-affective hardening through which the user rereads complex events within antagonistic, identitarian or conspiratorial frames that become increasingly simplified and morally polarised.

Y. **Weaponisation**: the transformation of platform affordances, media formats and relay vectors into operational instruments of influence, pressure, symbolic intimidation or coordination - that is, into means capable of producing effects beyond the mere circulation of a message.

7. **Mobilisation**: the passage from the reception and sharing of frames to the willingness to act - online or offline - through protest, adherence, fundraising, recruitment, social pressure or participation in repertoires of conflict.

It follows that the most intense radicalisation tends to develop in highly identitarian niches, the most efficient weaponisation passes through hybrid infrastructures, and the most effective mobilisation arises when divisive content is domesticated and translated into local political conflict.

One may therefore identify a **seven-stage operational model**:

1. Vulnerability reconnaissance: the prior identification of grievances, identity cleavages, traumatic memories, demographic segments and political windows susceptible to narrative activation.

2. Narrative packaging: the translation of those vulnerabilities into simple frames, emotionally marked, culturally recognisable and easily adaptable to different platform environments.

3. Initial seeding: the insertion of content into low-moderation or highly ideological channels, where the message can acquire intensity, coherence and the first signs of traction.

4. Laundering and domestication: the uptake of content by portals, commentators, local media or political actors who soften its external origin and recode it as an internal, plausible and shareable issue.

5. Cross-platform amplification: the synchronous or sequential circulation of the frame across different platforms, each of which strengthens a specific component - speed, emotion, memory, legitimisation, visibility or coordination.

6. Conversion into effects: the transformation of narrative exposure into measurable effects in terms of perception, agenda, political behaviour or offline mobilisation.

7. Adaptation and persistence: the continuous recalibration of content, targets and vectors on the basis of reactions within the information environment, so as to prolong the useful life of the campaign and preserve its capacity for reactivation.

This sequence helps explain why the label "Russian disinformation" is often inadequate: the problem lies not only in the origin of the message, but in its capacity to find proxies, relays and internal vulnerabilities.

4.2 Serbia

Serbia is the most significant case. Here, the pro-Russia vector is not normally anti-government; on the contrary, it often reinforces the existing power configuration by delegitimising the opposition, protests and civil society as instruments of alleged Western colour revolutions. RT Balkan and Sputnik Serbia operate without hindrance as generators and adaptors of narratives. Pro-government mainstream media regularly pick up their content. Laundering through tabloids and domestic broadcasters transforms external informational pressure into internal common sense (European Western Balkans, 2024; RSF, 2024; Reuters, 2022).

At the media level, Serbia is also the quantitative core of the regional ecosystem: large audiences for YouTube, Instagram, Facebook and TikTok, an extremely strong centrality of television, extensive use of messaging applications, and a transborder Serbian-speaking space that enables spillover into Bosnia and Herzegovina, Montenegro and Kosovo. In terms of integrated online-offline mobilisation, the openly pro-Russian demonstrations held in Belgrade in March 2022 should also be recalled as a sign of the symbolic and political depth of the pro-Kremlin ecosystem.

4.3 Bosnia and Herzegovina / Republika Srpska

In Bosnia and Herzegovina, the clearest pattern concerns the convergence between the pro-Kremlin ecosystem, Republika Srpska, and the secessionist/anti-state agenda promoted by Milorad Dodik, the principal political leader of Republika Srpska and an actor who has for years used institutional conflict with Sarajevo to consolidate domestic support and redefine the margins of autonomy of the Serb entity. In this context, FIMI intersects with historical revisionism, war memory, Serbian identity, the delegitimation of the Dayton settlement and Russian diplomatic protection: Moscow acts not merely as an external narrative source, but as a multiplier of legitimacy for local positions that contest the durability of the Bosnian state and present Western involvement as a hostile imposition. The function of the pro-Kremlin ecosystem, therefore, is not merely propagandistic, but connective, linking Russia's geopolitical agenda, local political entrepreneurship and the normalisation of secessionist discourse.

The combination of institutional fragmentation, informational vulnerability and continuity with the Serbian-speaking media space makes Bosnia and Herzegovina, and Republika Srpska in particular, one of the clearest points of contact between foreign influence and domestic destabilisation.

4.4 Kosovo

Kosovo is the theatre in which the online-offline combination of territorial destabilisation and information warfare is most visible. The crises in the north, and especially the Banjska attack of September 2023, showed how a security episode can generate peaks of disinformative engagement, visual manipulation, conspiracy theories, anti-Western blame shifting, and frames of fear and Serbian victimhood (Democracy Plus, 2024; QKSS, 2024; Reuters, 2024).

At the digital level, Kosovo is particularly exposed because it combines a youth environment deeply socialised on platforms, an expanding media ecosystem, high vulnerability to disinformation and the strong symbolic value of the territorial question. Telegram, Facebook, Serbian-language portals and cross-border relay play a crucial role here in the rapid transformation of crisis into a multilayered narrative war.

4.5 Montenegro

Montenegro represents the case in which the hybrid-threat dimension appears most visible in the strict sense. The cyber shock of 2022 showed how vulnerable a small, highly exposed NATO state can be to hybrid pressure, even in the presence of controversial public attributions. On the informational plane, Montenegro is also one of the countries in which there is strong Russian digital diplomacy activity, anti-NATO narrative, frames of lost sovereignty, and the political use of Serbian and Orthodox identity (Reuters, 2022; SEENPM/Our Media, 2025).

Here FIMI prospers in a context in which media ownership, external influence, identity polarisation and digital vulnerabilities overlap in particularly tight ways.

4.6 North Macedonia

North Macedonia is the most useful case for understanding the use of identity disputes as a FIMI vector. Following the Greek blockage of the country's NATO trajectory, the 2018 name referendum, the Prespa Agreement and the subsequent Bulgarian veto on the European path provided Moscow and pro-Russian ecosystems with ideal narrative material: national betrayal, humiliation, loss of identity, Western imposition and the erosion of traditional values.

