# Emerging Trends in PCVE

THE HUB. INSIGHTS

JUNE 2026

European Commission

EU Knowledge Hub on Prevention of Radicalisation

# About the Knowledge Hub

The EU Knowledge Hub on the Prevention of Radicalisation supports Member States in strengthening their efforts on preventing radicalisation through a comprehensive, whole-of-society approach.

It provides a collaborative platform bringing together policymakers, practitioners and researchers across the EU to exchange knowledge, experience and best practices.

*The views and opinions expressed in this Digital Magazine are solely those of the authors and do not necessarily represent or reflect the official position, views, or policies of the European Commission.*

# Editorial

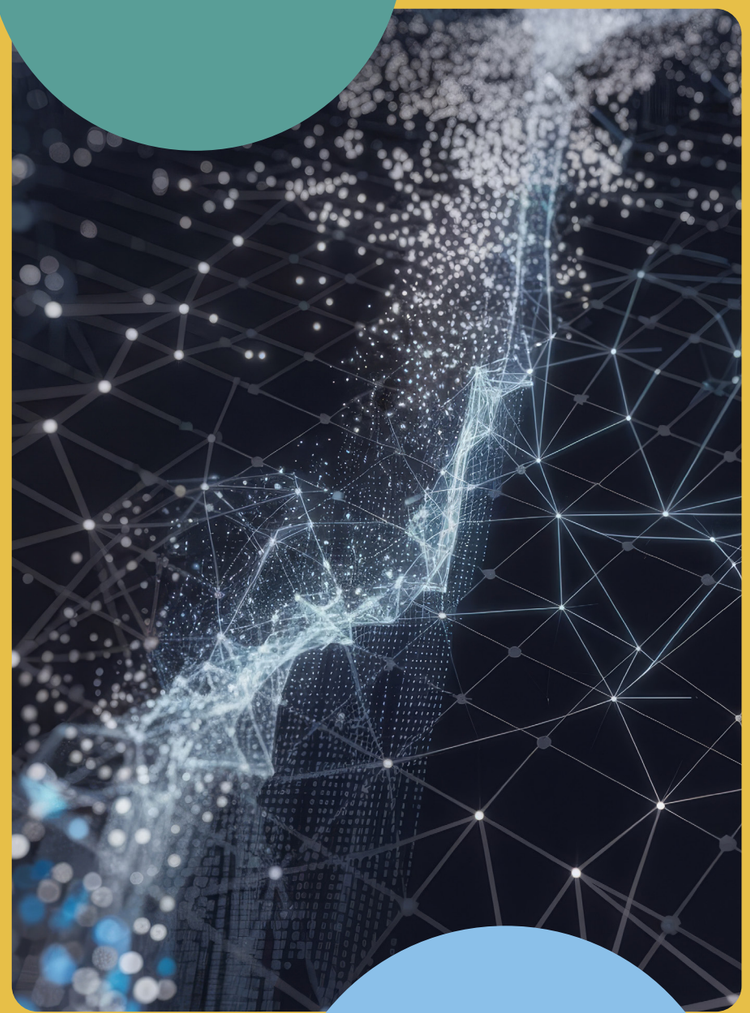
## Welcome to the fifth issue of The Hub. Insights: ‘Emerging Trends in PCVE’.

Welcome to the fifth issue of The Hub. Insights: ‘Emerging Trends in PCVE’.

The central challenge for PCVE is increasingly crisis anticipation, rather than crisis management. This issue aims to support that task by mapping emerging and highly salient trends for PCVE practitioners, policy makers, and researchers – looking at the advanced (and sometimes deceptively simple) tools extremists deploy, the digital ecosystem enabling them, and the evolving frameworks required to intercept them.

We open by exploring changing dynamics in radicalising narratives. From the modern evolution of Salafism to the transatlantic “culture wars” reshaping Europe, we analyse how narratives travel, adapt, and trigger systemic ideological spillovers. In this dynamic, we also discuss the role of ideology itself and whether extremist groups are beginning to ‘water down’ their hard ideologies to increase recruitment.

The single most rapidly changing environment for PCVE is in the digital sphere, where a complex cyber-social ecosystem has decentralised extremist propaganda, making interception harder than ever. This digital terrain stretches from the strategic manipulation of Wikipedia to the cutting-edge of Large Language Models (LLMs) and “LLM grooming” as a coming trend in disinformation techniques.



Central to the dynamism of high-tech driven digital extremism, we confront the implications of profit-maximising, addictive algorithm design on decentralised propaganda and security, and engage with the controversial discussion of what preventive measures should be taken. Yet, despite the high-tech driving changes in this environment, we emphasise the continued power of crude, low-tech online content which remains highly effective at mobilising followers. Across this landscape, we dissect how strategic communications can blunt Foreign Information Manipulation and Interference (FIMI).

Beyond propaganda, the nature of violence itself is morphing. We examine the transition from a general "culture of violence" to digitised Violence-as-a-Service (VaaS). Concurrently, we look at how online subcultures like the True Crime Community normalise the glorification of atrocities, creating psychological pathways into a deeply unanchored, nihilistic extremism.

When it comes to intervention: the sooner, the better. Accordingly, we focus heavily on youth and minors, mapping early warning signs to protect teenagers before mobilisation. Fittingly, our featured interview explores forensic psychological work, with a specialised focus on the radicalisation of minors. Alongside this, we examine the vital role of "Digital Street Workers" who actively patrol online spaces to safeguard vulnerable youth.

Finally, we address the sharp end of the security spectrum: already mobilised extremists. This issue reviews essential collective data on the management and legal realities of European Foreign Terrorist Fighters (FTFs) in Iraqi prisons, providing actionable insights for policymakers and practitioners dealing with high-risk threats.

The trends in these pages are unfolding in real-time. We hope this issue serves as both a manual and a roadmap to help you navigate, adapt to, and intercept the next generation of extremism.

# A Special Message

## Emerging Trends in PCVE: Data and Research as Our Crystal Ball

Terrorist and violent extremist activity is increasingly shaped by the misuse of digital and emerging technologies. Online radicalisation is on the rise, including among minors. Geopolitical developments, along with the malign influence of state and non-state actors, further complicate the threat landscape. The evolving nature of these threats requires a more adaptive and robust response. This is the context underpinning the EU's new ProtectEU Agenda to prevent and counter terrorism, which emerges as a flagship institutional initiative within the framework of ProtectEU: a European Internal Security Strategy.

The future of violent extremism in Europe will be shaped by convergence between ideologies, technologies, criminal ecosystems, and social vulnerabilities. Rather than a linear evolution of past threats, the emerging landscape points toward a more fragmented, hybrid, and less predictable forms of violence—requiring a fundamental rethinking of PCVE frameworks.

One of the most critical future dynamics is the deepening nexus between violent extremism and organised crime. Increasingly, the boundaries between ideological violence and profit-driven criminality are dissolving. Terrorist and extremist actors are expected to rely more heavily on criminal infrastructures—ranging from illicit financial networks to "violence-as-a-service" models—while criminal groups adopt tactics traditionally associated with terrorism, including intimidation, "symbolic violence" -deliberately strike symbolic locations—like monuments or religious sites—to challenge the legitimacy of the state and broadcast their ideology, and targeted attacks. Recent developments show how digital platforms facilitate cross-border recruitment for violent acts, often blurring whether violence is politically or economically motivated. This convergence not only enhances operational capabilities but also complicates detection, as actors move fluidly across legal and conceptual categories.

The future of online radicalisation is likely to be increasingly influenced by advances in artificial intelligence and digital technologies. Developments in generative AI may enable extremist actors to produce highly sophisticated, scalable and personalised content, facilitating the dissemination of tailored narratives that exploit individual vulnerabilities, grievances and behavioural characteristics. This shift from mass messaging to micro-targeted influence campaigns is likely to increase the effectiveness of recruitment, particularly among individuals who do not initially identify with a specific ideology but are vulnerable to grievance-based narratives.

Simultaneously, technologies such as deepfakes, synthetic media, virtual and augmented reality applications, metaverse environments and decentralised digital platforms are expected to transform the ways in which extremist communities communicate, recruit and mobilise supporters. These developments may further complicate detection, monitoring and intervention efforts, particularly as traditional content moderation approaches become less effective. In parallel, growing concerns have emerged regarding the role of algorithmic systems in shaping information exposure and potentially reinforcing polarisation, conspiracy beliefs, and extremist narratives. The increasing diffusion of "legal but harmful" content—often embedded within entertainment, humour, lifestyle material or influencer-driven communication—adds another layer of complexity to the online threat landscape. Consequently, future prevention efforts are expected to place greater emphasis

on platform governance, algorithmic accountability, digital resilience, media literacy and the responsible regulation of AI-enabled communication environments, moving beyond a sole focus on content removal towards a broader governance-based approach.

At the same time, the involvement of minors in extremist and criminal violence is likely to intensify. Young individuals are increasingly targeted through online ecosystems that combine elements of gaming, social media, and subcultural communities. Europol data indicates that nearly one-third of terrorism suspects in the EU are minors or young adults, with cases involving individuals as young as 12 planning attacks. Moreover, minors are now systematically recruited by criminal networks for roles that include not only logistics but also direct participation in violent acts. This trend reflects both a strategic adaptation by networks seeking to reduce legal risks and a broader societal vulnerability, where identity formation, marginalisation, and online exposure intersect. Future PCVE efforts will need to prioritise early prevention, digital safeguarding, and youth-focused interventions that go beyond traditional security approaches.

Hybrid extremism—where individuals combine elements from different belief systems, conspiracy theories, and personal grievances—will likely become more prevalent. This ideological fluidity challenges existing risk assessment tools, which are often built around fixed typologies such as jihadism or far-right extremism. A particularly concerning emerging phenomenon is the rise of nihilistic violence. Unlike traditional forms of extremism rooted in coherent ideological frameworks, nihilistic violent extremism is characterised by a rejection of meaning, authority, and social norms, often driven by a desire for chaos, notoriety, or personal gratification. Online communities have played a central role in fostering such dynamics, creating environments where extreme cruelty is normalised and even incentivised. These networks frequently attract young and psychologically vulnerable individuals, blending elements of extremist ideology, criminal behaviour, and subcultural identity into highly volatile forms of violence. The absence of clear ideological markers makes detection particularly challenging, as traditional risk indicators may no longer apply.

Looking ahead, radicalisation pathways will become increasingly individualised, decentralised, and technologically mediated. Artificial intelligence, immersive digital environments, and encrypted communication will enable more adaptive and resilient forms of extremist engagement. At the same time, hybrid threat actors—including state-linked entities—may continue to exploit these dynamics, leveraging criminal and extremist networks as proxies for destabilisation.

In this evolving context, PCVE must transition from reactive and ideology-based models toward anticipatory, behaviour-focused, and ecosystem-oriented approaches. This includes integrating insights from criminology, psychology, and data science; strengthening cooperation between security, social, and technological actors; and investing in resilience at the community level. As violence becomes more diffuse, youth-driven, and less ideologically defined, the ability to detect early signals and intervene across multiple domains will be central to future prevention efforts. That is why the EU Knowledge Hub is so important. It provides an integrated platform for exchange among researchers, practitioners, and policymakers, fostering a forward-looking approach. Effective prevention requires strong anticipatory capacity. While we cannot predict the future, we can leverage available data to explore plausible scenarios and develop informed, effective policies.

**Dr. Triantafyllos (Akis) Karatrantos**,
Chair of the EU Knowledge Hub Research Committee

# Contributors

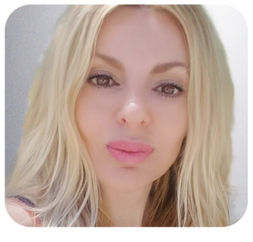
Aissa Bah

Alexander Ritzmann

Alexander Weissenburger

Arije Antinori

Dániel Rémai



Eva María Jiménez González

Fabian Wichmann


Ferdinand J. Haberl

Gazbiah Sans

Gijs Van Beek

Hanno Schedler

Javier Ruipérez Canales

Julia Berczyk

Jusaima Moaid-azm Peregrina


Lilla Schumicky-Logan

Markus Wagner

Mikkel Bøgeskov Eriksen

Olivier  Cauberghs

Terézia Ruff

Viktória Kuszi

Virginie Andre

# Editorial Board

To ensure high editorial standards, the Digital Magazine is supported by a dedicated Editorial Board comprising five permanent experts and one external specialist invited based on the edition's specific theme. This body is tasked with overseeing the magazine's content to guarantee its quality, integrity, and professional depth.

### Gabriel Drumm Calvin

Gabriel is a Project Consultant with expertise in EU-funded projects and holds a master's degree in international relations – European Studies. He has been employed at NTU International since 2023.

### Isabel Pérez Pérez

Isabel Pérez Pérez is a journalist and communications professional specialising in Middle East security, holding a PhD in Information and Communication and 12 years of field experience. She analyses geopolitical issues and communication dynamics for various media outlets.

### Javier Ruipérez Canales

Javier Ruipérez Canales is PhD in Social Sciences from the University of Granada and has over 15 years of experience in applied research and development of projects on the prevention of radicalisation and violent extremism, as well as in PCVE Strategic Communication. Javier is member of the European Research Community on Radicalisation (ERCOR) and the Network of Experts on Hate Crime and Under-reporting (REDOI).

### Andréas Hatzidiakos

Andréas C. Hatzidiakos, Ph. D. is a senior expert, with significant experience in security and defence matters. He conducts policy-oriented research and analysis on critical security issues, with a focus on Islamist-inspired extremism, radicalisation processes and recruitment (Online/Offline, Narratives & Propaganda, Youth and Education), drivers of Violent Extremism, and the challenge posed by FTFs & Family Members.

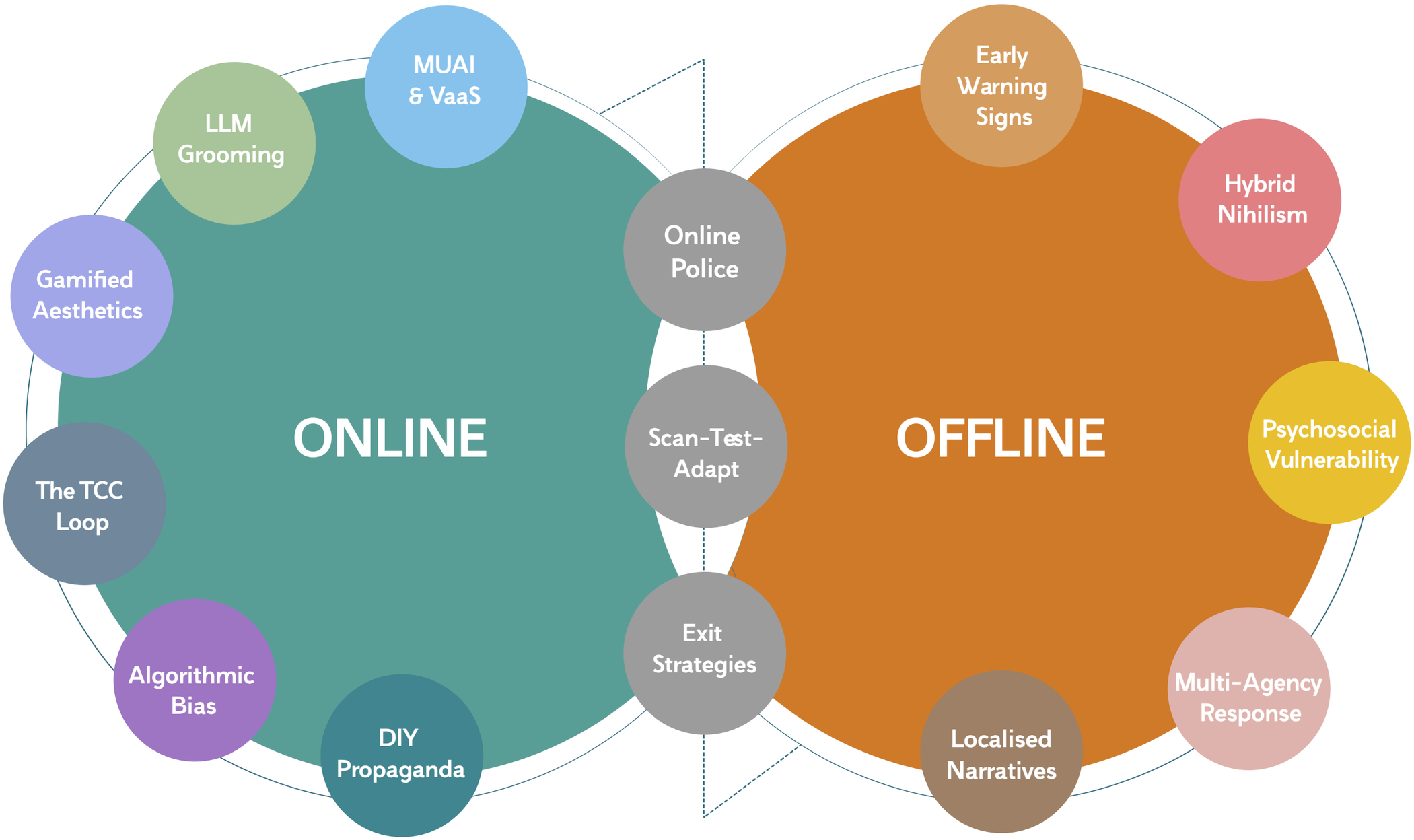
### Katrine Krogh Pedersen

Katrine K. Pedersen has spent nearly two decades working with digital youth culture. At the University of Copenhagen and the University of Washington, she examines the New Extremism and the subtle mechanisms of ideological grooming shaped by algorithms, influencers, and attention economies. She is the author of several books, including The Digitally Influenceable, and a frequent expert in television and international media, such as ABC News.

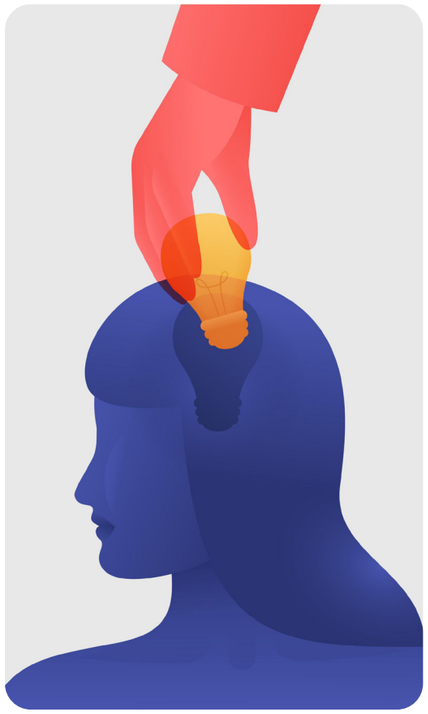
### Triantafyllos Karatrantos

Triantafyllos Karatrantos is a security and foreign policy expert specialising in radicalisation and terrorism, serving as a Research Associate at ELIAMEP and a Lecturer at the National and Kapodistrian University of Athens. With over 15 years of experience in counter-extremism research, he holds prominent advisory roles at both the European and national levels, and since 2026, he serves as Chair of the Research Committee of the EU Knowledge Hub on Prevention of Radicalisation at the European Commission.

# A Guide to Emerging Trends in PCVE



# Contents



# THE END OF IDEOLOGIES?

In recent years, especially since 7 October 2023, one could notice cross-ideological cooperations between different extremist groups in nearly every European country: we saw Kurdish communists demonstrating with Turkish fascists of the Ülkücü-movement against the war in Gaza, and the Western Queer-movement supporting the regime of the Islamic Republic of Iran.[1] Even beyond the conflicts in the Middle East, similarly astonishing alliances have been observed for some time now, such as when German far-right extremists hold joint events with Islamists.[2] It would therefore be easy to conclude that rigid ideological boundaries have lost their former significance. However, it remains to be seen if this conclusion holds true.

A closer look at the content of different Islamist groups in various social networks for example reveals many similarities. Nearly all of them address a supposed "Islamophobia" inherent in Western societies and reject the concept of labelling certain manifestations as extremist – even when this refers clearly to terrorist groups. They often also reject pluralistic and democratic concepts of society as well as sexual self-determination or the concept of gender equality.

[1] A video shared on X by the Austria-based journalist network Presseservice for example shows a demonstration in Vienna on 2 March 2024 against Israel. The footage appears to show a mix of participants, including Islamists, members of the Turkish Ülkücü movement (aka. "Grey Wolves"), "Queers for Palestine," and anti-imperialist groups demonstrating together: Presseservice Wien (03.03.2024): "X Posting / Video," X, https://x.com/PresseWien/status/1764224260854215114?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1764224260854215114%7Ctwgr%5Efa21d93afafdb62bb6a1a9c13a98b8039733cffe%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.derstandard.at%2Fstory%2F3000000210666%2Fmedien-von-pro-palaestina-demo-abgedraengt-kz-verband-wien-waehlt-neuen-vorstand [accessed 06.05.2026]; see also: Moritz Pieczewski-Freimuth (2025): Queers for Palestine: Die Verantwortung der Gender- und Queer-Studies, FFGI-Working Paper Nr. 3, Goethe Universität Frankfurt/Main. And: ROSA Österreich et al.: "Hands off Iran! / Instagram Posting," Instagram, https://www.instagram.com/p/DWXB6whgNWz/ [accessed: 08.05.2026].

[2] Der Spiegel (23.08.2006): "NPD-Kontakte zu Islamisten," *Der Spiegel*, https://www.spiegel.de/politik/deutschland/terror-npd-kontakte-zu-islamisten-a-433256.html [accessed 06.05.2026]; see also: Peter Finn (15.01.2003): "Germany Bans Islamic Group," *The Washington Post*, https://www.washingtonpost.com/archive/politics/2003/01/16/germany-bans-islamic-group/8220a0d6-442e-403c-8382-45fd315cacdb/ [accessed 06.05.2026].

These issues are just some of the themes increasingly taken up by Islamist influencers – regardless of their specific ideological background. The actors themselves are also becoming more similar in their presentation. They often rely on aesthetically appealing designs in their posts, frequently accompanied by popular music; their social media reels are professionally edited, and the content creators come across as equally polished. They present themselves as civil society activists championing legitimate causes and denounce perceived as well as actual injustices. Meanwhile, core ideological cornerstones – such as the (re) establishment of the Islamic caliphate or the installation of Sharia law – are at best treated covertly as they strive to project a pragmatic appearance. Just as the far-right Identitarian Movement has modelled its choice of methods and stylistic language on left-wing groups, modern Islamists also appear to increasingly exploit this trend for their own needs.[3] The consequence is that on the one hand they are adopting the aesthetic of both the modern far right and the far left to gather a wider audience across political beliefs. On the other hand, groups following this trend are also becoming increasingly indistinguishable from one another.

And this is precisely where a central problem for these actors could arise: if different groups are becoming increasingly similar and intentionally ambiguous about their core ideological elements, what can they pin down as their unique selling point to attract followers?

[3] Rita Abrahamsen, Jean-Françoise Drolet, Michael C. Williams et al. (2024): *World of the Right: Radical Conservatism and Global Order*, Cambridge: Cambridge University Press, pp. 34–66, https://www.cambridge.org/core/books/world-of-the-right/gramscian-right-or-turning-gramsci-on-his-head/3615A20542055567AFEDB1905C16B228 [accessed 06.05.2026]. Today, a similar strategic shift appears to be taking place within Islamist circles.

“Core ideological cornerstones are at best treated covertly as they strive to project a pragmatic appearance.”

Why should anyone take an interest in this particular group, when there are countless similar ones that may even reach a wider audience? There are already signs of a shift away from the uniformity of Islamist online content towards individually tailored websites and social media channels. A handful of groups associated with Hizb ut-Tahrir for example – an Islamist group proscribed in Germany and the UK – which had so far seemingly coordinated their social media presence, e.g. wordings and content creation, suddenly changed their strategy in the middle of last year.[4] The channels previously used were overhauled, renamed, and aligned with individuals instead of groups; This seems a more targeted approach to utilise the various platforms individually for a higher engagement.

Other groups, possibly even outside the Islamist spectrum, may follow this approach. In the course of the Gaza War for example, a large number of pro-Palestinian groups emerged, at least nominally still existing today.[5]
Nevertheless, the number of those actively participating within this scene has fallen sharply in recent times. Here as well, the different groups appear interchangeable both aesthetically and in terms of content despite a perfunctory appearance of diversity.

[4] Österreichischer Fonds zur Dokumentation von religiös motiviertem politischen Extremismus (Dokumentationsstelle Politischer Islam) (2025): Immer noch Jung. Hip. Islamistisch? Neue Entwicklungen bei Internet-Influencern mit Nähe zur Hizb ut-Tahrir, DPI Focus, https://www.dokumentationsstelle.at/fileadmin/dpi/publikationen/DPI_Focus_Immer_noch_Jung_Hip_Islamistisch.pdf [accessed 06.05.2026].

[5] Jay Ulfelder (30.05.2024): “Crowd Counting Consortium: An Empirical Overview of Recent Pro-Palestine Protests at U.S. Schools”, Harvard Kennedy School / ASH Center for Democratic Governance and Innovation, https://ash.harvard.edu/articles/crowd-counting-blog-an-empirical-overview-of-recent-pro-palestine-protests-at-u-s-schools/?utm_source=chatgpt.com [accessed: 08.05.1988]; Christophe Ayad, Soazig Le Nevé (18.03.2025): „How a New Generation of Pro-Palestinian Activists is Taking Root on French Campuses“, Le Monde, https://www.lemonde.fr/en/campus/article/2025/03/18/how-a-new-generation-of-pro-palestinian-activists-is-taking-root-on-french-campuses_6739265_11.html [accessed: 08.05.2026]

“If different groups are becoming increasingly similar and intentionally ambiguous about their core ideological elements, what can they pin down as their unique selling point to attract followers?”

Offers that differ only superficially from those of other providers do not seem sufficient to retain a steady followership in the long term.
A return to ideological polarisation, which can at least provide its supporters with a clear guidance, could therefore be imminent.

**Lessons Learned**
For a few years now, extremist groups seem to be becoming more ideologically flexible and similar to each other. It seems like rigid ideological boundaries are losing their significance.
This trend may come to a halt, as the different actors increasingly appear to be indistinguishable from each other and therefore need a unique selling point to attract new followers.

**Markus Wagner**
Project Management & Research Associate, Austrian Fund for the Documentation of Religiously Motivated Political Extremism (Documentation Centre Political Islam)

**“It seems like rigid ideological boundaries are losing their significance.”**

# A BIRD'S-EYE VIEW ON SALAFI RADICALISATION: SALAFISM AS A MODERN PHENOMENON IN A POSTMODERN WORLD

Salafism remains one of the main challenges for the prevention of radicalisation. Owing to its unique nature, as both backward looking yet utopian, the phenomenon has been one of the most dynamic strands of Islam for more than a decade. Alone in Germany around 11,500 people are estimated to follow this intransigent and strand of Islam,[1] which in its most benign form advocates the withdrawal from society, restrictive gender norms and a Manichean worldview that is spread through missionary activity (da'wa). In its most radical iteration, Salafis additionally advocate the use of terrorist violence. While this fundamentalist form of Islam is often perceived as an atavistic and anachronistic manifestation of contemporary Islam, it is neither. In its global vision and outreach, which is reflected in transnational networks as well as in its intellectual precepts, it is an intrinsically modern expression of Islamic thinking, acting and organising. Modernity, as understood in contemporary academic scholarship, does not so much refer to the process of the dispersion and adaptation of Western ideas, norms, and institutions derived from the Enlightenment, but to a more abstract, comprehensive subordination of nearly every aspect of life to a new register, defined by bureaucratisation, deterritorialisation, and rationalisation.[2]

**"Salafism remains one of the main challenges for the prevention of radicalisation."**

[1] Bundesamt für Verfassungsschutz (2019): Salafismus in Deutschland Missionierung und Jihad, Köln: Bundesamt für Verfassungsschutz, p. 5.
[2] On this see for example: Gudrun Krämer (2018): "Ḥasan al-Bannā un die Idee eines 'zeitgemäßen Islam'", in Florian Zemmin, Johannes Stephan, Monica Corrado (eds.): Islam in der Moderne, Moderne im Islam: Eine Festschrift für Reinhard Schulze zum 65. Geburtstag, Leiden: Brill, p. 255.

Effectivity and precision take precedence over mysticism and aestheticism; a productive tolerance of ambiguity becomes increasingly undermined by the search for univocal truths and definitional clarity; what was once unquestioned belief has to legitimise itself in the face of the influx of new ideas. This insight in the nature of Salafism as a modern phenomenon will go a long way to explain the attraction that Salafism has on people in search for clarity, identity and structure.

While in the West this process of modernisation happened gradually, it was drastically accelerated in the Middle East by European expansion over the course of a couple of decades during the 19th century CE. Muslim thinkers had to reevaluate their positions to come to terms with the searing questions around the apparent weakness of the Islamic umma, the community of Muslims, in comparison with both Western technological, scientific, and bureaucratic advancements on the one hand, and the waning societal and political importance of religion on the other.[3] The resulting reform strand of Islam appeared in the last decades of the 19th century and became known as Salafism. Salafis advocated for discarding nearly thirteen hundred years of Islamic scholarship and to reinterpret Islam following the method of the first generations of Muslims, the so-called *salaf al-salih* (the virtuous ancestors), who, unaffected by later intellectual developments, had to rely solely on the Quran and the sunna of Muhammad (i.e. his sayings and practices) and therefore – as Salafis argue until this day – practiced an unblemished Islam. Whereas in the beginning, this trend sought to modernise Islam[4] and to align and to a certain extend amalgamate it with Western scientific discoveries and philosophical innovations, by the 1920s these modernist inclinations began to dissipate and the more zealous and fundamentalist Salafism of today began to take hold.

Following the unprecedented horrors of the First World War, which gave testament to the more sinister aspects of Western modernity[5] while at the same time increasing direct European rule over much of the Middle East, Salafis started to look to the nascent Saudi state in the Najd, which, besides the Zaydi Imamate in northern Yemen, was the only country in the MENA (Middle East and North Africa) region to escape European conquest. Salafis flocked to the burgeoning country and let themselves become influenced by the austere and puritanical form of Islam, known after its founder as Wahhabism, practiced there. Returning home, they took these ideas, which still form an integral part of contemporary Salafi thought, with them.[6]

[3] On the intellectual influences of Western imperialism in the Arabic world, see: Albert Hourani (1983): Arabic thought in the liberal age, 1798-1939, Cambridge: Cambridge University Press, passim.

[4] On the main thinker of this strand of Salafism, Muhammad Abduh (1849-1905), see: ibid.: p. 13-160; Mark Sedgwick (2010): Muhammad Abduh, Oxford: One World Publications, passim.
[5] On this, see: Umar Ryad (2016): "A German "Illusive Love": Rashīd Ridā's Perceptions of the First World War in the Muslim World", in Erik-Jan Zürcher (ed.): Jihad and Islam in World War I: Studies on the Ottoman Jihad on the Centenary of Snouck Hurgronje's "Holy War Made in Germany", Leiden: Leiden University Press, p. 312-317.
[6] Henri Lauzière (2016): The Making of Salafism: Islamic reform in the Twentieth Century, New York, Columbia University Press, passim.

This export of what became known as puritanical Salafism, or (Neo-)Salafism, was heightened by the influence of members of the Muslim Brotherhood who fled to Saudi Arabia, seeking refuge from persecution in Egypt, which introduced a more activist, political drive into the movement from the mid-1950s onwards.[7] Simultaneously, the windfall of oil-money beginning in the 1970s enabled Saudi Arabia to spread this form of Salafism as a soft-power instrument against socialism and republicanism.[8] By the 1980s, a time by which many of the certainties of Enlightenment thinking had given way to postmodern – or alternatively late or high modern – relativism and reflexivity,[9] this form of Islamic thinking and acting had reached Europe.

Despite its archaic appearance, this puritanical Salafism is not only a product of modernity, but itself a modern form of Islam.[10] It is opposed to nuance and ambiguity and averse to mysticism and allegorical thinking. Its approach to Islamic scripture is literalist and based on the belief that the human mind could not fully comprehend God's will and should thus accept sacred writ at face value. For Salafis – as for other Islamists – Quran and sunna provide an all-encompassing model to guide individual, social and ultimately political life. Every action and idea has to be in accordance with

"Despite its archaic appearance, this puritanical Salafism is not only a product of modernity, but itself a modern form of Islam."

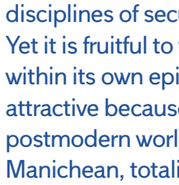
[7] John Calvert (2013): Sayyid Qutb and the Origins of Radical Islamism, Oxford: Oxford University Press, p. 276-280.
[8] Gilles Kepel (2014): Jihad: The Trail of Political Islam, London: I.B Tauris, p. 51-80.
[9] Anthony Giddens (1990): The Consequences of Modernity, Stanford: Stanford University Press, passim.
[10] On the modern character of fundamentalist religion in general, see: Shmuel Eisenstadt (1999): Fundamentalism, Sectarianism and Revolution: The Jacobin Dimension of Modernity, Cambridge: Cambridge University Press, passim.