Coordinated campaigns have been observed on Facebook, Instagram, TikTok, X and Telegram, together with the use of automated profiles, conspiratorial Facebook groups, Telegram as an echo chamber, and the radicalisation of anti-gender, anti-establishment and anti-Western themes. In this sense, North Macedonia may constitute a laboratory of hybridisation between local grievances and Russian narratives.

4.7 Albania

Albania is the country in which the evidence of direct Russian operations appears weaker. This does not mean the absence of risk. The research cited in the text nonetheless shows the circulation of narratives hostile to NATO and the EU, the local relaying of Russian or Serbian statements, and a prevailing model of indirect penetration based on narrative importation, media echo and laundering through local media or regional proxies (BIRN Albania, 2024; NDI Albania, 2025).

The country's comparatively stronger Euro-Atlantic anchoring limits the structural depth of such penetration, but it does not eliminate the possibility of informational contamination and tactical convergence between anti-Western frames and domestic polarisation.

Table 2. Comparative State/Platform Matrix

COUNTRY / AREA	MAIN OPERATION / CAMPAIGN	PRINCIPAL VECTORS	TARGET / EFFECT	ONLINE / OFFLINE	ATTR.	WHY IT MATTERS
REGIONAL	Portal Kombat / 'Pravda' network in several Balkan languages	clone sites, automation, relay from pro-Russian sources, Telegram, RT	information saturation, content laundering, penetration in Serbia and spillover into BiH, Albania and North Macedonia	online	A/B	Strongest case of a transnational infrastructure attributable to a pro-Russian ecosystem
Serbia	RT Balkan / Sputnik Srbija + laundering through pro-government media	portals, television, tabloids, social media	delegitimation of protests, the opposition and civil society; anti-EU / anti-NATO framing	online + broadcast + offline	B	Main hub of the Serbian-speaking space and of narrative domestication
Bosnia and Herzegovina / RS	Informational and political support for Dodik / secessionist narrative	Serbian-speaking media, Russian statements, RS ecosystem	erosion of Bosnian statehood, ethnic polarisation, delegitimation of the West	online + institutional + offline	B	Point of convergence between local agenda and Russian projection
Kosovo	Informational escalation around the northern crises and Banjska	Serbian / pro-Serbian portals, social media, cross-border disinformation	intensification of fear, delegitimation of Kosovo, KFOR and the West	coordinated online + offline	B/C	Clearest theatre of convergence between events on the ground and information warfare
Montenegro	Cyber shock of 2022 + FIMI pressure	cyber-attacks, Russian diplomatic Facebook activity, external information ecosystem	pressure on a NATO state, institutional distrust, geopolitical polarisation	online, with systemic offline effects	C	Shows the intertwining of hybrid pressure and informational vulnerability
North Macedonia	Anti-NATO / anti-EU / 'traditional values' FIMI	Facebook, Instagram, TikTok, X, Telegram, weakly regulated sites	polarisation, distrust, identitarian and moral anxieties	predominantly online	B/C	Paradigmatic case of the exploitation of identity disputes
Albania	Indirect penetration / laundering of anti-NATO and anti-EU narratives	local media, decontextualised relays, regional proxies	pollution of public debate, spread of anti-Western frames	online	C	Shallower structural penetration, but not an absence of risk

Table 3. Timeline of the Main FIMI Opportunity Windows

PERIOD / EVENT	NARRATIVES	OBJECTIVES	VULNERABILITIES EXPLOITED	PLATFORMS / VECTORS
2020-2021 | COVID-19 pandemic	virus created/ hidden, Big Pharma, EU failure, Sputnik V as proof of Russian effectiveness	erode trust in Western institutions; increase Russian prestige	low health literacy, distrust of elites	Facebook, messaging apps, portals, television; Serbia as vaccine diplomacy hub
Feb-Dec 2022 | Russian invasion of Ukraine	NATO responsible, Russia defensive, hypocritical West, double standards	realign public opinion; reduce support for sanctions; fuse Ukraine with Kosovo	grievances linked to 1999, anti-Westernism, transborder Serbian-speaking space	RT Balkan, Sputnik Srbija, tabloids, television, YouTube, Telegram
2023 | protests and polarisation in Serbia	colour revolution, NGOs and media as external agents	delegitimise the opposition and civil society; preserve the existing power structure	distrust in pluralism, heavy TV + portals + Facebook consumption	RT Balkan, Sputnik, pro-government media, Facebook, YouTube
2023 | northern Kosovo crises	Serbs under siege, Kosovo illegitimate, West complicit	mobilise Serbia-centred solidarity; undermine trust in KFOR/EU/US	territorial fractures, fear, high symbolic value of Kosovo	Serbian-speaking portals, Telegram, Facebook, television
2023-2024 | Banjska and post-Banjska	attack reframed as self-defence or conspiracy, anti-Western blame shifting	confuse responsibility; turn a security crisis into a narrative war	polarised environment; weak control over portals	social media, portals, Telegram, cross-posting and media laundering
2024 | Portal Kombat / Pravda	flooding of localised pro-Russian content	saturate the ecosystem, shape search and recommendation	dependence on search/social, republishing, weak verification	multilingual site networks, SEO, automation, Telegram as source
2024-2025 | Bosnia/RS and Dodik	conviction framed as political persecution, RS under threat, West anti-Serb	legitimise soft secessionism and the erosion of the Bosnian state	institutional fragmentation, war memory, identity politics	Serbian-speaking media, political statements, portals, television, social media
2024-2026 | AI + automation convergence	multiplication of pre-existing narratives and hyper-localisation	scale FIMI volume, speed and personalisation	cognitive saturation, low algorithmic transparency	site networks, social media, AI tools, synthetic/hybrid content

5. CONCLUSIONS

The analysis confirms that the Western Balkans are not an informational periphery, but a European space in which high connectivity, fragile institutions, conflictual memory, small media markets and geopolitical competition produce an especially intense vulnerability. The Russian threat thrives not because everything is remotely directed from Moscow, but because the region offers numerous points of entry and operational anchoring: historical grievances, transborder linguistic spaces, low transparency in the online sector, incomplete literacy, distrust of the media, and local actors willing to relay external narratives for internal purposes (EEAS, 2025; SEENPM/Our Media, 2025; ISD, 2024/2026).

For this reason, the formula "Russian disinformation" is inadequate. The real problem is an ecosystem in which:

a) Telegram tends to favour radicalisation and the preparation of mobilisation.
b) Automated sites and pseudo-news maximise volume, persistence and deniability.
c) Facebook and YouTube normalise.
d) Television, tabloids and mainstream portals legitimise.
e) Domestic actors translate the whole into internal political conflict.

FIMI, therefore, is not merely content, but architecture, a socio-cognitive infrastructure, a local translation of geopolitical pressure, and a mode of emotional cultivation.

5.1 Future Trajectories: MUAI and High-Risk Criminal Networks

The most likely evolutionary vector of the threat is the convergence between FIMI, AI-based automation and the Malicious Use of AI (MUAI) (Antinori, 2025). Recent European analyses indicate that the use of AI in FIMI is reducing the costs of scale while increasing personalisation, translation, audio-video synthesis, brand imitation and multimodal manipulation. In the context of the Western Balkans, this implies at least five potential developments:

I. More credible synthetic content in local languages: increasingly accessible generative models make it possible to produce texts, voice-overs, subtitles and visual assets that imitate local linguistic registers at lower cost and with fewer signs of artificiality.

II. The multiplication of pseudo-outlets and cloned sites: automation makes it possible rapidly to populate domains and portals with large volumes of para-journalistic content, thereby increasing frame persistence and the false pluralism of sources.

III. Micro-adaptation of messages to specific communities: the same narrative nuclei can be inflected for different targets - young people, seniors, diasporas, religious communities, Serbian-speaking or Albanian-speaking publics - without losing strategic coherence.

IV. Emotionally high-activation audio and video deepfakes: synthetic content simulating statements, incidents or visual evidence can reactivate trauma, fear, indignation and feelings of siege with a persuasive force greater than that of written text.

V. Very rapid multi-platform saturation: the combination of automated generation, translation, scheduling and continuous testing makes it possible to inject many variants of the same frame and to measure their cognitive and emotional performance almost in real time.

The leap would therefore be not only quantitative – "more propaganda" - but qualitative: an adaptive industrialisation of manipulation. By this expression I mean a model in which the production, localisation, distribution and optimisation of content no longer occur in episodic or artisanal technique, but as an iterative process grounded in automation, modularity and continuous feedback. In the case of the Western Balkans, this means that already existing fractures - Kosovo, Dodik/Republika Srpska, identity disputes in North Macedonia, Montenegrin sovereignty, the memory of 1999, Serbian-speaking anti-Westernism - can be treated as available cultural repertoires, that is, as archives of symbols, traumas, lexicons and antagonisms to which differentiated versions of the same frame can be applied. AI does not replace the previous ecosystem: it makes it cheaper, faster, more translatable and more difficult to attribute, above all because it allows the tone, format and emotional intensity of the message to be adapted almost continuously to audience reactions.

A second, even more insidious development concerns the potential exploitation of regional High-Risk Criminal Networks (HRCNs) as FIMI proxies and/or service providers. Europol stresses that criminal networks can operate as proxies for hybrid actors in the cyber-social ecosystem, while further studies describe Russophone criminal networks as facilitators of continental hybrid threats, especially in cybercrime, money laundering and opaque support services (Europol, 2025; CEPOL, 2025; European Parliament, 2026).

In a context such as the Balkans, HRCNs may offer FIMI not so much ideology as enabling capacities: laundering financial flows towards media or pseudo-media ecosystems; shielding shell companies; procuring digital infrastructures, SIM farms, hosting and synthetic identities; informal intimidation of journalists, page administrators and/or local actors; connections between criminal markets, ultras, violent subcultures and online communities; and the use of crypto and cash-based circuits to finance operations with low attributable visibility. In this scenario, organised crime does not replace the information operator; rather, it becomes its logistical and financial hinterland.[4]

The future hybrid threat, therefore, may not present itself as a campaign immediately recognisable as "Russian", but rather as a chain of opaque services: synthetic content, multi-platform laundering, local relays, shielded financing, selective intimidation, and the use of marginal actors endowed with a capital of violence and access to transborder grey economies. Prevention will therefore have to shift from the single piece of content to the infrastructure, from the evident falsehood to the synthetic flow, and from the visible media outlet to the circuit of proxies that makes FIMI sustainable over time.

It is worth recalling that information warfare does not begin where the first false item appears. It begins much earlier, when a society loses the capacity to distinguish between conflict and the representation of conflict. In the Western Balkans, vulnerability is not an accident but a structure, the product of wounded memories, weak media markets, insecure political identities and porous narrative boundaries. This is why FIMI works: it does not invent a void, it organises what already exists. It does not create hostility from nothing; it gives it form, rhythm, lexicon and a target. AI will make this dynamic faster, cheaper and more ubiquitous. Criminal networks may render it more opaque, more resilient and better protected. The real problem, then, will not be simply recognising the lie. It will be understanding who carries it, who finances it, who makes it socially credible and emotionally resonant, and who, in the end, converts it into an architecture of power.

[4] Arije Antinori (2026) High-Risk Criminal Networks (HRCNs) as a Proxy Actor in Foreign Information Manipulation and Interference (FIMI): a Hybrid Threat to Public and National Security in Special Conference Edition of the European Law Enforcement Research Bulletin.