Salafism's rigid understanding of right and wrong.[11] Whereas Islamic jurisprudence traditionally knows five degrees to classify human actions, in Salafism and other forms of Islamism this is usually reduced to the binary forbidden (haram) and allowed (halal). Countless publications on Salafi 'aqida (core doctrinal tenets) attest to the urge to explain the basics of belief and cleanse religious doctrine as well as everyday life of everything that is not sanctioned by a Salafi reading of Islamic scripture. Similar to the spread of catholic catechisms in the sixteenth century as a reaction to the Reformation, Salafism's 'aqida literature is an attempt to canonise "true Islam" in the face of intellectual challenges and reintroduce it into society.[12] It provides an alternative body of thought to Western modernity, which can be broadly defined here by its emancipative Enlightenment thinking and ideals such as individual and religious freedom as well as natural and inalienable universal rights. As an Islamic counter model to Western modernity, it is the negative image of its intellectual twin brother – progressive or liberal Islam. Both are deterritorialised, deculturised[13] attempts to reformulate and define Islam, offering moral spaces one can inhibit independent of national and cultural background. Yet whereas progressive Islam tries to accord Islam with Western modernity, Salafism seeks to spread its own form of modernity.[14]

[11] On an excellent summary of the intellectual precepts of contemporary Salafism, see: Joas Wagemakers (2016): *Salafism in Jordan: Political Islam in a Quietist Community*, Cambridge: Cambridge University Press, p. 39-59.
[12] Olivier Roy (2004): *Globalised Islam: The Search for a New Ummah, London*: Hurst & Company, p. 232-272; Dale F. Eickelman and James Piscatori (2004): *Muslim Politics*, Princeton: Princeton University Press, p. 37-45.
[13] Roy: Globalised Islam, p. 257-286.
[14] Ibid.: p. 149; Thomas Bauer (2019): *Die Kultur der Ambiguität: Eine andere Geschichte des Islams, Berlin, Verlag der Weltreligionen*, p. 65.

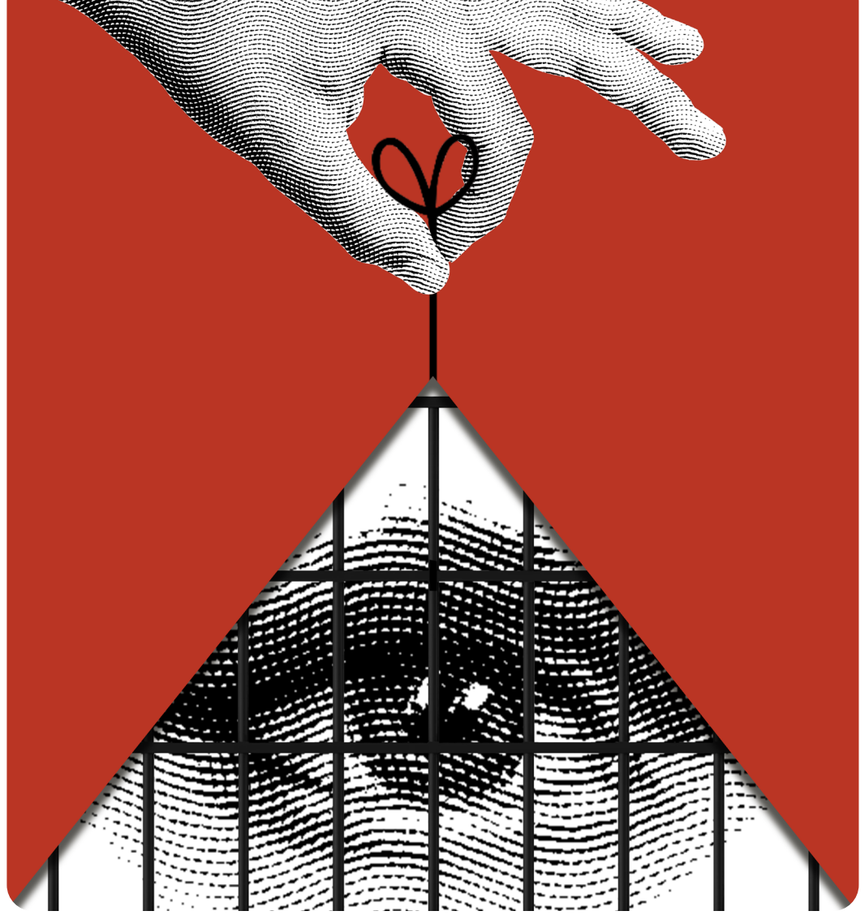
While none of this is particularly new, it so far has largely eluded the more practically oriented disciplines of security and terrorism studies. Yet it is fruitful to take the phenomenon seriously within its own epistemic context. Salafism is attractive because it is modern in an increasingly postmodern world. It is exactly its unambiguity and Manichean, totalitarian character distinguishing between purity and corruption, right and wrong, ingroup and outgroup that is perfectly suited for adolescents seeking – as Giddens calls it – "ontological security".[15]

The certainty it offers, helps to come to terms with the effects of the scepticism, arbitrariness and superficiality that defines the postmodern paradigm. Salafism embeds the believer within a fixed symbolic and moral space, empowering themhim or her through the conviction of belonging to a select group following God's eternal truth. Taking a step back from the myriads of indicators and variables for the sensibility to become radicalised identified by researchers over the last decades,[16] instead choosing a more abstract approach to the attraction of radical beliefs, opens up new pathways to see Salafi radicalisation as a symptom of larger societal developments, rather than the result of individual grievances or the alleged socio-religious particularities of Islam.



**Alexander Weissenburger**
Head of Research, Senior Researcher, Austrian Fund for the Documentation of Religiously Motivated Political Extremism (Documentation Centre Political Islam)

**"Salafism is attractive because it is modern in an increasingly postmodern world."**



[15] Giddens: The Consequences of Modernity, p. 92.
[16] A recent Australian study found 99 radicalization models and a total of 786 variables contributing to radicalization. Emily Corner, Helen Taylor (2023): "Grievance-fuelled violence: Modelling the process of grievance development", Research Report 27, Canberra: Australian Institute for Criminology, p. 18.

## Library

1. Bauer, Thomas. Die Kultur der Ambiguität: Eine andere Geschichte des Islams, Berlin, Verlag der Weltreligionen, 2019.
2. Eisenstadt, Shmuel. Fundamentalism, Sectarianism and revolution: The Jacobin Dimension of Modernity, Cambridge, Cambridge University Press, 1999.
3. Giddens, Anthony. The Consequences of Modernity, Stanford, Stanford University Press, 1990.
4. Lauzière, Henri. The Making of Salafism: Islamic reform in rthe Twentieth Century, New York, Columbia University Press, 2016.
5. Roy, Olivier. Globalised Islam: The Search for a New Ummah, London, Hurst & Company, 2004.

# HOW THE TRUE CRIME COMMUNITY USES DARK IRONY AND MEMES TO CELEBRATE MASS VIOLENCE

A TikTok video shows an animation of a mass shooter set to a catchy tune. The comments overflow with messages of glorification or emoji like 🥰 (Figure 1). On Discord, teenagers share a meme of a notorious mass killer with red laser eyes (Figure 1). On Tumblr, fan art of the Columbine attackers is tagged #hybristoblr (Figure 1). To the untrained eye, these posts go unnoticed or, at best, are judged as tasteless humour.

To researchers and law enforcement, it is something much more worrying: in some cases this can be considered a sophisticated system of meme-based communication and dark irony through which the True Crime Community, also known as the TCC, normalises (mass) violence and, in the most extreme cases, radicalises youngsters into carrying out attacks of their own.


Figure 1

**Aesthetics Over Ideology?**

Unlike most ideologically driven extremist movements, the TCC does not recruit around a manifesto or political ideology. What binds this online community together is not belief but content. Memes, edited footage of terrorist attacks, fan art, and merchandise desensitise participants and, in extreme cases, inspire them to follow in the footsteps of the Columbine shooters, Sandy Hook Elementary shooter, or Charleston Church shooter.

Although the TCC is considered a part of the Nihilistic online ecosystem by most researchers, it should be emphasised that not all members should be seen as the next potential mass shooter. The picture is more complicated than a gateway to mass violence. A portion of TCC members is driven not by violent ambition but by fascination or even hybristophilia, sometimes called "killer groupie" syndrome, a sexual or romantic attraction to people who have committed serious crimes. This can manifest through creating fan art of perpetrators, collecting memorabilia, or building shrines to attackers. Understanding this distinction matters enormously for professionals: fascination is not the same as intent, and mixing the two leads to both missed threats and unnecessary harm to young people who pose none.

The sheer diversity of motivations drawing people to True Crime content creates a significant challenge for professionals trying to identify genuine risk.

### Memetic Violence

The True Crime Community has developed a distinctive visual and memetic language that can be defined *as memetic violence*. This is the normalisation and glorification of violence through repeated ironic or aestheticised online content. The machinery behind it is more complex than most people realise.

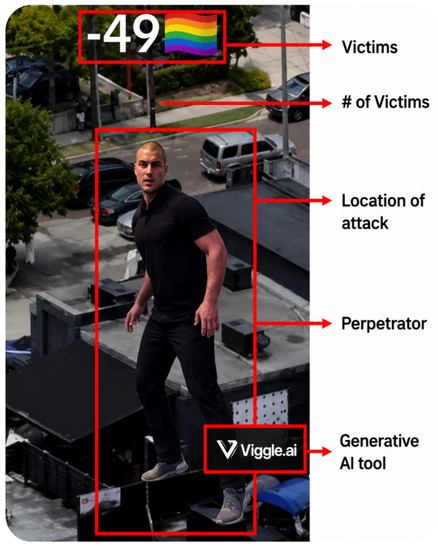



Figure 2

Viggle, Align Motion, and other generative AI tools, have become a powerful instrument for creating TCC content and evading automated content moderation (Figure 2). A typical example is a dancing perpetrator and a photo of their attack location in the background. Beside them, a victim count. Flanking it, an emoji chosen to mock the ethnicity of the victims: 🍫 for Black victims, 🌮 for Latin Americans, 🐷 for Jews or Muslims, 🏳️‍🌈 for the LGBTQ+ community, etc. The video is soundtracked by a trending audio to maximise algorithmic reach.

On Tumblr and Pinterest, mass killers are the subjects of mood boards, fan art, and romanticised edits (Figure 3).

What makes this softening of propaganda so dangerous is that real violence gets repackaged to look just like any other social media content. It uses the same styles, same formats, and same casual tone, until it stops feeling shocking at all and simply becomes part of the daily scroll.

### Platforms and the Moderation Gap

Social media platforms are not just failing to stop TCC content. In many cases they are even helping it spread. Their algorithms are designed to push content that gets clicks and reactions. And violent material does exactly that ... But there is a second problem beyond the algorithm.

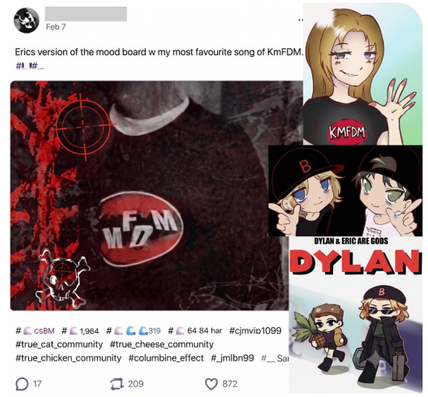



Figure 3

The TCC community constantly invent new words, hashtags, and symbols to replace the ones that get banned, staying one step ahead of the tool's platforms use to find and remove harmful content.

When platforms ban a hashtag, the community simply migrates to a coded alternative. As some platforms have banned the True Crime Community hashtag, #TrueChimeCommunity, #TrueCheeseCommunity, and #TrueCringeCommunity have all cycled in and out of use as each variation gets flagged and removed. Emoji combinations perform the same function: 🍵👀👀 (Tea Sea Sea) and 🍵🌊🌊 (Tea See See) function as a stand-in for TCC. These codes are clear among those who know their significance, yet meaningless to a content moderator scanning for known keywords.

TikTok, Tumblr, and Discord have each taken steps to ban some of the TCC content. But the shape-shifting nature of TCC community means that content migrates, mutates, and resurfaces faster than any platform can respond. Banning a hashtag does not remove content, it teaches it to hide better. This is not a problem that platform goodwill alone will solve. It requires constant investment in detection systems that can identify patterns and coded language, not just known keywords, and pressure on platforms to treat that investment as an obligation rather than a choice.

**“What makes this softening of propaganda so dangerous is that real violence gets repackaged to look just like any other social media content.”**

**Attacks Linked to TCC**

The link between TCC and real-world violence is well-documented and growing. Since the start of 2024, at least 15 school shootings or foiled attack plots have been connected to the community, with at least seven attacks carried out and nine more stopped before they could happen. In the United States alone, these incidents left at least 11 people dead and 45 injured, figures that, according to the Institute for Strategic Dialogue (ISD), make TCC-linked school shootings significantly deadlier during this period than attacks linked to any other extremist movement, including ideologically motivated ones.

Among the confirmed cases Abundant Life Christian School shooting in Wisconsin (US). The shooter, 15-year-old Natalie Rupnow, was an active participant in TCC. She quickly became a celebrated figure within the online community. This illustrates the loop at the heart of TCC where each attack generates new fandom content, drawing in the next generation of admirers. The shooter at Antioch High School in January 2025 referenced her before his attack and the shooter of the August 2025 Annunciation Church wrote her name on his rifle.

The problem is not confined to the United States. In June 2025, a 21-year-old with documented ties to TCC forums killed 11 students at the Dreierschützengasse High School in Graz, Austria.

**“The picture is more complicated than a gateway to mass violence.”**

In the United Kingdom, the July 2024 Southport attack, a 17-year-old stabbed and killed three young girls at a children's dance class, carries the characteristics.

What connects these cases across continents is not ideology, geography, or background. It is an online ecosystem that celebrates violence as identity.

**Recognising the Warning Signs**

For professionals working with young people such as teachers, social workers, etc., the challenge is not the absence of warning signs. It is knowing which ones to take seriously.

Many of the indicators are clearly visible in classrooms and online. An obsessive focus on specific perpetrators; fan art or creative writing that romanticises mass killers, and language or symbolism drawn from TCC culture or specific attacks. A teenager with a dark sense of humour is not a threat. A teenager who idolises mass shooters, actively participates in TCC spaces, and begins to identify personally with perpetrators may be.

The distinction is not always easy to draw, and it requires research, training, and expertise. A standard radicalisation checklist is not designed to catch non-ideological, aesthetics-driven radicalisation. In at least one European case in Southport, an individual with clear warning signs was referred to prevention programmes multiple times and was not accepted, because the systems in place were looking for ideology and did not find one.

**“For professionals working with young people such as teachers, social workers, etc., the challenge is not the absence of warning signs. It is knowing which ones to take seriously.”**

**Conclusion**

Just like other Nihilistic Online Subcultures, the True Crime Community sits uncomfortably outside the categories that law enforcement, mental health professionals, and policymakers have traditionally used to identify radicalisation. It has no clear ideology, and no central leadership. Members look, on the surface, like teenagers consuming popular culture. That is exactly what makes it difficult to credibly detect and analyse.

Raising awareness among professionals is an urgent priority. But awareness without nuance causes its own damage. Overreaction holds serious risks of criminalising edgy adolescent behaviour, stigmatising mental health struggles, and pushing vulnerable young people further underground, away from the support they need. Early intervention rooted in genuine care is both the more ethical and more effective response. Better tools, better training, and better cross-sector collaboration are what professionals need to fight this online phenomenon.

**Olivier Cauberghs**
Researcher, InSite Academy and Thematic Panel 3 on “New Technologies and the Online Dimension” Co-Leader

## Library

1. CTC Sentinel: True Crime Community: Understanding the Depths of Digital Fandom and Performative Violence https://ctc.westpoint.edu/true-crime-community-understanding-the-depths-of-digital-fandom-and-performative-violence/
2. ISD: Memetic violence: how the true crime community generate its own killers, https://www.isdglobal.org/digital_dispatches/memetic-violence-how-the-true-crime-community-generates-its-own-killers/

# ACROSS THE ATLANTIC: IDEOLOGICAL SPILLOVERS, DEMOCRATIC RESILIENCE, AND EUROPE'S ARCTIC NARRATIVE FRONTIER

## From Culture Wars to Ice Giants: How Narratives Travel, Adapt, Memefy and Mobilise

**"Cross-border circulation of narratives is not a secondary phenomenon, but a defining feature of the contemporary democracy threat landscape, with implications that increasingly blur the boundary between influence and interference."**

Over the past year, Europe has experienced a marked intensification of transatlantic ideological spillovers, with direct implications for democratic resilience and prevention of radicalisation. This refers to the growing circulation across borders of political narratives, polarising debates, and mobilisation strategies that originate in one context but are rapidly reinterpreted and repurposed in another. Political messaging, mobilisation strategies, and culture-war framings originating in the United States are increasingly diffusing into European information environments, where they are rapidly adapted to local grievances, partisan dynamics, and extremist mobilisation pathways.