REFERENCES

1. Arije Antinori (2025) Malicious Use of Artificial Intelligence (MUAI): l'uso malevolo dell'intelligenza artificiale nell'ecosistema cyber-sociale *in* Sicurezza e scienze sociali XIII, 2/2025.
2. Arije Antinori (2026) High-Risk Criminal Networks (HRCNs) as a Proxy Actor in Foreign Information Manipulation and Interference (FIMI): a Hybrid Threat to Public and National Security *in* Special Conference Edition of the European Law Enforcement Research Bulletin.
3. BIRN Albania (2024) The Distribution of Disinformation Narratives by Hostile Actors against NATO and the EU in the Albanian Media.
4. Carnegie Europe (2021) Vaccine Geopolitics and the EU's Ailing Credibility in the Western Balkans.
5. CEPOL (2025) Western Balkans Tackle High-Risk Criminal Networks through Advanced Training in The Hague.
6. Clingendael (2023) Little Substance, Considerable Impact: Russian Sources of Influence in Serbia, Montenegro, and Bosnia and Herzegovina.
7. Council of Europe / European Audiovisual Observatory (2025) Resilience to Foreign Information Manipulation and Interference (FIMI) in Eastern Europe and the Western Balkans.
8. DataReportal (2025) Digital 2025 / 2026: Albania; Bosnia and Herzegovina; Kosovo; Montenegro; North Macedonia; Serbia.
9. Democracy Plus (2024) Vulnerability Index of Disinformation in Kosovo.
10. EEAS (2025) 2024 Report on EEAS Activities to Counter FIMI.
11. EEAS (2025) 3rd EEAS Report on Foreign Information Manipulation and Interference Threats.
12. EEAS (2026) 4th EEAS Report on Foreign Information Manipulation and Interference Threats.
13. EPRS (2023) Russia's Influence in the Western Balkans.
14. EPRS (2025) Information Manipulation in the Age of Generative Artificial Intelligence.
15. Europol (2025) EU-SOCTA 2025 - Executive Summary.
16. European Parliament (2021) Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them.
17. European Parliament (2026) Addressing the Nature and Impact of Organised Crime on the International Scene.
18. European Western Balkans (2024) Russian State Media in Serbia Support the Government with Anti-Western Narratives.
19. IKS - Institute of Communication Studies (2025) Russian FIMI in North Macedonia: Exploiting Vulnerabilities Through Bilateral Disputes.
20. ISD (2024/2026) Monitoring Influence & Disinformation Campaigns in the Western Balkans (MEDIWEB).
21. Keegan, K. (2022) Clarity for Friends, Confusion for Foes: Russian Vaccine Propaganda in Ukraine and Serbia.
22. Montenegro Media Institute (2025) Strengthening Online Protection for Minors in Montenegro.

23. NDI Albania (2025) The Vulnerability of Albanian Politics to Foreign Interference.
24. OSCE Serbia (2023; 2026) Media Users over the Age of 65 in Serbia; Media Literacy of Serbia's Citizens.
25. QKSS (2024) Kosovo in Russian Foreign Policy Discourse.
26. RAN (2022) Online Radicalisation and P/CVE Approaches in the Western Balkans.
27. RCC (2018) A New Virtual Battlefield: How to Prevent Online Radicalisation in the Cyber Security Realm of the Western Balkans.
28. Reuters (2022-2025) regional dispatches on Serbia, Bosnia and Herzegovina, Kosovo and Montenegro.
29. RSF (2024) From Russia to Serbia: How RT Spreads the Kremlin's Propaganda in the Balkans despite EU Sanctions.
30. RUSI (2025) Russia, AI and the Future of Disinformation Warfare.
31. SEENPM / Our Media (2025) Regional Overview and Country Reports for the Western Balkans.
32. Viginum (2024) Portal Kombat: A Structured and Coordinated Pro-Russian Propaganda Network.

AMBIENT RADICALISATION: HOW FIMI EXPLOITS POLARISATION

Jordy Nijenhuis

1. Introduction

Foreign Information Manipulation and Interference (FIMI) has become a concerning feature of today's information environment. It is increasingly recognised as a strategic tool used to distort public debate, exploit societal fault lines, and weaken democratic resilience (European External Action Service [EEAS], 2025; EEAS, 2026). At the same time, this evolving landscape challenges how we understand related phenomena such as radicalisation.

Traditionally, online harms such as disinformation, hate speech, and radicalisation have often been approached as separate issues, each with their own policy frameworks, institutional responses, and research traditions. In discussions around radicalisation in particular, one of the dominant frames has long been one of ideology, recruitment, and violence; individuals were understood to be drawn into extremist movements through exposure to coherent ideological narratives, social networks, and deliberate mobilisation toward violent or anti-democratic action.

That model still matters. But it is no longer enough.

Today's information environment is more fragmented, more emotional, and more opportunistic. Rather than trying to convince people through coherent ideological narratives alone, FIMI often works by exploiting what is already there: tensions, frustrations, grievances, uncertainty, and divisions within societies. It does not necessarily need to recruit people into a clear movement. Often, it simply needs to deepen distrust, amplify polarisation, and make more extreme interpretations of reality feel normal and justified.

Across Europe, there is growing evidence that foreign and domestic actors use coordinated information campaigns to intensify polarisation, undermine trust in institutions, and destabilise democratic processes (EEAS, 2025; ISD, 2024). In practice, this means that FIMI rarely operates in isolation. It interacts with domestic disinformation, conspiracy narratives, hate speech, identity-based hostility, and broader forms of online radicalisation. These harms do not sit neatly apart. They overlap, reinforce one another, and can all be weaponised.

This has important implications for how we understand and respond to these challenges. If disinformation fuels polarisation and vice versa, if this polarisation in turn creates openings for hate speech, and if those dynamics in turn make people more susceptible to radical narratives, then treating these issues as separate policy silos is no longer sufficient. Rather than addressing disinformation, hate speech, and radicalisation as if they exist on separate islands, we need a more holistic approach that takes seriously how these phenomena interact within the same information ecosystem.

It is in this context that this paper introduces the concept of ambient radicalisation. The term helps capture a shift away from older models centred primarily on explicit recruitment and ideological conversion towards violence. Instead, it draws attention to a more diffuse process in which people are gradually pushed toward more extreme positions through repeated exposure to polarising, manipulative, and emotionally charged content, which in turn can accelerate radicalisation when a crisis or triggering incident occurs. In this model, the target is not just a narrow at-risk group. The target is society itself.

1.1 Methodological note

This paper takes a conceptual and illustrative approach. It draws on existing research, institutional reports, and selected case studies from Europe and the Western Balkans to explore how FIMI interacts with broader information dynamics. The cases were chosen to reflect different pathways through which polarisation, disinformation, and online environments intersect with radicalisation processes, rather than to establish direct causal relationships.

2. From Ideological Recruitment to Ambient Radicalisation

Prevailing models of radicalisation have focused on how people are drawn into extremist ideologies through recruitment and social networks. Individuals were thought to move along relatively identifiable pathways: exposure to extremist ideas, contact with like-minded networks or recruiters, and gradual adoption of more rigid and often violent worldviews. This model has shaped much of the policy, research, and prevention work in the field (Neumann, 2013; Horgan, 2008). In the context of groups such as Daesh (ISIS) or organised far-right movements, these dynamics were visible. Radicalisation was often intentional, structured, and directional. There was a message, a messenger, and a movement (Wiktorowicz, 2005; EU Radicalisation Awareness Network, 2019). But this model also assumes that radicalisation requires alignment, that people need to be convinced of a coherent ideology before they move toward more extreme positions.

That assumption is increasingly incomplete.

In today's information environment, radicalisation does not always begin with ideology. It often begins with emotion. Frustration about politics, distrust in institutions, anxiety about identity or economic security, or a sense of injustice or exclusion.

FIMI operates precisely at this level.

Research on disinformation ecosystems has consistently shown that emotionally charged content is more likely to be engaged with, shared, and internalised (Vosoughi et al., 2018; Brady et al., 2017). Rather than building ideological coherence, it exploits emotions. Rather than recruiting individuals into clearly defined movements, it exposes large and diverse audiences to content that amplifies grievances, simplifies complexity, and sharpens divisions. Over time, this repeated exposure can shift perceptions of reality: what feels credible, what feels acceptable, and what feels justified. This aligns with findings from the EEAS that FIMI campaigns systematically exploit "existing societal vulnerabilities" and amplify polarisation rather than create entirely new narratives (EEAS, 2025).

This is what we could describe as "ambient radicalisation".

Ambient radicalisation is not driven by a single actor, ideology, or pathway. It is diffuse, cumulative, and often difficult to detect. It unfolds across platforms, across topics, and across communities. Individuals are not necessarily "pulled into" extremism; they are gradually pushed outward, away from nuance, toward more absolute and polarised positions. Research into online radicalisation pathways increasingly highlights these non-linear, decentralised processes (ISD Global, 2023; Moonshot, 2022).

Importantly, this process does not require a clear endpoint. People may not identify with extremist labels or organisations. Yet their trust in democratic institutions may erode, their tolerance for opposing views may decrease, their openness to conspiratorial or exclusionary narratives may increase, and, in some cases, they may come to see violence as a legitimate response. Studies on conspiracy belief systems show how such narratives can act as "gate-

way frames" that normalise more extreme positions over time (Douglas et al., 2019). In this sense, the line between mainstream and fringe also becomes increasingly blurred.

This shift also helps explain why polarisation has become such a central feature of the current information landscape. Polarisation is not just a by-product of disagreement. It is a condition that can be actively amplified and strategically exploited. Research in the Western Balkans shows that foreign information manipulation often reinforces existing identity-based and political divisions, making compromise more difficult and increasing social fragmentation (ISD Global, 2024; Council of Europe, 2025).

It is important to distinguish between FIMI and radicalisation. FIMI refers to coordinated and manipulative activity in the information space by foreign actors aimed at influencing public debate and undermining democratic processes. Radicalisation, by contrast, describes a broader social and psychological process through which individuals or groups move toward more extreme positions, which may or may not involve violence. While these phenomena can intersect, they are not interchangeable. FIMI can contribute to the conditions in which radicalisation becomes more likely by amplifying polarisation, distrust, and emotionally charged narratives, but it is only one of several factors shaping these dynamics.

3. Case Studies

While polarisation is shaped by a range of factors, FIMI can amplify and exploit these dynamics in ways that intensify division and increase the risk of escalation. In some cases, these dynamics intersect with real-world violence. This does not suggest a direct or linear causal link between disinformation and violent acts. Rather, it highlights how sustained exposure to polarising and manipulative narratives can contribute to environments in which violence becomes more thinkable, justifiable, or even legitimate.

It is important to note that there is not always clear or direct evidence that specific incidents or narratives are the result of coordinated foreign information manipulation. In many cases, the dynamics described here emerge from a complex interaction between domestic actors, media environments, and online communities. However, research consistently shows that FIMI campaigns tend to exploit precisely these kinds of existing tensions and societal fault lines, amplifying domestic conflicts rather than creating them from scratch (EEAS, 2025). This makes it difficult to draw clear boundaries between foreign influence and domestic information dynamics, even when the underlying mechanisms are similar.

3.1 COVID-19 Protests and Violence Against Institutions (Europe-wide)

The COVID-19 pandemic created a highly volatile information environment across Europe, characterised by uncertainty and widespread social and economic disruption. These conditions made public health measures, vaccination campaigns, and government decision-making particularly susceptible to polarisation and manipulation.

Within this context, disinformation and conspiracy narratives were widely circulated across online platforms, often framing pandemic responses as forms of authoritarian control, elite manipulation, or coordinated deception. For example, widely shared claims portrayed COVID-19 vaccines as tools for population control or surveillance, while other narratives framed lockdown measures as evidence of "medical tyranny" or government overreach. In several countries, these claims intersected with broader anti-government and anti-system narratives, bringing together previously distinct audiences under a shared frame of institutional distrust (EEAS, 2022).

Importantly, these narratives did not operate in isolation. They interacted with existing grievances related to trust in government, economic insecurity, and perceived loss of individual freedoms. This created a convergence of audiences, where individuals with different concerns, ranging from vaccine scepticism to broader anti-establishment views, became part of overlapping and reinforcing information ecosystems.

These dynamics became particularly visible during waves of protests across several European countries, including Germany, the Netherlands, France, and Belgium. While many protests were peaceful, others escalated into confrontations with law enforcement, attacks on journalists, and acts of violence against public institutions (Reporters Without Borders, 2021; Reuters, 2021). Monitoring and reporting from this period highlighted how online narratives contributed to increased hostility toward authorities and legitimised more confrontational forms of protest. In some instances, protest messaging and mobilisation were directly shaped by online narratives that framed authorities as illegitimate or oppressive, lowering thresholds for confrontation and contributing to more aggressive forms of protest behaviour.