As Ursula von der Leyen noted at the World Economic Forum Annual Meeting 2026, Europe is operating in a context shaped by geopolitical instability, technological acceleration, and growing pressure on democratic trust. In parallel, Dominique de Villepin — whose diplomatic legacy was established by his pivotal 2003 opposition to the Iraq War and the George W. Bush administration's pursuit of a preemptive strike without an international mandate— has highlighted the risks associated with an increasingly fragmented and contested international order, where competing narratives shape both perception and strategic positioning. Taken together, these dynamics highlight that the cross-border circulation of narratives is not a secondary phenomenon, but a defining feature of the contemporary democracy threat landscape, with implications that increasingly blur the boundary between influence and interference.

**From Transatlantic Flow to Local Adaptation**
To understand how these spillovers shape European information environments, it is first necessary to examine how external narratives are adapted at the local level.

Transatlantic spillovers operate through both the diffusion of ideas and processes of belief alignment, whereby external messaging is adapted rather than directly replicated. Rather than functioning as direct transfers, these processes involve localisation, through which external narratives are selectively aligned with domestic grievances, political dynamics, and cultural reference points. This dynamic is evident in the European uptake of U.S.-origin discourses related to anti-globalism, institutional distrust, and identity politics (see table 1).

Across several Member States, such themes have been localised to target EU governance, electoral processes, and social policy. Anti-globalist rhetoric, for example, is reframed as opposition to European integration, while *deep state* narratives are adapted to question the legitimacy of EU institutions. This dynamic is evident in Germany, where an investigation into a far-right extremist network revealed the adoption of conspiracy narratives akin to U.S.- derived deep state and QAnon ideologies, which were used to question institutional legitimacy and underpin plans to overturn the constitutional system.

These processes increase resonance with domestic audiences by embedding external narratives within locally meaningful grievance structures, thereby contributing to polarisation and, in some cases, facilitating pathways towards radicalisation.

At the same time, spillovers do not produce uniform effects. Evidence suggests that exposure to external political developments can also generate backlash responses, reinforcing support for democratic norms in some contexts. This is reflected in discourse surrounding Greenland, where heightened geopolitical attention has also produced countervailing messaging emphasising sovereignty, democratic governance, and local agency.

From a policy perspective, this highlights that the central issue is not the origin of narratives, but their function - how they are interpreted, contested, and repurposed within specific contexts to shape perceptions of legitimacy, trust, and threat.

In addition to digital channels, these spillovers are mediated through institutional and networked actors, including transnational religious and values-based organisations. Such networks act as vectors for diffusion and localisation, particularly on issues related to identity, morality, and social policy. Rather than simply transmitting ideas, they embed them within local cultural and political contexts, increasing their perceived legitimacy and reach.

**“These processes increase resonance with domestic audiences by embedding external narratives within locally meaningful grievance structures, thereby contributing to polarisation and, in some cases, facilitating pathways towards radicalisation.”**

To support a structured assessment of these dynamics, the overview below identifies key transatlantic ideological spillover narratives, outlines their adaptation within European contexts, and highlights their implications for prevention and strategic communications.

Taken together, these dynamics establish adaptation as the foundational mechanism of transatlantic spillovers, through which externally originating narratives acquire local meaning and political relevance. This provides the basis for understanding how such narratives can subsequently scale and circulate across digital environments.

**Digital Amplification and Feedback Loops**

While local adaptation explains how narratives gain relevance, their scale and persistence are shaped by digital ecosystems.

Digital ecosystems act as primary accelerators of transatlantic ideological spillovers, shaping how political messaging is disseminated, interpreted, and embedded. Social media platforms, alternative media networks, and encrypted messaging services enable rapid and large-scale distribution, often prioritising polarising or emotionally charged content through algorithmic systems.

“Digital ecosystems act as primary accelerators of transatlantic ideological spillovers, shaping how political messaging is disseminated, interpreted, and embedded.”

## Transatlantic Ideological Spillovers:
### Narrative Pathways and Implications

| Narrative Cluster | Core Framing (Transatlantic Origin) | European Adaptation | Implications for Domestic Communication & PCVE |
|---|---|---|---|
| **Institutional Distrust Narratives** | Elites and institutions are corrupt, controlled or manipulated. | • Targeting EU institutions, elections and governance. | • Erodes institutional legitimacy.<br>• Enables conspiracy-driven mobilization. |
| **Anti-Globalism & Sovereignty** | External actors and global institutions undermine national control and identity. | • Opposition to EU integration, climate policy and supranational regulation. | • Weakens cohesion and cooperation.<br>• Reinforces zero-sum narratives. |
| **Identity & Cultural Threat** | Civilisational decline driven by migration, liberal values or cultural change. | • Adapted into anti-migration and LGBTQ+ and anti-'woke' campaigns. | • Increases polarization.<br>• Fuels grievance-driven radicalization pathways. |
| **Media Distrust & Disinformation** | Mainstream media are biased, dishonest or part of a hidden agenda. | • Growth of alternative media ecosystems and encrypted narratives across Europe. | • Fragmented information space.<br>• Strengthens echo chambers. |
| **Free Speech & Anti-Censorship** | Regulation and content moderation are framed as suppression of free speech. | • Opposition to EU digital regulation and platform content policies. | • Delegitimizes regulatory tools.<br>• Reinforces normalization of hate and resistance narratives. |
| **Platform Governance Resistance** | Digital platforms should remain unrestricted and self-governed. | • Criticism of EU frameworks (e.g. Digital Services Act) as overreach. | • Undines persistence of harmful content.<br>• Limits enforcement of enforcement measures. |
| **Religious Nationalism** | National identity should be grounded in religion and traditional values. | • Challenges to secular governance and inclusivity (e.g. in some Member States). | • Reinforces exclusionary identity narratives.<br>• Increases ideological radicalization risks. |
| **Geopolitical Narratives (e.g. Grievances)** | Strategic competition and territorial control are framed in transnational or existential terms. | • Debates on NATO security, sovereignty and external influence. | • Normalizes adversarial and bellicose framing.<br>• Shapes geopolitical distrust. |
| **Global Crisis Integration (e.g. Iran, Gaza)** | External conflicts are framed through identity and perceived injustice. | • Rapid incorporation into domestic discourse via identity grievances and diaspora narratives. | • Emotional amplification.<br>• Cross-border narrative convergence. |
| **Political Signaling & Amplification** | High-visibility figures and movements shape political and cultural debate online. | • External messaging influence adopted by parties and electoral narratives. | • Creates feedback loops.<br>• Blurs boundaries between domestic and external influences. |

**Key Insight:** Spillovers are not linear transfers of ideas, but adaptive processes shaped by digital amplification, political signalling and local grievance structures.

Table 1

*Source: Author's analysis, drawing on original research on transatlantic ideological spillovers, narrative diffusion, and adaptation patterns across European contexts.*

A defining feature of the current environment is the role of high-visibility political signalling. Statements made in one context – whether at international forums, during electoral campaigns, or via personal platforms – can quickly influence discourse elsewhere. These signals are actively reinterpreted and selectively amplified by political actors, influencers, and online communities.

Rather than creating new narratives, these systems intensify visibility and circulation, enabling locally adapted frames to scale rapidly across interconnected information environments.

This process creates indirect narrative transfer, whereby external messaging becomes embedded within domestic debate. In this way, the boundary between domestic and external discourse becomes increasingly blurred, complicating attribution and response.

The interaction between political signalling and platform dynamics generates feedback loops: content is imported, adapted, amplified, and in some cases re-exported into transnational information ecosystems. Cross-platform migration further intensifies these effects, enabling material originating in fringe spaces to enter mainstream environments and reach broader audiences.

These feedback loops do not simply increase exposure; they stabilise and reinforce particular narrative frames through repetition and cross-platform reinforcement, increasing their visibility and perceived legitimacy over time.

**“For strategic communications, the challenge is not only the speed of dissemination but the recursive nature of these dynamics, where narratives are continuously reshaped through cycles of amplification and reinterpretation.”**

For strategic communications, the challenge is not only the speed of dissemination but the recursive nature of these dynamics, where narratives are continuously reshaped through cycles of amplification and reinterpretation. As a result, narratives that gain sufficient traction through these processes are more likely to influence how issues are framed within mainstream discourse.

**Greenland, Arctic Security, and the Normalisation of Adversarial Narratives**

As amplified narratives circulate across platforms, their effects become visible in how geopolitical issues are framed within mainstream discourse.

The growing geopolitical focus on Greenland provides a salient example of how transatlantic spillovers intersect with European security and radicalisation dynamics. Beyond traditional security considerations, it illustrates how geopolitical developments are mediated through narratives that shape perception and polarisation.

Analysis conducted through the European Observatory of Online Hate monitoring dashboard (April 2025 - April 2026) provides insight into these dynamics. The dataset includes approximately 130,500 English-language social media posts, primarily from YouTube (51%), Twitter (41%), and TikTok (3%).

While overall toxicity levels remain relatively low (10.6% of posts classified as toxic; average score 0.19), qualitative patterns are significant. Political content accounts for approximately 83% of toxic messaging, and around 66% of these posts contain violent or conflict-oriented language.

Frequently occurring terms such as “invade” and “bully” indicate a consistent adversarial framing of geopolitical developments. While only a small proportion of content reaches high toxicity thresholds, the broader pattern is significant: conflict-oriented language becomes integrated into mainstream discourse, contributing to the normalisation of adversarial framing. In this context, normalisation refers not to the presence of extremist content, but to the increasing acceptability of conflict-based interpretations within everyday political communication.

The word cloud analysis further illustrates the structure of this discourse environment. Prominent terms – including references to key geopolitical actors (e.g. “Trump”, “Russia”, “China”, “Iran”), regions (e.g. “Europe”, “Ukraine”, “Canada”), and conflict-related language (e.g. “invade”, “war”, “forces”) – indicate a highly politicised and security-oriented framing of Greenland-related discussions.
The co-occurrence of geopolitical references with derogatory or polarising terms also points to the blending of political discourse with emotionally charged and adversarial language.

From a policy perspective, this pattern demonstrates how geopolitical topics are embedded within broader conflict-oriented interpretative frames, where global power competition, identity politics, and polarisation intersect. In this way, adversarial framing becomes structurally embedded within how geopolitical developments are interpreted, even in the absence of explicitly extremist content.


For strategic communications, the central concern is not the presence of explicit extremist ideology, but the normalisation of adversarial framing within mainstream discourse. This creates permissive environments in which:

- conflict-oriented narratives become more socially acceptable;
- geopolitical competition is increasingly perceived in zero-sum terms;
- audiences become more receptive to escalatory or exclusionary messaging over time.

For EU Member States engaged in Arctic security – including Denmark, Finland, and Sweden – this highlights the need to integrate narrative analysis into broader security frameworks. As Finnish President Alexander Stubb has emphasised, navigating this environment requires *value-based realism*, balancing principled positioning with credible and context-sensitive communication.

Similarly, Greenlandic Prime Minister Jens-Frederik Nielsen stated at the Copenhagen Democracy Summit 2026, “Our only demand is respect. (…) Look at us as a likeminded partner that you will work together with, not simply stomp on”. He further reiterated that Greenland was “not for sale.” These remarks illustrate how questions of sovereignty, legitimacy, and democratic partnership are increasingly articulated through the language of pressure, coercion, and strategic influence.

**“For strategic communications, the central concern is not the presence of explicit extremist ideology, but the normalisation of adversarial framing within mainstream discourse.”**

## Case Study: Memes and the Normalisation of Bellicose Framing


*Figure 1. Screenshots of a Youtube AI-generated Greenland-related video content illustrating stylised militarised imagery, symbolic geopolitical framing, and narrative amplification through synthetic media*

If the Greenland case illustrates how adversarial narratives become normalised at the level of language and discourse, AI-generated content demonstrates how these narratives are translated into visual, symbolic, and emotionally resonant forms.

The circulation of AI-generated video content related to Greenland on platforms such as YouTube illustrates how synthetic media can shape the tone and interpretation of geopolitical developments within digitally mediated information environments.

The visual presentation of this material is highly stylised and symbolic. Scenes depicting militarised formations, territorial flags, and coordinated movement – often incorporating anthropomorphised or fictional elements – blend realism with exaggeration. The result is memorable, high-impact content that emphasises strength, unity, and strategic control, while blurring distinctions between satire, fiction, and plausible political representation.

A second identifiable category of content draws extensively on popular culture and mythological references. Visual and narrative elements echo franchises such as *Game of Thrones*, Vikings, and The Lord of the Rings, alongside Nordic mythology (e.g. frost giants or Jötnar) and fantasy gaming aesthetics associated with *World of Warcraft* and *God of War*. These references evoke themes of conflict, territorial struggle, and heroic identity, embedding contemporary political developments within familiar cultural archetypes. In doing so, they shift narratives from informational framing towards immersive and identity-driven storytelling, increasing emotional engagement and interpretative resonance. These dynamics may be especially pronounced among younger audiences, who are more embedded within digitally mediated environments and more likely to engage with visually and emotionally driven content formats.

This convergence of entertainment and political storytelling enhances both accessibility and affective appeal, enabling complex geopolitical developments to be communicated through simplified and symbolically dense narratives.

While such references are not inherently linked to radicalisation, they form part of a broader symbolic repertoire that can be mobilised in digital environments to foster shared identities and collective interpretations.
This aligns with wider evidence that ideological actors - particularly within extremist milieus - frequently draw on medieval and mythological imagery to construct identity-based narratives and situate present-day issues within longer civilisational frames.


*Figure 2. Screenshots of Youtube AI-generated imagery combining mythological and popular culture elements to construct emotionally charged narratives of conglict, sovereignty and identity, illustrating how entertainment-based aesthetics can reinforce adversarial geopolitical framing.*

In transatlantic contexts, this dynamic increasingly intersects with culture-war discourses, where questions of identity, sovereignty, and values are reframed through simplified and highly evocative symbolic lenses.

Subtitles and accompanying messaging frequently reinforce adversarial themes, including territorial assertion, resistance to external influence, and collective mobilisation. While not necessarily extremist, such content contributes to the normalisation of conflict-oriented discourse within widely accessible and shareable formats.

As described by one of the reviewed video creators, the content is framed as “more than just entertainment - it is a thunderous call to protect national sovereignty (...) a bold affirmation of the pride and resilience of a nation thriving in the heart of the frozen Arctic”. This framing illustrates how geopolitical developments are rearticulated as calls to collective mobilisation, translating abstract political issues into emotionally compelling narratives of defence, identity, and agency.

Qualitative analysis of user comments indicates that audience responses frequently mirror and amplify these themes. Users adopt similarly adversarial language when discussing territorial control, geopolitical competition, and perceived power asymmetries, illustrating how such representations are internalised and reproduced at scale.

Importantly, this material is optimised for visibility and rapid dissemination, aligning with platform dynamics that prioritise visually striking and emotionally impactful content.

As a result, synthetic representations of this kind can reach wide audiences and shape perceptions, even in the absence of factual grounding.

This transformation is significant: narratives are no longer only interpreted cognitively, but experienced affectively, increasing their memorability, shareability, and potential for identity-based alignment. In this way, visual and synthetic media do not merely reflect existing narratives but intensify their emotional salience and capacity for mobilisation.

**Narrative Convergence Beyond the Transatlantic Space**

These dynamics are not limited to transatlantic exchanges but operate within a broader system of global narrative convergence. Events in regions such as Iran and Ukraine are rapidly integrated into European (dis)information environments, often through pre-existing ideological frames.

Such developments are not merely reported; they are interpreted, repurposed and embedded within ongoing debates around governance, identity, and conflict. In this context, narratives become modular, enabling global events to be selectively aligned with domestic grievances and existing belief systems. This modularity allows the same event to be interpreted through multiple ideological lenses, reinforcing polarisation and increasing the emotional intensity of public discourse.

These processes are also visible in reciprocal and iterative exchanges across contexts, where geopolitical events are not only interpreted but actively reworked through memetic and visually mediated formats. Narratives are increasingly contested, remixed, and redeployed across transnational digital spaces, enhancing both their adaptability and their reach.

**“This transformation is significant: narratives are no longer only interpreted cognitively, but experienced affectively, increasing their memorability, shareability, and potential for identity-based alignment.”**

A clear illustration is the emergence of reciprocal meme wars, in which geopolitical actors respond to one another through stylised and memetic content. Recent examples include the circulation of AI-generated, LEGO-style videos used to reframe and contest competing narratives through satire, symbolism, and visual storytelling. Such exchanges show how conflict communication increasingly operates through iterative and performative cycles in which narratives are countered, remixed, and amplified across digital environments.

This content circulates within hybrid information environments – reshared by Iranian state-affiliated outlets, amplified by Russian media, and engaged with by transnational audiences, including Western viewers. In this way, narratives travel beyond their original context and gain global reach.