In this context, the role of FIMI and disinformation was not to create opposition to public health measures, but to amplify distrust, intensify emotional responses, and connect disparate grievances into a more cohesive anti-system narrative. The information environment acted as a multiplier, increasing the visibility and perceived legitimacy of more extreme positions.

While most individuals exposed to these narratives did not engage in violence, the cumulative effect contributed to a shift in what was considered acceptable behaviour in public protest contexts. Confrontation with authorities, hostility toward journalists, and, in some cases, violence against institutions became more visible and, for some groups, increasingly normalised.

This case illustrates how ambient radicalisation can unfold across broad segments of society. Rather than targeting specific individuals, sustained exposure to polarising and distrust-driven narratives contributed to an environment in which escalation became more likely, and where the boundaries between protest, confrontation, and violence became more fluid.

3.2 Kosovo–Serbia Tensions

Tensions between Serbia and Kosovo in 2023–2024 show how highly polarised information environments can intersect with real-world violence. Periods of political crisis in northern Kosovo were accompanied by escalating rhetoric, and in September 2023, an armed attack in Banjska involving heavily armed militants and resulting in multiple casualties.

Alongside developments on the ground, the information environment became highly contested. During and immediately after the Banjska incident, misleading and unverified information circulated widely across media and social platforms, including false claims, mislabelled imagery, and contradictory reporting. For instance, misleading content included the reuse of unrelated or outdated images presented as evidence from the incident, conflicting reports about casualties and perpetrators, and unverified claims about responsibility that circulated before official confirmation. These narratives contributed to confusion and heightened emotional responses in an already volatile context.

These dynamics unfolded within a broader regional context in which disinformation and foreign-aligned narratives have been documented to reinforce inter-ethnic divisions and undermine trust in institutions. Research has shown that such narratives often emphasise victimhood, threat, and illegitimacy of the opposing side, contributing to a more polarised and emotionally charged information environment (ISD Global, 2024).

Importantly, these narratives do not originate from a single source. They are shaped by a combination of domestic political communication, media dynamics, and externally amplified messaging. In such contexts, FIMI does not create the underlying conflict, but can act as a multiplier of tension, increasing the emotional intensity of events and shaping how they are interpreted by wider audiences.

During moments of crisis, the rapid spread of misleading or incomplete information can amplify fear, anger, and hostility. In the case of the Banjska incident, this contributed to an environment in which narratives of threat and confrontation gained prominence, increasing the risk that tensions escalate further.

This case reflects a key feature of ambient radicalisation in conflict-affected contexts. Rather than directly causing violence, sustained exposure to polarising and threat-based narratives contributes to an environment in which escalation becomes more likely, and where violent confrontation can more easily be framed as justified or inevitable.

3.3 Slovakia 2022 Shooting

The 2022 shooting outside an LGBTQ+ bar in Bratislava, Slovakia, is a case of how online radicalisation dynamics can intersect with real-world violence. The attacker, who killed two people and injured another, acted alone and was not formally affiliated with an extremist organisation. However, he was not radicalised in isolation. While this case is not primarily driven by FIMI, it illustrates the broader logic of ambient radicalisation, where exposure to networked online narratives, rather than coordinated foreign manipulation, contributes to shifts in perception and justification.

Investigations showed that the perpetrator had been active in online spaces where extremist, conspiratorial, and hateful narratives circulated. He produced a manifesto and was influenced by a range of ideologies, including antisemitic, anti-LGBTQ+, and conspiracy-driven narratives. These included references to the so-called "Great Replacement" theory and other framings that portray minority groups as threats to society. Analysts and researchers have noted that these narratives are not confined to isolated extremist communities, but circulate more broadly across online ecosystems, often in less explicit or more coded forms (GNET, 2022). Research on online extremist ecosystems and networked radicalisation).

Rather than following a single, linear pathway of ideological recruitment, the attacker was exposed to a wider constellation of narratives that contributed to a worldview shaped by grievance, exclusion, and perceived threat. These dynamics are not isolated. Similar narratives have been explicitly referenced in several violent attacks, including the 2019 Halle attack in Germany and the Christchurch attack in New Zealand. In these cases, perpetrators framed violence as a response to perceived existential threats linked to migration, identity, and demographic change. The idea of acting in defence of a threatened group or civilisation is a recurring feature in such attacks (Macklin, 2019; Davey & Ebner, 2019). What is important in this context is not only the presence of these narratives, but their accessibility and circulation across online spaces, where they can be encountered, adapted, and reinforced over time.

This reflects a broader shift in how radicalisation can unfold. Instead of being driven by direct recruitment or organisational ties, it can emerge from sustained exposure to an online environment in which harmful narratives are widely accessible, repeatedly encountered, and increasingly normalised. In such environments, the boundaries between mainstream discourse and extremist content can become blurred, making it easier for individuals to adopt more radical interpretations over time.

3.4 France 2023 Riots

The riots in France in June–July 2023, following the killing of 17-year-old Nahel Merzouk, illustrate how a rapidly contested information environment can accompany large-scale escalation and mobilisation. What began as protests quickly escalated into widespread unrest, with thousands of arrests, hundreds of injured officers, and significant destruction of public and private property (Reuters, 2023a; Full Fact, 2023). Alongside the events on the ground, the information space became highly contested. The unrest was accompanied by a surge in misleading and manipulated content circulating across social media platforms. Fact-checking organisations documented a wide range of false claims, including mislabelled videos, fabricated narratives, and inflammatory content designed to exaggerate the scale of violence or frame it in civilisational or ethnic terms (Full Fact, 2023). Moments of crisis become fertile ground for disinformation. Major public events, particularly those involving violence, tend to trigger spikes in misleading content that can inflame tensions and shape how events are interpreted by wider audiences (Full Fact, 2023; Reuters, 2023a).

In the case of the France riots, misleading narratives circulated both domestically and internationally, often reinforcing polarised framings of the unrest. These included claims portraying the unrest as a "civil war," narratives attributing collective blame to specific communities, and exaggerated or fabricated reports about the scale and coordination of violence. Such framings reinforced polarised interpretations of the events and contributed to a more emotionally charged and confrontational information environment (Full Fact, 2023). These narratives did not create the underlying grievances, but they contributed to an increasingly volatile information environment in which anger, fear, and hostility were amplified.

At the same time, policymakers explicitly recognised the role of the information environment in shaping the escalation. French authorities publicly raised concerns about the impact of social media and misinformation during the riots, including discussions about restricting access to platforms in moments of unrest (Reuters, 2023b). This case illustrates a key dynamic of ambient radicalisation. The violence itself was triggered by a specific incident, but the way it unfolded, and the scale at which it spread, was shaped by a highly polarised and rapidly evolving information environment. Disinformation did not directly cause the riots, but it acted as an accelerant, amplifying tensions, reinforcing hostile narratives, and contributing to conditions in which violence could escalate more quickly and more widely.

4. A Model of How FIMI Exploits Polarisation

The starting point is rarely ideology. More often, it is a pre-existing tension, grievance, or vulnerability. This can be political distrust, identity-related anxiety, fear linked to migration, frustration over economic conditions, or anger toward institutions. These are not invented by FIMI. They already exist within society, often rooted in real experiences, perceptions, or unresolved political tensions.

The first step is the identification of a fault line. Foreign and domestic actors alike monitor which issues are already emotionally charged and socially divisive. The most effective narratives are usually not entirely fabricated. They are built around existing sensitivities, because these are more likely to resonate and spread.

The second step is amplification. Once a fault line is identified, narratives are pushed that heighten its emotional intensity. This often involves framing events in terms of betrayal, threat, humiliation, injustice, or loss. Complex realities are reduced to simplified and emotionally loaded oppositions: us versus them, truth versus lies, freedom versus control, survival

versus surrender. At this stage, the goal is not necessarily to persuade people of a coherent worldview, but to make them feel that something fundamental is under attack.

The third step is normalisation through repetition and circulation. As narratives are repeated across platforms, picked up by different actors, echoed in different formats, and integrated into wider online discussions, they begin to feel less fringe and more familiar. This is a crucial point. People do not need to fully believe a narrative for it to shape their perceptions. Repetition alone can make an idea feel more plausible, more mainstream, or at least more discussable.

The fourth step is erosion of trust and moral boundaries. As people are repeatedly exposed to narratives that portray institutions as corrupt, opponents as dangerous, or compromise as betrayal, trust begins to weaken. This affects not only trust in governments or media, but also trust in democratic processes, public debate, and other social groups. At the same time, moral boundaries can begin to shift. Language becomes more hostile, exclusionary positions become easier to justify, and confrontational responses start to feel more acceptable.

The fifth step is behavioural hardening. This does not always mean violence, and in most cases it does not. But it can mean a hardening of attitudes, greater openness to dehumanising or conspiratorial narratives, increased support for anti-democratic measures, and a growing willingness to endorse repression, intimidation, or even violence as legitimate responses. Evidence since the COVID-19 pandemic suggests that these dynamics have intensified rather than diminished. Surveys across Europe show declining trust in institutions compared to pre-pandemic levels, alongside increased political and social polarisation (Eurofound, 2023; OECD, 2023). At the same time, longitudinal polling indicates that support for strong leaders who bypass democratic processes has increased in several countries over the past decade, including during and after the pandemic period (Pew Research Center, 2020; 2023). These shifts are closely linked to increased exposure to emotionally charged and conspiratorial content, which has been shown to reinforce in-group/out-group dynamics and hostility toward opposing groups (Brady et al., 2017; Douglas et al., 2019). Importantly, this process is not linear and it is not always centrally coordinated. It can move back and forth between stages, accelerate during moments of crisis, or take place gradually over time. It also does not require everyone to move in the same direction.

5. Looking Ahead

The implications of ambient radicalisation are not only analytical, but also increasingly relevant for policy and regulation. Looking ahead, the policy response is likely to become more layered, but also more contested. In the EU, the Digital Services Act (DSA) is now the main regulatory backbone for platform accountability. It applies across the EU, imposes the strictest obligations on very large online platforms and search engines, and creates tools around risk assessment, transparency, oversight, and enforcement. That matters, but it would be a mistake to assume that regulation alone will solve the problem. It can help force platforms to take systemic risks more seriously, including risks linked to illegal hate speech and disinformation, but it cannot by itself rebuild trust, reduce polarisation, or undo the cumulative effects of ambient radicalisation. In other words, the DSA can constrain some of the infrastructure through which manipulation spreads, but it is not a substitute for broader democratic resilience.

For the Western Balkans, the next few years will likely be defined by a dual challenge: closer alignment with European regulatory frameworks on the one hand, and continued exposure to fragile information environments on the other. Council of Europe and related regional work points to both growing attention to FIMI resilience and uneven preparedness for DSA-style

implementation across the region. Recent regional work has stressed that alignment with the DSA needs to be cross-sectoral and participatory, and also warned that online-harm regulation can itself be misused if it is not grounded in freedom-of-expression safeguards. That warning is especially relevant in contexts where media capture, weak oversight, and high political polarisation already complicate responses to disinformation and manipulation (Council of Europe, 2025).

A more complex question is how consistently the concept of FIMI can be applied across different geopolitical contexts. Under the EEAS framing, FIMI refers to manipulative and interfering activity in the information space by a foreign actor. However, as tensions around Europe's information governance model increase, the line between diplomatic engagement, ideological campaigning, and potential information interference may become more difficult to draw. Recent developments have also highlighted growing friction around the Digital Services Act and cross-border information policies, illustrating how contested this space is becoming.

This is likely to be one of the defining challenges ahead. The next phase of this debate will not only be about identifying individual actors, but about understanding how information environments are shaped, how narratives travel, and how they influence perceptions of legitimacy, conflict, and acceptable behaviour. If ambient radicalisation is driven in part by the conditioning of these environments, then future responses will need to focus not only on detecting manipulation, but on strengthening resilience at the societal level. That includes rebuilding trust, reducing polarisation, and creating conditions in which more extreme interpretations of reality are less likely to take hold or spread.