This dynamic is also visible in audience reception. Engagement with AI-generated LEGO-style geopolitical content extends beyond its original context, reaching transnational audiences who actively interpret and internalise these narratives. For example, in response to a recent viral AI-generated LEGO-style video depicting the Iran-U.S. conflict – characterised by stylised portrayals of U.S.

actions as unjust – one US based user comments: "*Well here I am at 67 and Iran AI videos are singing exactly what I'm thinking and I'm loving it*".

However, such responses do not necessarily indicate support for the originating actor or its broader geopolitical position. Rather, they reflect processes of narrative recognition and projection, in which viewers perceive the content as articulating pre-existing beliefs. In this case, resonance appears to stem less from alignment with Iran as a political actor than from recognition of the narrative framing – particularly depictions of U.S. actions as unjust or illegitimate.

At the same time, audience responses point to a broader shift in how credibility is constructed. Comments such as "Iran Lego Animations are more accurate news reporting than any corporate media outlet in the west" and "This isn't even propaganda... that's literally what happened" indicate how memefied and synthetic formats can be interpreted not as distortion, but as authentic or truthful representations.

This suggests that narrative authority is increasingly decoupled from source and instead grounded in emotional alignment, perceived coherence, and resonance with existing worldviews.

Memefied narratives therefore function not only as vehicles of circulation but as mechanisms of validation, enabling audiences to affirm and amplify particular interpretations of geopolitical events.

These dynamics have direct implications for radicalisation pathways. Assessments from UK security and intelligence communities have consistently highlighted that foreign policy developments can act as motivating or framing factors in radicalisation pathways, particularly when interpreted through narratives of grievance or perceived injustice. Past terrorist attacks in locations such as London, Manchester, and Australia demonstrate how global events can be integrated into local justifications for violence.

This dynamic however is not new. What has changed is its scale, speed, and structural integration within contemporary information environments. In an echo system characterised by declining trust and ever-growing challenges to information integrity – content travels faster, reaches wider audiences, and is more readily adapted.

As the preceding examples illustrate, emotionally resonant and memefied narratives can facilitate rapid cross-context identification, enabling individuals to internalise and reproduce externally generated frames as expressions of their own beliefs.

When linked to identity or perceived injustice, such narratives can gain traction quickly and persist beyond the original triggering event, increasing their potential relevance within radicalisation processes.

**The Deceit Era: A Structural Shift in the Information Environment**

The cumulative effects of these dynamics reflect a broader structural shift in the information environment.

These developments can be understood as part of a broader *Deceit Era*, characterised by the erosion of shared evidentiary standards and an increasing reliance on emotionally resonant narratives. This dynamic aligns with broader observations that contemporary political narratives increasingly evolve in response to overlapping and recurrent crises, reinforcing their adaptability and persistence within public discourse.

In this context, the proliferation of synthetic media, alongside declining trust in traditional information sources, is reshaping how credibility is assessed. Rather than competing primarily on accuracy, narratives increasingly compete on emotional alignment, perceived authenticity, and coherence with existing worldviews.

This contributes to a more complex information integrity landscape, where the distinction between verified information, interpretation, and opinion becomes increasingly blurred.

Importantly, this shift explains why amplified and emotionally resonant narratives gain traction: not simply because they are visible, but because they align with how audiences construct meaning and trust in contemporary digital environments.

While digital infrastructures continue to play a reinforcing role, the significance of this shift lies less in the mechanics of dissemination and more in how credibility and legitimacy are constructed by audiences. Danish Prime Minister Mette Frederiksen warned at the Copenhagen Democracy Summit 2026, the inability to regulate algorithmic systems risks contributing to "a more fragmented [and] more divided political landscape". This reinforces broader concerns regarding how digitally mediated environments amplify emotionally resonant and polarising narratives. As illustrated in the Greenland case, where conflict-oriented interpretations gained traction despite relatively low levels of explicit toxicity – and further reinforced through visually mediated and synthetic content – emotionally resonant and identity-consistent narratives are more likely to be accepted and retained, regardless of their evidentiary basis.

For strategic communications, this represents a fundamental change in operating conditions. Narratives no longer compete solely on accuracy, but on their ability to resonate with existing identities, grievances, and worldviews.

**"Importantly, this shift explains why amplified and emotionally resonant narratives gain traction: not simply because they are visible, but because they align with how audiences construct meaning and trust in contemporary digital environments."**

This has direct implications for radicalisation and prevention. Transnational narratives – particularly those linked to identity, perceived injustice, or geopolitical conflict – can:

- spread more rapidly across platforms and audiences;
- embed more deeply within communities through repetition and reinforcement;
- accelerate mobilisation dynamics by lowering thresholds for engagement.

This environment does not generate transatlantic spillovers in itself, but it conditions how they are received, interpreted, and sustained over time. Narratives originating in one context can be rapidly adapted, emotionally reinforced, and embedded within another, often with limited friction or verification.

From a PCVE perspective, this highlights the need to move beyond content-focused responses towards a deeper understanding of how narratives gain traction, how trust is constructed, and how meaning is formed across digital environments.

**“From a PCVE perspective, this highlights the need to move beyond content-focused responses towards a deeper understanding of how narratives gain traction, how trust is constructed, and how meaning is formed across digital environments.”**

**An Anticipatory Gap in Current PCVE Approaches**

These structural changes expose a critical limitation in current PCVE and strategic communications frameworks.

The European Union has developed robust capabilities to address hostile foreign information manipulation and interference, particularly in relation to state-sponsored threats. However, **transatlantic ideological spillovers present a qualitatively different challenge.**

These dynamics are:

- **High-visibility** rather than covert;
- **Originating in democratic partner contexts** rather than adversarial actors;
- Indirect in their influence, yet **cumulative in their impact.**

This creates a distinct anticipatory gap. Existing frameworks – often structured around domestic radicalisation indicators or hostile foreign interference – are not fully configured to capture how mainstream political and ideological narratives originating in democratic partner contexts are reinterpreted, legitimised, and embedded within European extremist environments.

This gap also reflects a broader conceptual limitation: transatlantic spillovers have traditionally been understood in terms of influence rather than interference. However, as these dynamics become more structured, persistent, and politically consequential, the distinction between influence and interference becomes increasingly blurred. While such narratives may not constitute coordinated or state-directed interference, their cumulative effects can shape political discourse, perceptions of legitimacy, and mobilisation pathways in ways that are functionally comparable to interference-like outcomes.

This shift is further reflected in the increasing use of stylised and performative representations of conflict within official and semi-official communication. Recent analysis highlights how real footage of military action has been combined with imagery and aesthetics drawn from video games and cinematic productions, framing acts of violence through the visual language of spectacle and national triumph.

Such developments challenge existing analytical and policy frameworks, which are primarily designed to identify covert manipulation or coordinated interference, but are less equipped to address high-visibility, narrative-driven dynamics that operate through emotional engagement, performative amplification, and audience participation.

In this context, narrative-driven framing of geopolitical relations – often characterised by adversarial or coercive language – can also place indirect pressure on established norms of international conduct. While not amounting to formal violations of international law, such discursive patterns may contribute to the normalisation of more confrontational or "bullying" approaches to international relations, particularly when amplified and internalised across domestic audiences.

Violent and non-violent extremist actors increasingly draw on transnational narratives for:

- legitimacy, by aligning with broader political discourse;
- framing strategies, by embedding local grievances within global narratives;
- mobilisation cues, by responding to perceived developments beyond national contexts.

Importantly, originating discourse does not need to be explicitly extremist to have downstream radicalising effects. When such narratives are normalised within mainstream discourse and reinforced through emotionally resonant and symbolic forms, they can contribute to grievance construction and lower thresholds for engagement in harmful or violent action.

**Strengthening Strategic Communication for Prevention**

Addressing this gap requires a shift from reactive to anticipatory approaches.

Strategic communications should be positioned as a core prevention capability.

This includes:

- systematic monitoring of cross-border diffusion;
- early identification of amplification patterns;
- analysis of local adaptation processes;
- development of credible, trust-based communication strategies.

This also requires the sustained promotion of democratic narratives centred on institutional legitimacy, civic participation, social cohesion, and democratic agency. As highlighted during the Copenhagen Democracy Summit 2026, strategic communications must increasingly connect security, economic resilience, and democratic values into coherent public narratives that reinforce public trust, collective responsibility, and confidence in democratic systems. Danish Prime Minister Mette Frederiksen similarly warned that "if people don't trust that tomorrow will be better than yesterday, then they stop believing in democracy", highlighting how democratic resilience increasingly depends not only on countering harmful narratives, but also on sustaining public confidence in democratic futures.

To operationalise this shift, three areas require particular attention:

- The development of narrative early-warning capabilities, enabling institutions to identify emerging cross-border narratives before they become embedded within domestic discourse;
- The integration of narrative analysis into broader security and geopolitical assessments, particularly in strategically sensitive regions such as the Arctic, where narrative framing increasingly shapes perceptions of legitimacy and conflict;
- The expansion of pre-bunking and narrative-level interventions, focusing not only on correcting misinformation but on anticipating and countering emotionally resonant and identity-driven narratives before they gain traction.

This may also require closer coordination between strategic communications, intelligence, and policy communities to ensure that narrative developments are treated as early indicators of broader security-relevant shifts.

At the same time, responses must remain proportionate. Overly restrictive approaches risk reinforcing narratives of censorship and institutional overreach. Debates surrounding initiatives such as the European Democracy Shield illustrate the complexity of operating in contested environments, where policy measures can be reframed through adversarial lenses.

As EU Commissioner Michael McGrath has noted, Europe is operating "in an era where the manipulation of information is increasingly used as a geopolitical weapon". This highlights a central tension: efforts to strengthen resilience must avoid reinforcing the very distrust they seek to address.

**Lessons Learned**

1. **Adaptation over transfer** – Transatlantic ideological spillovers do not operate through direct replication, but through localisation, where narratives are aligned with domestic grievances, political dynamics, and cultural reference points, increasing their resonance and impact.
2. **Amplification without origin** – Digital ecosystems do not generate narratives but significantly extend their scale, persistence, and visibility through cross-platform feedback loops that stabilise and reinforce particular frames over time.
3. **Normalisation without explicit extremism** – Adversarial and bellicose framing can become embedded within mainstream discourse even in the absence of explicitly extremist content, creating permissive environments for escalation.
4. **Visualisation and gamification of conflict** – Synthetic, meme-based, and visually mediated content translates political narratives into emotionally resonant and symbolic forms, increasing their memorability, shareability, and appeal – particularly within digitally embedded and younger audiences. At the same time, it increasingly frames geopolitical developments through the logic of entertainment, competition, and gaming, transforming conflict into engaging and performative narratives that can obscure the human, political, and strategic consequences of war.
5. **Greenland as a narrative frontier** – In contexts where geopolitical competition intersects with local identity and demographic dynamics, narrative framing plays a central role in shaping perceptions of legitimacy, sovereignty, and conflict.
6. **From influence to interference** – In democratic partner contexts, cumulative narrative effects are increasingly blurring the boundary between influence and interference, shaping political discourse and mobilisation pathways without requiring coordinated or state-directed action.
7. **Democracy under narrative pressure** – These dynamics reshape not only what citizens believe, but how they engage politically, increasingly privileging confrontational, zero-sum, and coercive modes of democratic participation, with direct implications for democratic resilience.
8. **Radicalisation through narrative resonance** – Radicalisation pathways are increasingly facilitated not through exposure to explicitly extremist content, but through sustained engagement with emotionally resonant, grievance-based narratives. Memetic and modular formats enable individuals to recognise and internalise these narratives as expressions of their own beliefs, lowering barriers to adoption and creating openings for more extreme interpretations over time.

**Conclusion**

Transatlantic ideological spillovers are now embedded within Europe's radicalisation landscape, operating through interconnected processes of adaptation, amplification, and convergence.

Taken together, these dynamics form a cumulative chain: narratives are adapted locally, scaled through digital ecosystems, normalised within mainstream discourse, and reinforced through emotionally resonant and visually mediated formats within a broader structural environment that favours narrative coherence over verification.

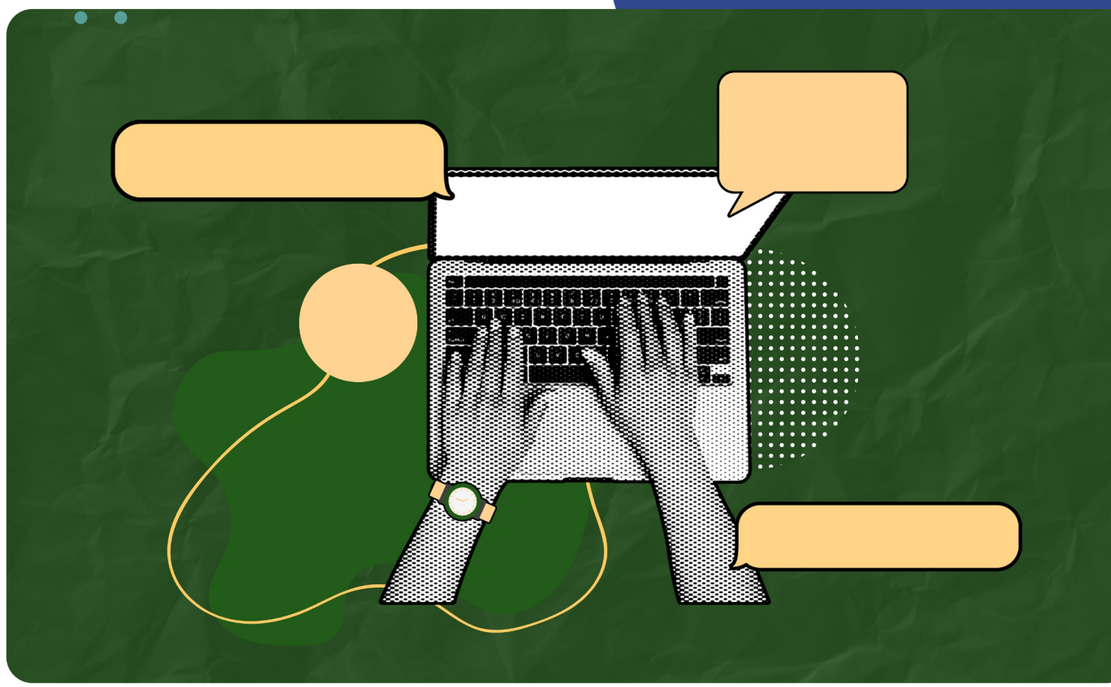
In this context, the challenge for the European Union is not to restrict the circulation of ideas, but to strengthen its capacity to anticipate how messaging is interpreted, internalised, and mobilised across contexts, particularly as the boundary between influence and interference becomes increasingly blurred. As highlighted during the Copenhagen Democracy Summit 2026, "security is not only military. It is democracy, it is social, it is human". This reflects the extent to which democratic resilience, social cohesion, and information integrity are increasingly interconnected within contemporary security environments.

Ultimately, strengthening democratic resilience will depend not only on responding to harmful narratives but on sustaining public trust, democratic legitimacy and a share sense of collective agency in an era increasingly defined by narrative competition, strategic ambiguity and geopolitical pressure.

**"The challenge for the European Union is not to restrict the circulation of ideas, but to strengthen its capacity to anticipate how messaging is interpreted, internalised, and mobilised across contexts, particularly as the boundary between influence and interference becomes increasingly blurred."**

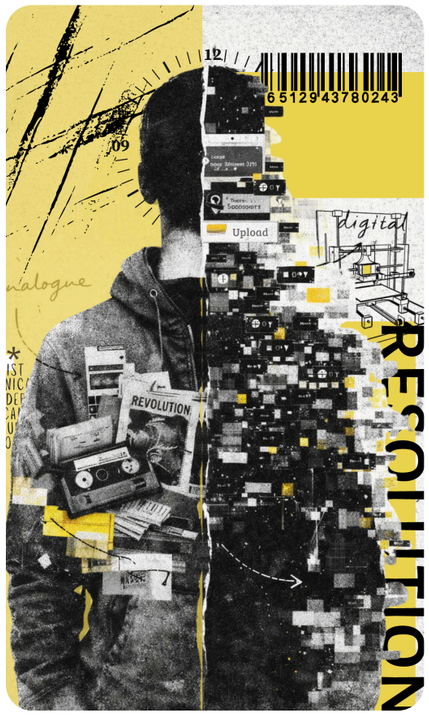
**Virginie Andre**

Kare Ry, EU KH Special Adviser in StratComms



## Library

1. Bergmann, E. (2025). The Strategic Exploitation of Conspiracy Theories by Populist Leaders. *Genealogy*, 9(2), 41. https://doi.org/10.3390/genealogy9020041
2. Costa-Font, J., & Ljunge, M. (2023). *Ideological spillovers across the Atlantic? Evidence from Trump's presidential election. European Journal of Political Economy*, 76, 102231.
3. Ebner, J. (2023). *Going mainstream: How extremists are taking over.* Ithaka Press.
4. Lo Mascolo, G. (Ed.). (2023). T*he Christian Right In Europe: Movements, Networks, And Denominations.* Transcript Verlag.
5. OECD (2022), *Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions, Building Trust in Public Institutions*, OECD Publishing, Paris, https://doi.org/10.1787/b407f99c-en.
6. Podvorna, O. (2026). *The case of Greenland: Peace and security in the Arctic* (PRIF Working Paper No. 71). Peace Research Institute Frankfurt (PRIF). Access at: https://www.prif.org/fileadmin/Daten/Publikationen/Prif_Working_Papers/PRIF_WP_71_barrierefrei.pdf




# HOW DIGITAL TECHNOLOGIES DECENTRALISE THE PRODUCTION OF EXTREMIST PROPAGANDA

**Digital technologies have not only expanded the reach of extremist propaganda—they have fundamentally decentralised its production**

"Propaganda is no longer produced primarily by established organisations or recognised ideological entrepreneurs, but by a wider range of decentralised actors using readily available digital tools."

Extremist communication has undergone a profound structural transformation over the past decades. Whereas propaganda once depended heavily on organisational infrastructure—such as party structures, scene magazines, physical distribution networks, or access to printing facilities—digital technologies have made the production and dissemination of ideological content far more accessible. Individuals, small groups, and loosely connected networks can now create propaganda materials with comparatively little technical effort, distribute them across platforms and borders, and build digital communities around them.

This shift has fostered an increasingly pronounced do-it-yourself (DIY) logic of extremist communication. Propaganda is no longer produced primarily by established organisations or recognised ideological entrepreneurs, but by a wider range of decentralised actors using readily available digital tools. Public debate and much of the academic literature have tended to focus on the platforms through which extremist content circulates and the reach it achieves. Less attention has been paid to the ways in which technological tools themselves reshape the production capacities of extremist actors. This matters because technological change does not simply affect dissemination; it redistributes communicative power. The result is not the disappearance of organised extremism, but a more complex communication environment in which formal groups, informal milieus, and individual producers increasingly overlap.

### Early Adaptations: Extremist Scenes and New Media Technologies

Historically, extremist milieus have frequently been early adopters of new communication and production technologies. Contemporary digital propaganda production did not emerge abruptly but developed gradually from earlier media practices. Even analogue extremist milieus and early digital networks already contained elements of a DIY logic that has intensified significantly with the expansion of digital technologies.

### Fanzines and Scene Media as Early DIY Communication

During the 1980s and early 1990s, self-produced media formed an important infrastructure for extremist communication. Within right-wing extremist milieus, numerous fanzines and scene magazines emerged, particularly within the skinhead and neo-Nazi scenes. Publications associated with the Blood & Honour network combined music-related content, scene news, and ideological articles while simultaneously facilitating networking within the scene. Within Islamist milieus, communication during the 1990s was dominated by printed publications of religious-political organisations as well as cassette recordings of sermons.

Although these forms of media production already displayed improvised DIY characteristics, they remained comparatively resource-intensive and were usually tied to organisational structures as well as physical distribution channels.

### Mailbox Networks and the Internet

By the late 1980s and early 1990s, extremist milieus had begun experimenting with computer-based communication systems. Within the right-wing extremist spectrum, mailbox networks based on Bulletin Board Systems (BBS) emerged, enabling activists to exchange propaganda materials and scene-related information. In jihadist extremist contexts, the use of digital communication spaces increased during the late 1990s. Early internet platforms and online forums enabled, for the first time, supra-regional and partially transnational networking among supporters.
These early digital environments already hinted at the decentralised communication patterns that would later become central to online extremist ecosystems.

With the wider diffusion of the internet and the availability of digital layout and graphic design software, the production conditions for extremist propaganda changed significantly from the late 1990s onwards. Groups were increasingly able to design their own content and publish it independently via websites and online platforms.

Within the right-wing extremist spectrum, the international forum Stormfront developed into a major communication platform. In jihadist contexts, actors made use of digital magazines such as Inspire to disseminate ideological narratives and propaganda. For the first time, extremist actors were able to reach broader audiences without relying on traditional gatekeepers such as publishing houses or printing facilities. Internet publishing and desktop publishing

**“With the wider diffusion of the internet and the availability of digital layout and graphic design software, the production conditions for extremist propaganda changed significantly from the late 1990s onwards.”**

therefore marked an important step towards a more decentralised and increasingly DIY-oriented propaganda environment. The concept of "leaderless resistance", in which autonomous actors operate without centralised organisational structures, found a technological counterpart in this emerging form of digital DIY communication.

**The Present: Platformised Propaganda and the Individualisation of Extremist Communication**

With the rise of social media platforms and online games, the structure of extremist communication has undergone a further transformation. Whereas propaganda was previously often produced by identifiable organisations or structured scene environments, digital platforms now enable a much stronger individualisation of communication.

What distinguishes the present from earlier forms of DIY propaganda is not the existence of self-produced content as such, but the scale, speed, accessibility, and reach with which it can now be created and circulated. Earlier forms of scene-based media production were often slow, materially constrained, and dependent on relatively stable distribution networks. Contemporary digital platforms, by contrast, allow content to be produced, adapted, and redistributed almost instantly, often with minimal cost and little prior expertise. This matters because it expands the range of actors able to participate, shortens production cycles, and makes extremist communication more responsive to events, trends, and platform-specific dynamics.

Within this environment, a pronounced DIY logic of extremist propaganda production has developed.

"What distinguishes the present from earlier forms of DIY propaganda is not the existence of self-produced content as such, but the scale, speed, accessibility, and reach with which it can now be created and circulated."

Extremist actors strategically utilise different platforms according to their communicative affordances: longer video content on streaming platforms, and short, attention-grabbing clips on rapidly circulating platforms such as TikTok or Instagram.

Social media enables direct communication with potential audiences without the need for organisational infrastructure. Platforms function not only as distribution channels but also as spaces for networking, identity formation, and mobilisation.

Within the right-wing extremist spectrum, transnational online subcultures have emerged since the 2010s, frequently grouped under the label alt-right. Messaging platforms such as Telegram play an important role in internal communication, coordination, and network building.

Jihadist extremist actors have likewise utilised social media systematically for propaganda and recruitment purposes. This became particularly evident during the peak phase of the so-called Islamic State's online propaganda campaigns, which included professionally produced videos and digital magazines.

Digital communication and physical actions are increasingly intertwined – for example when acts of violence are live-streamed or when real-world protests are strategically staged for digital audiences. Overall, extremist communication has become increasingly networked, decentralised in production, and highly dependent on platform structures.

"Overall, extremist communication has become increasingly networked, decentralised in production, and highly dependent on platform structures."

**Digital Games as Spaces of Propaganda**
In addition to social media and short-form visual content, extremist actors increasingly utilise interactive media formats to communicate and disseminate ideological content. One example is the modification and appropriation of digital games, which are deliberately used for propagandistic purposes. Within the right-wing extremist spectrum, early attempts were made to alter popular games – for instance, by integrating National Socialist symbolism or ideologically reshaping gameplay, as seen in modified versions of Counter-Strike. In the jihadist extremist context, the use of digital games extends beyond classical modifications. In games such as Arma 3, Grand Theft Auto, or Minecraft, existing game worlds, mechanics, and community structures are appropriated and ideologically reframed. The focus is less on the development of entirely new games and more on creative appropriation: scenarios are reenacted, narratives are adapted, and symbolic references are introduced – for example through roleplay formats or staged performances within the game environment.

Such practices draw on established game mechanics while leveraging their popularity and accessibility. They also serve as tools for communication and recruitment, allowing extremist actors to engage with potential supporters in interactive and immersive environments. At the same time, they follow a DIY logic: existing digital infrastructures are appropriated and ideologically recoded with relatively low technical effort.

Interactive media thus expand the repertoire of extremist communication by adding a playful and immersive dimension that is particularly appealing to younger audiences.

**Creative Tools and Mobile Production Studios**
In addition to digital platforms, new creative production tools play an increasingly important role. Software applications have significantly simplified the creation of visual content and lowered the technical barriers to entry. Programmes such as Canva or CapCut allow users without professional design expertise to produce graphics, videos, and social-media-optimised content. Digital technologies increasingly merge production and distribution capacities. Individual actors can create and immediately disseminate content via video formats, podcasts, websites, or digital music production platforms. Supported by creative software – and increasingly by AI-based tools – even single individuals can produce media content and distribute it globally.

Powerful devices such as smartphones or standard consumer computers further facilitate these processes. Devices primarily designed for everyday communication simultaneously function as mobile production studios for video, audio, and image content. This results in a communication environment in which virtually any individual can become both producer and broadcaster.

**Future Perspectives: Automation and Digital Fabrication**

Building on these broader shifts in low-threshold content production, the growing use of generative artificial intelligence represents a further step in the simplification and acceleration of digital propaganda production. Systems such as Stable Diffusion or Midjourney allow users to generate visual content through simple text prompts. Image production, which previously required design skills and technical expertise, can therefore be largely automated. For extremist actors, this development opens new possibilities for propaganda production. Content can be produced more rapidly, varied easily, and tailored to different target audiences. Consequently, the potential scalability of digital communication campaigns increases considerably.

The broader shift toward simplified, decentralised production does not remain confined to digital communication. It also extends, in more limited but analytically significant ways, into the realm of material production. Digital fabrication technologies such as 3D printing allow physical objects to be manufactured on the basis of digital design files.

This dynamic became particularly visible in debates surrounding the release of design files for the 3D-printed pistol Liberator in 2013. These files could be distributed online and downloaded globally, while the actual production occurred locally.

**“Today, digital tools primarily reshape the production conditions of extremist communication. Propaganda is increasingly produced within decentralised networks of individual actors who utilise platforms, creative software, and visual communication formats.”**

Structurally, this logic mirrors developments observed in digital propaganda production: designs or content circulate online, while implementation and use occur in decentralised settings.

At the same time, this development challenges traditional control mechanisms. While access to weapons is regulated in many states, digital design files can circulate globally while manufacturing takes place locally and often remains difficult to monitor.

Conclusion

The evolution of extremist communication demonstrates a continuous adaptation to technological change. From fanzines to mailbox networks, and from early internet forums to contemporary social media platforms, extremist scenes have frequently adopted emerging technologies at an early stage.

Today, digital tools primarily reshape the production conditions of extremist communication. Propaganda is increasingly produced within decentralised networks of individual actors who utilise platforms, creative software, and visual communication formats.

Emerging technologies such as generative AI and digital fabrication may further accelerate these dynamics.

For researchers, prevention practitioners, and security authorities, this implies the need to understand extremism more strongly as a technologically shaped adaptation phenomenon – one in which not only ideologies and networks, but also the infrastructures of production themselves must be taken into analytical consideration.

For PCVE and strategic communications, these developments suggest a need to look beyond fixed groups, formal organisations, or identifiable influencers alone. As propaganda production becomes more decentralised, prevention efforts must pay closer attention to the practices, tools, and content formats through which extremist communication is created and circulated. This includes detecting emerging visual styles, meme cultures, platform-specific adaptations, and the use of creative tools that lower the threshold for participation. It also requires a broader understanding of audiences. Individuals are no longer targeted only as consumers of extremist content, but increasingly as potential contributors, remixers, and disseminators. This shifts the focus of prevention from exposure alone to participation, and from message reception to the wider ecosystems in which extremist communication is produced, adapted, and normalised.

**Fabian Wichmann**
Research Associate, Grüner Vogel e.V. and Thematic Panel 1 on "Ideologies and Conspiracy Narratives" Co-Leader

**Info Box**

**Technological Milestones in the Production of Extremist Communication**

**1980s–1990s**
Fanzines, scene magazines, and music publications shape the communication culture of extremist milieus. Production remains largely analogue and is typically tied to organisational structures.

**Late 1980s–1990s**
First forms of digital networking emerge through mailbox systems and Bulletin Board Systems (BBS). Extremist actors begin to explore and use digital communication spaces.

**Late 1990s–2000s**
The spread of the internet and desktop publishing enables independent websites, digital propaganda materials, and international networking.

**2010s**
Social media, gaming platforms, and messaging services encourage more individualised and network-based communication within extremist milieus.

**2020s**
Low-threshold creative tools, AI, mobile devices, and platform economies enable a largely decentralised DIY production of extremist content.

**Current developments**
Generative artificial intelligence and digital fabrication accelerate the automation and scalability of extremist propaganda production. At the same time, they intensify the diffusion of information and contribute to a growing flood of informal content that overloads information environments and makes it increasingly difficult to distinguish between authentic and artificially generated materials.

# FRAME, AMPLIFY, MOBILISE: HOW FIMI FUELS RADICALISATION DYNAMICS

**“FIMI refers to coordinated, intentional patterns of behaviour aimed at manipulating the information environment, often by foreign state or state-linked actors.”**

In the months leading up to the 2024 European elections, coordinated online narratives began circulating across multiple platforms claiming that democratic institutions were systematically rigged and incapable of representing citizens’ interests. These narratives did not emerge spontaneously. They were amplified through networks of coordinated accounts, repackaged across languages, re-adapted across contexts, and reinforced by seemingly unrelated actors, creating the impression of widespread public distrust.

This type of coordinated activity reflects a structured effort to manipulate information environments in ways that shape how individuals interpret reality and position themselves within it. Understanding these dynamics requires moving beyond the notion of “fake news” and towards a more systemic concept: Foreign Information Manipulation and Interference (FIMI).

**FIMI as a System, Not Just Content**

FIMI refers to coordinated, intentional patterns of behaviour aimed at manipulating the information environment, often by foreign state or state-linked actors. However, FIMI is not limited to the dissemination of false information. Rather, it involves a combination of tactics, infrastructures, and actors operating across platforms to shape perceptions and influence societies.

As defined by the European External Action Service, FIMI is a "manipulative and coordinated" activity that may not necessarily be illegal but can significantly undermine political processes and societal trust. It operates through complex ecosystems that include overt and covert media channels, proxy networks, bot infrastructures, and increasingly, AI-generated content, making attribution difficult and impact diffuse.

**Why FIMI Matters for Radicalisation**

While FIMI is often discussed in relation to elections or geopolitical competition, its implications go further. One of its most significant effects lies in its interaction with radicalisation processes.

Current evidence suggests that disinformation and FIMI do not directly "cause" violent extremism. Rather, they support radicalisation processes by acting as risk multipliers, interacting with existing grievances, vulnerabilities, and identity dynamics to create environments in which radicalisation becomes more likely. Radicalisation is not linear or deterministic, but probabilistic and multi-final: similar exposures may lead to different outcomes, yet disinformation can accelerate cognitive opening, emotional alignment, and later mobilisation under certain conditions.

Disinformation contributes to the formation of "incubator environments" where extremist narratives can take root and translate into mobilisation under certain conditions.

**"Disinformation contributes to the formation of "incubator environments" where extremist narratives can take root and translate into mobilisation under certain conditions."**

This catalytic role can operate across different levels. At the individual level, it shapes how people interpret reality and trust information. At the community level, it reinforces polarisation and in-group/out-group dynamics. At the societal level, it undermines shared epistemic ground and institutional legitimacy.
FIMI hardly creates those grievances later exploited in radicalisation and violent extremism, but it amplifies, frames, and mobilises them.

**How Manipulation Becomes Mobilisation**

FIMI contributes to radicalisation, mobilisation, and violent extremism by reshaping the emotional, social, and moral conditions under which individuals interpret conflict, belonging, and action. A first mechanism lies in emotional activation. Manipulative narratives are crafted to trigger fear, anger, humiliation, or moral outrage. These emotional responses reduce critical thinking and increase susceptibility to simplified or extremist interpretations. In this vein, content related to conflict, identity, or perceived injustice, such as war imagery or narratives of victimisation, can intensify emotional engagement and lower cognitive barriers to radical frames.

A second mechanism lies in amplification mechanisms, including coordinated inauthentic behaviour, bot networks, and cross-platform dissemination.

These dynamics create the illusion of consensus, making certain narratives appear widely accepted. As individuals are more likely to adopt beliefs they perceive as socially validated, this contributes to the normalisation of polarising or extremist views.

A third mechanism concerns moral reframing. FIMI narratives often structure reality through stark binaries: victims and enemies, patriots and traitors, defenders and threats. Through repeated exposure, these frames can harden in-group identities, lower empathy towards out-groups, and contribute to normative shifts, where previously unacceptable ideas, including violence, become increasingly legitimate.