REFERENCES

1. AFP Fact Check. (2023). False and misleading content circulated during the unrest in France. https://factcheck.afp.com
2. Brady, W. J., Wills, J. A., Jost, J. T., Tucker, J. A., & Van Bavel, J. J. (2017). Emotion shapes the diffusion of moralized content in social networks. Proceedings of the National Academy of Sciences, 114(28), 7313–7318. https://www.pnas.org/doi/10.1073/pnas.1618923114
3. Balkan Investigative Reporting Network (BIRN). (2023). Kosovo remains vulnerable to disinformation, BIRN report concludes.
4. https://birn.eu.com/news-and-events/kosovo-remains-vulnerable-to-disinformation-birn-report-concludes/
5. Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. Proceedings of the National Academy of Sciences, 118(9). https://www.pnas.org/doi/10.1073/pnas.2023301118
6. Council of Europe. (2025). Strengthening resilience to FIMI in Eastern Europe and the Western Balkans. https://rm.coe.int/iris-extra-2025-strengthening-resilience-to-fimi-in-e-europe-w-balkans/488029863a
7. Davey, J., & Ebner, J. (2019). The Great Replacement: The violent consequences of mainstreamed extremism. Institute for Strategic Dialogue. https://www.isdglobal.org/isd-publications/
8. Democracy for Development (D4D). (2024, July 9). The need for fact-checking from the media in Kosovo.
9. https://d4d-ks.org/en/editorial/the-need-for-fact-checking-from-the-media-in-kosovo/
10. Douglas, K. M., Sutton, R. M., & Cichocka, A. (2019). The psychology of conspiracy theories. Current Directions in Psychological Science, 28(6), 538–542. https://journals.sagepub.com/doi/10.1177/0963721417718261
11. Edelman. (2024). Edelman Trust Barometer 2024. https://www.edelman.com/trust/2024/trust-barometer
12. Eurofound. (2023). Living, working and COVID-19: One year into the pandemic. https://www.eurofound.europa.eu/publications/report/2023/living-working-and-covid-19-one-year-into-the-pandemic
13. European Commission. (2024). The Digital Services Act. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act
14. European Commission. (2025). Code of Conduct on countering illegal hate speech online+ integrated into the DSA framework. https://digital-strategy.ec.europa.eu/en/policies/code-conduct-illegal-hate-speech-online
15. European Council on Foreign Relations. (2021). Europe's invisible divides: How COVID-19 is polarising European politics. https://ecfr.eu/publication/europes-invisible-divides-how-covid-19-is-polarising-european-politics/
16. European External Action Service. (2022). 2nd EEAS report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

17. European External Action Service. (2025). 3rd EEAS report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

18. European External Action Service. (2026). 4th EEAS annual report on foreign information manipulation and interference threats. https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en

19. Full Fact. (2023). False and misleading claims shared during the France riots. https://full-fact.org

20. Global Network on Extremism and Technology. (2022). Insights on networked online extremism and violent ecosystems. https://gnet-research.org

21. Horgan, J. (2008). From profiles to pathways and roots to routes: Perspectives from psychology on radicalization into terrorism. The ANNALS of the American Academy of Political and Social Science, 618(1), 80–94.

22. Institute for Strategic Dialogue. (2023). Online ecosystems, extremism and radicalisation research. https://www.isdglobal.org/isd-publications/

23. Institute for Strategic Dialogue. (2024). Monitoring influence and disinformation campaigns in the Western Balkans. https://www.isdglobal.org/wp-content/uploads/2024/12/Monitoring-Influence-and-Disinformation-Campaigns-in-the-Western-Balkans.pdf

24. Macklin, G. (2019). The Christchurch attacks: Livestream terror in the viral video age. CTC Sentinel, 12(6), 18–29. https://ctc.westpoint.edu/the-christchurch-attacks-livestream-terror-in-the-viral-video-age/

25. Moonshot. (2022). Online radicalisation pathways. https://moonshotteam.com

26. Neumann, P. R. (2013). The trouble with radicalization. International Affairs, 89(4), 873–893.

27. OECD. (2023). Drivers of trust in public institutions in Europe. https://www.oecd.org/governance/trust-in-government/drivers-of-trust-in-public-institutions.htm

28. Pew Research Center. (2020). Global attitudes toward democracy in Europe and beyond. https://www.pewresearch.org/global/2020/02/27/global-attitudes-toward-democracy-in-europe-and-beyond/

29. Pew Research Center. (2023). Satisfaction with democracy and political systems over time. https://www.pewresearch.org/global/2023/03/22/satisfaction-with-democracy-and-political-systems/

30. Reuters. (2021, December 5). Several injured as Dutch COVID protest turns violent. https://www.reuters.com

31. Reuters. (2023a, July 1). France riots: unrest spreads after police shooting. https://www.reuters.com

32. Reuters. (2023b, July 4). France considers response to social media role in riots. https://www.reuters.com

33. Reuters. (2025b, August 7). Rubio orders U.S. diplomats to launch lobbying blitz against Europe's tech law. https://www.reuters.com/sustainability/society-equity/rubio-orders-us-diplomats-launch-lobbying-blitz-against-europes-tech-law-2025-08-07/

34. Reuters. (2026a, February 18). U.S. plans online portal to bypass content bans in Europe and elsewhere. https://www.reuters.com/world/us-plans-online-portal-bypass-content-bans-europe-elsewhere-2026-02-18/

35. Reuters. (2026b, March 18). JD Vance to visit Hungary ahead of April election. https://www.reuters.com

36. Reporters Without Borders. (2021). German protests against COVID-19 measures: Persecution of journalists behind the façade of a citizen movement. https://rsf.org/en/german-protests-against-covid-19-measures-persecution-journalists-behind-fa%C3%A7ade-citizen-movement

37. Van Bavel, J. J., et al. (2022). The role of social and political polarization in COVID-19 pandemic outcomes. Proceedings of the National Academy of Sciences, 119(14). https://www.pnas.org/doi/10.1073/pnas.2119690119

38. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151. https://www.science.org/doi/10.1126/science.aap9559

39. Wiktorowicz, Q. (2005). Radical Islam rising: Muslim extremism in the West. Rowman & Littlefield.

Institute of Communication Studies

www.iks.edu.mk info@iks.edu.mk