One of the clearest ways in which these mechanisms matter is through their role in shaping contemporary mobilisation and recruitment dynamics. When linked to disinformation, these operate through high-volume attention capture and information flooding, followed by more selective forms of conversion. Large quantities of emotionally charged content, such as graphic war footage, martyrdom imagery, dehumanising labels, or simplified moral binaries, broaden the pool of susceptible individuals by saturating the information environment and generating a sense that violence is imminent, meaningful, and widely endorsed. Cases linked to ISIS online ecosystems, Hamas-affiliated Telegram channels, and conflict-related disinformation illustrate how emotionally saturated media environments can intensify moral outrage, reinforce identity-based interpretations of conflict, and facilitate mobilisation pathways.

**"FIMI narratives often structure reality through stark binaries: victims and enemies, patriots and traitors, defenders and threats."**

As such, recruitment no longer depends only on long-term ideological socialisation; it increasingly emerges through information flooding, emotional readiness, and networked amplification.

In this context, mass dissemination often precedes personalised engagement. Open platforms are used to identify receptive audiences, after which selected individuals may be drawn into more controlled digital spaces, often encrypted channels, where ideological reinforcement, instruction, vetting, funding, or operational guidance become feasible. Naturally, mobilisation does not always culminate in formal membership of extremist organisations. It may instead take the form of low-threshold and episodic actions: sharing inflammatory content, joining protests, participating in online harassment, engaging in situational violence, or providing logistical support. In this sense, manipulated audiences themselves can become part of the operational ecosystem.

**Preventing Radicalisation in a Manipulated Information Environment**

If FIMI contributes to radicalisation indirectly, prevention must address both dimensions together. This begins with overcoming policy fragmentation. Disinformation and PCVE frameworks still operate too often in parallel, despite addressing overlapping dynamics of grievance, vulnerability, mobilisation, and early warning. A more integrated approach would make it easier to detect when information manipulation is no longer simply distorting perceptions but is beginning to facilitate radicalisation pathways.

Strategic communication approaches are equally important within integrated prevention frameworks. Countering disinformation linked to radicalisation cannot rely exclusively on fact-checking or content removal, since emotionally resonant narratives often derive their persuasive power from underlying grievances, identity dynamics, and perceptions of exclusion rather than from factual accuracy alone. Effective responses therefore require longer-term, proactive rather than reactive communication strategies capable of building credibility, reinforcing institutional (vertical) and citizen-to-citizen (horizontal) trust, and offering alternative interpretive frames before extremist narratives consolidate. In practice, this involves investing in locally trusted messengers, community-based communication initiatives, culturally grounded counter-narratives, and narrative coherence across institutional actors.

Prevention must also operate upstream. Media literacy, pre-bunking, and broader resilience-building strategies are essential because they reduce susceptibility prior to exposure, rather than intervening only once harmful narratives have already taken hold. This is particularly important in contexts characterised by information voids, weak trust in institutions, and high emotional salience.

At the same time, preventive capacity must be rooted locally. Civil society organisations, community actors, educators, and local media are often the first to detect shifts in narratives, target audiences, and community tensions.

**“Civil society organisations, community actors, educators, and local media are often the first to detect shifts in narratives, target audiences, and community tensions.”**

Their role is especially important in environments where disinformation resonates through everyday grievances and culturally specific frames that cannot be captured by abstract monitoring alone.

Platform governance should also be addressed. Improving transparency, limiting coordinated inauthentic behaviour, and strengthening content moderation, particularly in under-resourced languages, has become essential.

Equally important is contextual understanding. Monitoring capacities must account for cross-platform, cross-lingual dynamics, particularly in regions where dialects and informal channels play a central role.

In its current form, FIMI cannot be eliminated. The decentralised, adaptive nature of digital information ecosystems makes this unrealistic in the short term. However, its impact can be reduced. By targeting infrastructures rather than individual narratives, strengthening societal resilience, and integrating disinformation into broader prevention frameworks, policymakers can increase the cost, complexity, and risk of manipulation. Over time, such an approach may not stop FIMI, but it can make it less effective, less scalable, and less attractive as a tool of influence.

**Jusaima Moaid-azm Peregrina**
Researcher and Project Coordinator, Euro-Arab Foundation for Higher Studies

# FROM "CULTURE OF VIOLENCE" TO VIOLENCE-AS-A-SERVICE (VaaS): RADICALISATION PATHWAYS IN THE CYBER-SOCIAL ECOLOGY OF VIOLENCE

**"From the initial digitalisation of terrorism to the global dissemination of documented cruelty by Daesh, from memeified hate, cultic milieus, sextortion networks, do-it-yourself violent know-how, to the Malicious Use of AI (MUAI), violence has gradually become more immersive, shareable, incentivised, and operationally transferable."**

Violence-as-a-Service (VaaS) is the outcome of a broader cyber-social transformation rather than a narrow criminal innovation. In fact, contemporary violence must be understood as an ecosystem, something shaped by the interaction of platforms, fringe networks, visual cultures, online hate, coercive communities, synthetic media, and decentralised infrastructures. From the initial digitalisation of terrorism to the global dissemination of documented cruelty by Daesh, from memeified hate, cultic milieus, sextortion networks, do-it-yourself violent know-how, to the Malicious Use of AI (MUAI), violence has gradually become more immersive, shareable, incentivised, and operationally transferable. In this sense, the relevance of VaaS for radicalisation and Preventing and Countering Violent Extremism (PCVE) lies in its capacity to connect exposure, belonging, coercion and task-based compliance before, alongside, or even in the absence of fully articulated ideological commitment. Young people stand at the centre of this shift, not only as passive spectators, but as targets, recruits, producers, and increasingly as exploitable actors within fluid hybrid ecosystems. In this perspective, VaaS appears as the transactional crystallisation of an evolving step in the cyber-social ecology of violence.

The key point, therefore, is not that violence moved online and/or that VaaS emerged from one ideology, one platform, or one crime type, but it is the outcome of an evolving cyber-social environment in which circulation, spectatorship, belonging, coercion, and tasking are distributed and (re-)shaped one another over time across multiple spaces. So VaaS must be considered as the endpoint of a longer transformation in the culture, communication, and social organisation of violence, rather than as a stand-alone tactic. Young people are particularly exposed to this ecology. Many are permanently connected yet deeply atomised – socially present in networks but often isolated in everyday life, searching for recognition, identity, intimacy, and status – while being shaped by algorithmic forms of socialisation. In practice, this means that the same systems that promise connection also expose them to harmful content, hostile group norms, and increasingly persuasive synthetic actors. The result is a condition that can be described as "connective isolation": a state in which networked visibility coexists with weak attachment, fragile social competence, vulnerability to manipulation, and heightened exposure to pathways of escalation.

**Disintermediation, Mediamorphosis, and the Culture of Violence**

Digital disintermediation – as the erosion of traditional editorial, institutional and spatial gatekeepers that once limited access to violent material - has replaced analogue scarcity with persistent circulation.

**"So VaaS must be considered as the endpoint of a longer transformation in the culture, communication, and social organisation of violence, rather than as a stand-alone tactic."**

Minors have gained easier access not only to pornography but also to humiliation, torture, gore, execution footage, and violent challenge content through feeds, chats, repost chains, gaming-adjacent spaces, and algorithmic drift. The result is not merely more content but a different ecology of access: on-demand, portable, replicable, remixable, and socially shareable. Exposure occurres not only through deliberate searching, but also through ambient discovery in feeds, gaming-adjacent spaces, chats, and recommendation systems. Violence is no longer exceptional material encountered at the margins; it has become everyday background content, available for repeated viewing, ironic circulation, and peer bonding. The "mediamorphosis of terrorism"[1] has intensified this broader digital transition. While earlier terrorist organisations understood the communicative value of mediated violence, Daesh was the first malicious actor to globalise easy-to-consume violence on this scale; turning terror, sadism, and cruelty into a serialised, platform-native quasi-genre, often spectacularised through visual codes drawn from Western culture.

[1] "Mediamorphosis of Terrorism" is [...] *the rapid transformation in which the medium is not only a container of messages aimed to generate terror, such as in traditional propaganda strategies, but it also becomes 'media-terror' itself, an asymmetric weapon of the globalized contemporary reality throughout the violent action/representation digital nexus. The 'mediamorphosis' is strongly linked to the transition from the 'analogue' world - organized in a hierarchy and institutional centres of information and knowledge production which used a one-to-many communication model - to the digital world. The latter is a reticular and globalized world, exclusively based on a many-to-many communication model - founded on cross-mediality and populated by users - generated and remediated contents disseminated across the Web.*
Antinori, A. (2017). The "Jihadi Wolf" Threat: The Evolution of Terror Narratives between the (Cyber-)Social Ecosystem and Self-Radicalization "Ego-System". Paper presented at the 1st European Counter Terrorism Centre conference on online terrorist propaganda, Europol, The Hague.

"Mediamorphosis of Terrorism" *must be considered as [...] the transformation process of terrorism, occurred between the 20th and 21st Century through a transition from an analogical and hierarchical communication model to a digital and horizontal model, owing to the development of the Internet. This allowed terrorist actors to experience a continuous "technolution," that is an evolution in which the technological-digital factor in constant development constitutes the main driver for change and, therefore, terrorist entities' primary resource. [...].*
Antinori, A. (2017). The "Swarm Wolf". Understanding to prevent the evolution of terror. In T. J. Gordon, E. Florescu, J. C. Glenn, & Y. Sharan (Eds.), Identification of Potential Terrorists and Adversary Planning: Emerging Technologies and New Counter-Terror Strategies. NATO Science for Peace and Security Series (pp. 51–59). IOS Press. doi:10.3233/978-1-61499-748-1-51.

This spectacularisation through sophisticated video production, symbolic serialisation, beheadings, torture, burnings, humiliations, and sadistic executions was formatted not as incidental evidence of violence but as immersive communication, spectacle, pedagogy, and identity performance.
As moderation pressure increased, the material and its aesthetics migrated from mainstream visibility towards mirror channels, fringe platforms, gore archives, and shock communities. What persisted across this migration was not necessarily the original ideology but the grammar of violence as visibility, prestige, domination, and proof-through-display. This is one of the key bridges between the "culture of violence" of a decade ago and the later emergence of service-oriented markets of violent action, also influencing other violent extremist/terrorist infospheres.

**Fringe migration, Memes, and Online Hate**
As moderation increased on mainstream platforms, users and materials began shifting more between image boards, fringe platforms, encrypted channels, gaming-adjacent spaces, and decentralised social networks.

**"Violence is no longer exceptional material encountered at the margins; it has become everyday background content, available for repeated viewing, ironic circulation, and peer bonding."**

4chan, 8kun, Gab, Telegram, Discord, Twitch, DLive, Steam, and parts of the Fediverse[2] began forming a cross-platform chain through which users could move from discovery to bonding, from irony to commitment, and from visibility to resilience. Within this ecosystem, visual storytelling has become decisive. Memeification – the process of turning an event, image, person, etc. into a meme – compresses ideology, "dark irony", humour, and transgression into portable symbolic units, whilst online hate links misogyny, racism, humiliation, dehumanisation, and violence fandom across milieus. Online hate therefore acts as the connective tissue of this cyber-social ecology. The same logics have also "normalised" hostile political communication and symbolic aggression.

The current landscape is therefore an ecosystem rather than a set of separate ideological boxes. Gore archives, school-shooter fandoms, incel and black-pill spaces, dangerous challenges, accelerationist milieus, "saints culture" - a subculture based on glorification and veneration of far-right terrorists within certain extremist cyber-social communities -, occult-coded scenes, and coercive online communities overlap through shared moods, scripts, and migratory routes.

[2] The Fediverse is a decentralised network of interoperable social platforms. It may be understood as a decentralised ecosystem in which communication takes place across independently governed servers rather than within a single platform. This architecture enhances pluralism and user autonomy, but it can be also exploited to disseminate violent contents.

Particularly important are coercive communities in which misogyny, humiliation, self-harm, sexual coercion, violent spectacle, and extremist rhetoric converge. Gender-based violence is especially central in the violent far-right infosphere and related subcultures. In incel, male-supremacist, accelerationist, and nihilistic milieus, abuse of women and girls can function as grievance narrative, bonding ritual, humiliation script, and proof of domination. Violent material becomes expression, control, belonging, and obedience at once.

**Young People, Connective Isolation, and Cultic Traps**

Young people are central to this transformation because they are often hyperconnected yet socially atomised. Many live in a state of "connective isolation". The risk lies precisely in this conjunction: heightened exposure increases reachability, while weak social anchoring limits the relational and institutional supports that might mitigate manipulation, normalisation, or escalation. Harmful content can therefore reach them not as an episodic drama but as a persistent ambient culture. A plausible pathway begins with edgy humour, gore curiosity, or humiliating memes. It continues through community capture, where transgression becomes authenticity and status. Then it escalates into violent testing, including self-harm, doxxing[3], sextortion, swatting, and/or assault. Gamification helps explain why these environments are experientially powerful: violence is reformatted as mission, ranking, challenge, progression, and performance.

"Young people are central to this transformation because they are often hyperconnected yet socially atomised. Many live in a state of 'connective isolation'."

Occult-coded, "violent" neo-satanic, and cultic milieus can intensify this pathway. But some online cultic scenes use taboo, secrecy, elitism, esoteric symbolism, and pseudo-intimacy to fascinate vulnerable users and then convert belonging into compliance. In this sense, grooming and sextortion are not marginal, they can become mechanisms for manufacturing obedience and preparing later criminal tasking.

**Synthetic Contamination**

The Malicious Use of AI (MUAI) deepens all these processes. It multiplies symbolic production, accelerates movement from fascination to script, and introduces synthetic relations through AI-generated personae, chats, images, voices, avatars, and pseudo-companions. What earlier violent subcultures achieved through memes, reposting, and roleplay can now be done faster, more cheaply, and more persuasively. Users can also produce violent GenAI imagery and short-form videos themselves, turning production into a participatory practice rather than a specialist skill. MUAI also functions as an interoperability technology.

[3] Doxxing refers to the non-consensual exposure of a person's private identifying information online – such as real name, address, workplace, contact details, etc. –, often as a means of intimidation, reputational harm, or social coercion.

It enables actors who differ ideologically and organisationally – extremists, coercive communities, sexual offenders, scammers, brokers, and organised criminal actors – to inhabit a shared synthetic ecosystem in which strategies, scripts, markets, and target categories can be learnt, exchanged, developed, and deployed across boundaries.

The deeper issue is synthetic contamination. Increasingly large portions of the cyber-social environment can be partially artificial. Identities, testimonials, screenshots, confessions, threats, sexual images, support networks, and reputational signals can all be generated, altered, or amplified synthetically. This contaminates the relational, evidentiary, and epistemic layers through which trust is formed online. Europol now describes online child sexual exploitation (CSAM) as a field being transformed by generative AI. The most precise way to frame this development is not to say that synthetic CSAM created organised crime from nothing, but that it marks an unprecedented convergence between synthetic media and Organised Crime interest around child-abuse material, making children and adolescents more scalable, more targetable, and easier to compromise through impersonation, blackmail, reputational attack, and remote coercion. For VaaS, the implication is severe: synthetic contamination lowers the cost of selecting, testing, directing, and outsourcing vulnerable young people as targets, intermediaries, or perpetrators.

A connected implication concerns participatory fabrication. In many decentralised, hate-saturated, and extremist-adjacent milieus, the "culturalisation" of violence no longer stops at watching, remixing, or glorifying violent content. Young users are encouraged to experiment with violent GenAI imagery and video, whilst do-it-yourself capability – 3D-printed firearms, drone adaptation, improvised explosive know-how, parts lists, blueprints, and troubleshooting – is increasingly framed as competence, authenticity, and status. What is normalised is not only the object but the pedagogy. Tutorials, iterative experimentation, peer validation, and the connective sharing of failure and improvement across boards, encrypted chats, channels, and federated services. This matters because it turns operational preparation into a cultural practice. For minors and young adults already immersed in online hate, extremist ideologies, or violent subcultures, the threshold between fantasy, simulation, and actionable capability becomes thinner.

**Lessons Learned**

- VaaS should not be understood merely as a criminal tactic, but as a product of an evolving cyber-social ecosystem in which represented violence, online hate, coercion, subcultures, and operational tasking intersect.

**"For minors and young adults already immersed in online hate, extremist ideologies, or violent subcultures, the threshold between fantasy, simulation, and actionable capability becomes thinner."**

- Young people are central because they are hyperconnected yet often atomised, exposed to algorithmic forms of socialisation, harmful content, and belonging dynamics that may position them simultaneously as targets, victims, recruits, and actors.
- Online hate is not merely toxic content, but the connective tissue linking misogyny, racism, humiliation, nihilism, and violent subcultures, thereby preparing the ground for coercion, criminal fandom, and violence.
- MUAI alters both the scale and the nature of the threat: identities, relationships, images, threats, and blackmail material can now be synthetically generated and personalised, lowering the threshold for grooming, sextortion, and remote tasking.
- VaaS is now also a matter of national and European security, because such ecosystems can be exploited by hostile actors to foster internal instability, cultivate lone actors, and undermine democratic societies at low cost.

**Conclusion**

In conclusion, VaaS is not simply outsourced violence; it is the transactional crystallisation of a long cyber-social transformation. Disintermediation made violent material ubiquitous; terrorist mediamorphosis made it immersive; fringe migration made it resilient; memes and online hate made it highly viral; coercive and cultic communities made it binding; gender-based violence inside far-right, accelerationist, and nihilistic milieus made domination itself connective; gamification made violence playable; and MUAI made it scalable and tied to participatory violent production. High-risk Criminal Networks and violence brokers use VaaS, whilst sextortion networks such as 764 turn grooming and blackmail into compliance. Extremist, nihilistic, and cultic milieus exploit the same ecology for "dark propaganda", while tribute communities devoted to violent incels, school shooters, and serial killers keep violence socially available as imitation scripts and dark status models.

**"If violence has become ecological, distributed, participatory, synthetic, and transactionally transferable, then PCVE must also become ecological."**

This represents a relevant security threat at both the MS and EU level, also because hostile state and non-state actors may exploit these ecosystems through manipulative information to amplify hate, cultivate a new generation of young Connective Lone Actors (CLAs) and/or small cells at low cost, and destabilise European democracies from within. Yet this security implication should not lead to an exclusively repressive, offender-focused, or ideology-centred response. From a PCVE perspective, the central implication is that VaaS cannot be addressed through a platform-specific and/or ideology-only paradigm. If violence has become ecological, distributed, participatory, synthetic, and transactionally transferable, then PCVE must also become ecological. Prevention must move upstream from the detection of explicit extremist commitment towards the identification of cross-milieu pathways through which fascination, humiliation, misogyny, grievance, gore consumption, violent fandom, coercive intimacy, and task-based compliance gradually converge. The relevant preventive unit is therefore not only the radicalised individual, but the cyber-social pathway that makes violence meaningful, available, rewarding, and actionable.

At the same time, such an approach must avoid securitising youth culture as such, or collapsing online deviance, subcultural experimentation, mental distress, coercive victimisation, and terrorist mobilisation into a single category. The objective of PCVE in this field should not be to police adolescence, irony, or digital subculture, but to identify the moments at which relational vulnerability is converted into obedience, visibility into status, humiliation into bonding, and fantasy into tasking. This requires behavioural, socio-relational, and ecological indicators rather than merely ideological ones: movement across fringe and/or encrypted spaces, participation in violent prestige economies, escalating tolerance of cruelty, adoption of misogynistic or dehumanising scripts, involvement in sextortion or coercive peer networks, experimentation with violent GenAI outputs, and the acquisition or sharing of do-it-yourself operational knowledge.

Consequently, PCVE should prioritise disruption of pathways, not only removal of content. Content moderation remains necessary, but it is insufficient where violent cultures are migratory, memetic, encrypted, decentralised, and rapidly reconstituted. Preventive work must introduce friction into the processes that make VaaS viable: recruitment into coercive communities, the circulation of violent prestige models, the normalisation of gendered domination, the conversion of shame into blackmail, the gamification of harm, and the synthetic fabrication of trust.

This implies stronger reporting and referral mechanisms for sextortion and/or coercive grooming, closer coordination between schools, families, youth services, platforms, Law Enforcement Agencies (LEAs), and specialist NGOs, and the development of exit infrastructures for young people embedded in violent, cultic, nihilistic, or criminally exploitative online milieus. In the age of VaaS, compliance may precede belief, coercion may precede identity, and tasking may precede radicalisation.

The most important PCVE lesson is therefore that prevention must address not only violent messages, but the infrastructures of violent cyber-socialisation. VaaS emerges where violence becomes visible, desirable, imitable, monetisable, delegable, and technically actionable. Countering it requires more than counter-narratives. It requires counter-ecologies: resilient peer environments, credible adult mediation, gender-sensitive education, synthetic-media literacy, trauma-informed digital safeguarding, platform accountability, early disruption of coercive networks, and cross-border intelligence capable of recognising convergences between extremist, criminal, cultic, and AI-enabled harms. Only by intervening in the conditions that make violence (cyber-)socially meaningful and operationally transferable can PCVE respond adequately to VaaS as one of the defining security challenges of the contemporary cyber-social landscape.

**Arije Antinori**
Professor of Criminology at Sapienza University of Rome
Stratcomms/AI Senior Leading Expert at the EU Knowledge Hub on Prevention of Radicalisation

## Library


1. Antinori, A. (2015). La “mediamorfosi” del terrorismo jihadista tra iconoclastia e stato sociale. Federalismi.it – Rivista di diritto pubblico italiano, comparato, europeo, (17), 2–17. https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=30330&content=La%2B%27mediamorfosi%27%2Bdel%2Bterrorismo%2Bjihadista%2Btra%2Biconoclastia%2Be%2B%2Bstato%2Bsociale&content_author=%3Cb%3EArije%2BAntinori%3C%2Fb%3E
2. Antinori, A. (2016). From the Islamic State to the 'Islamic State of Mind': The evolution of the jihadisphere and the rise of the lone jihad. CEPOL. https://www.cepol.europa.eu/sites/default/files/10-arije-antinori.pdf
3. Antinori, A. (2017). The “Jihadi Wolf” Threat: The Evolution of Terror Narratives between the (Cyber-)Social Ecosystem and Self-Radicalization “Ego-System”. Paper presented at the 1st European Counter Terrorism Centre conference on online terrorist propaganda, Europol, The Hague. https://www.europol.europa.eu/sites/default/files/documents/antinoria_thejihadiwolfthreat.pdf
4. Antinori, A. (2017). The “Swarm Wolf”. Understanding to prevent the evolution of terror. In T. J. Gordon, E. Florescu, J. C. Glenn, & Y. Sharan (Eds.), Identification of Potential Terrorists and Adversary Planning: Emerging Technologies and New Counter-Terror Strategies. NATO Science for Peace and Security Series (pp. 51–59). IOS Press. doi:10.3233/978-1-61499-748-1-51. https://share.google/Nq2m3U4wRUavlsI2k
5. Antinori, A. (2025). Malicious use of artificial intelligence (MUAI): L'uso malevolo dell'intelligenza artificiale nell'ecosistema cyber-sociale. Sicurezza e Scienze Sociali. https://siss.terni.unipg.it/ojs/index.php/siss/article/download/151/32
6. Europol. (2024). The recruitment of young perpetrators for criminal networks. https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The-recruitment-of-young-perpetrators-for-criminal-networks.pdf
7. Europol. (2025). From instigator to perpetrator: How violence-as-a-service operates. https://www.europol.europa.eu/media-press/newsroom/news/instigator-to-perpetrator-how-violence%E2%80%91%E2%80%91%E2%80%91service-operates
8. Gartenstein-Ross, D., & Chace-Donahue, E. (2025). The Order of Nine Angles: Cosmology, practice & movement. Studies in Conflict & Terrorism. https://doi.org/10.1080/1057610X.2023.2186737
9. GNET. (2023). Cults and online violent extremism. https://gnet-research.org/wp-content/uploads/2023/07/GNET-39-Cults-Online-Violent-Extremism_web.pdf
10. Taylor, M., Quayle, E., & Horgan, J. (2026). Radicalisation in coercive online communities: A research note. Perspectives on Terrorism. https://pt.icct.nl/article/radicalisation-coercive-online-communities-research-note
11. Europol. (2025). The changing DNA of serious and organised crime (EU-SOCTA 2025). https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
12. GIFCT. (2023). Risks and challenges in online communities for 3D-printed firearms among extremists and terrorists. https://gifct.org/wp-content/uploads/2023/09/GIFCT-23WG-0823-3DPrinting-1.1.pdf
13. GNET. (2025). Droning on: The response to use of drones by domestic violent extremists. https://gnet-research.org/2025/01/27/droning-on-the-response-to-use-of-drones-by-domestic-violent-extremists/
14. GNET. (2026). Modern warfare: The Islamic State's emerging drone instruction ecosystem. https://gnet-research.org/2026/01/09/modern-warfare-the-islamic-states-emerging-drone-instruction-ecosystem/

# NIHILISTIC VIOLENCE, PSYCHOLOGICAL PATHWAYS AND THE BLIND SPOTS OF PCVE IN A DIGITAL AGE

**“Unlike ideologically driven extremism, nihilistic violence has been described as not oriented towards coherent political or religious objectives, but rather towards the glorification of violence itself, often as a source of status, recognition and meaning within digitally mediated subcultures.”**

Recent European threat assessments highlight a growing challenge that does not fit neatly within traditional prevention of violent extremism (PVE) and counterterrorism frameworks: nihilistic violent extremism. Unlike ideologically driven extremism, nihilistic violence is not oriented towards coherent political or religious objectives but towards the glorification of violence itself, often as a source of status, recognition, and meaning within digitally mediated subcultures (Source). It disproportionately involves adolescents and young adults and is frequently embedded in online ecosystems that reward transgression, notoriety, and performative cruelty (Source).

Clinical and empirical research increasingly suggests that, particularly among youth, nihilistic violence reflects developmental distress rather than ideological commitment. This article integrates clinical findings, developmental psychology, and EU level analyses to examine psychological pathways to nihilistic and lone actor violence, the catalytic role of digital environments, and persistent gaps at the interface between mental health services and PCVE.

**Developmental Vulnerabilities and Psychological Pathways**
Adolescence is characterised by profound neurodevelopmental reorganisation, including the ongoing maturation of executive functions, emotional regulation, and impulse control (Source). At the same time, identity formation, individuation, and sensitivity to perceived injustice intensify. Clinical data from specialised services indicate that adolescents referred for violent extremism frequently present with stress related disorders, externalising symptoms, and accumulated grievances linked to family, school, and peer contexts.

In this context, nihilistic violence often functions as an idiom of distress rather than a coherent ideological stance. Violent symbols, extremist imagery and hybrid narratives are frequently mobilised provocatively, instrumentally or aesthetically—to shock, transgress social norms, or elicit reaction—rather than to pursue political goals (Source). Developmental trauma, disrupted attachment, and difficulties in mentalisation may further reduce the capacity to integrate emotions, reflect on consequences and sustain empathy, increasing the risk of violent outbursts under stress (Source).

**"For vulnerable adolescents, online spaces may provide recognition and community that are lacking offline."**

**Digital Environments as Catalysts**
Digital ecosystems do not merely host radicalisation processes; they actively shape them. Nihilistic violent extremism has emerged within loosely connected online subcultures located in what EU analyses describe as an "edgesphere" of extreme internet communities, where violence is aestheticised, gamified, and converted into social currency or "clout" (Source).

For vulnerable adolescents, online spaces may provide recognition and community that are lacking offline. Algorithmic amplification, anonymity, and cross platform migration facilitate escalation from passive consumption to performative identification and, in some cases, offline violence. EU and Europol reporting further highlights that minors are often targeted through grooming-like dynamics in gaming platforms and social media, including emotional manipulation, coercion, and blackmail, which normalise violence and erode social boundaries (Source).

**Clinical and Population Level Evidence**
Clinical evidence consistently indicates that nihilistic violence is more prevalent among adolescents than adults referred for violent extremism. In a large clinical sample, nearly half of minors were assessed as being at risk of nihilistic rather than ideological violence, compared with approximately one quarter of adults. Stress related disorders and emotion regulation difficulties were significantly more common among minors, while psychotic disorders remained relatively rare (Source).

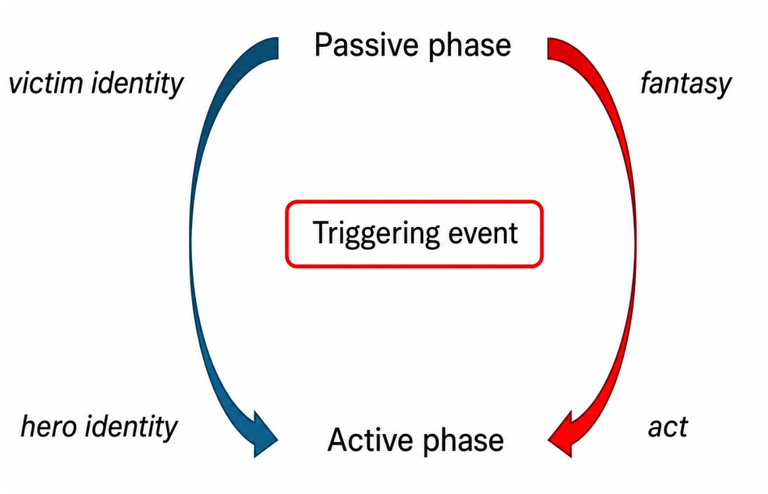
Grievances play a central role across both ideological and nihilistic trajectories. Among adolescents, school related conflicts, bullying, and family grievances are particularly prominent, while many young people remain in contact with their families and embedded in educational settings – highlighting the dual role of these environments as both risk and protective factors (Source). Planning capacity among adolescents is often impulsive and poorly developed compared with adults, complicating risk assessment and increasing the danger of misinterpreting provocation as organised intent (Source).

"Planning capacity among adolescents is often impulsive and poorly developed compared with adults, complicating risk assessment and increasing the danger of misinterpreting provocation as organised intent."

These findings are mirrored at the population level. Using machine learning methods, Haghish et al. (2023) demonstrated that extremist attitudes among adolescents could be identified with reasonable accuracy based on a broad range of psychosocial variables. The most influential predictors related to parenting quality, externalising behaviour, lifestyle factors, and overall wellbeing, while protective factors such as parental monitoring and social support were as informative as risk factors (Source).

**From Distress to Nihilistic Violence**
Psychological pathways to lone actor and nihilistic violence are best understood as dynamic processes rather than linear trajectories. Individuals may move between a passive phase, characterised by a consolidating victim's identity rooted in perceived injustice, exclusion, or humiliation, and an active phase triggered by a psychologically salient event that confirms this sense of grievance. Following such a trigger, violent fantasy – previously confined to the internal mental landscape – may become externally visible as a compensatory mechanism that restores agency, reverses power asymmetries, and provides meaning, often reinforced by digitally mediated subcultures that reward transgression.

"Psychological pathways to lone actor and nihilistic violence are best understood as dynamic processes rather than linear trajectories."




*A Psychodynamic Crisis Laden Model of Progressive Desensitization to Violence. Bah, A., & Lindberg, J. (2025). I, a terrorist? Warelia-publishing.*

For a subset of individuals, desensitisation, impulsivity, and weakened emotional regulation – particularly during adolescence – facilitate a transition from fantasy to action. Violence functions less as a political instrument than as a means of externalising distress. Post act, a temporary hero identity may reframe victimhood into recognition and control, especially when amplified online. Nihilistic extremism thus adds a new dimension to traditional victim–perpetrator dynamics. Importantly, this process is not fixed, highlighting the importance of early, developmentally informed intervention.

**PCVE Gaps at the Mental Health Interface**

Despite frequent contact with mental health services, many adolescents on pathways towards nihilistic or lone actor violence fall between systems. PCVE frameworks remain largely ideology-centred and insufficiently attuned to developmental distress, trauma, and digitally mediated identity formation (Source). Conversely, mental health services often lack clear guidance on how to assess and respond to extremist related expressions that do not meet thresholds for acute psychiatric intervention.

Standard clinical risk assessment tools are poorly equipped to capture online behaviours, symbolic identification with violent subcultures, or the performative dynamics of digital violence. Clinicians may struggle to distinguish provocation, protest, and identity experimentation from trajectories involving credible risk, particularly when ideological content is hybrid, ironic, or deliberately ambiguous. Over securitised responses risk reinforcing marginalisation, exacerbating grievances, and accelerating withdrawal into online extremist milieus.

**Towards Developmentally Informed Prevention**

Addressing nihilistic and lone actor violence requires moving beyond narrowly content focused ideological models and integrating perspectives that account for psychological needs,

**“Despite frequent contact with mental health services, many adolescents on pathways towards nihilistic or lone actor violence fall between systems.”**

developmental dynamics and digitally mediated environments; in this context, models such as the 3N model, grounded in significance quest theory, provide a useful starting point (Source). Mental health services should not be repositioned as security instruments but recognised as essential partners in early prevention. Clinical evidence supports grievance based, trauma informed, and systemic interventions that prioritise reintegration and minimise exclusion (Source).

Improved clinician training on extremist pathways, structured enquiry into digital lives, and clear consultation and information sharing frameworks between mental health services, schools, social services, and law enforcement are central. EU level regulatory efforts addressing platform accountability and systemic online risks, such as those under the EU Digital Services Act , are an important complement but cannot substitute for early psychosocial intervention.

**Lessons Learned**

PCVE strategies should prioritise families and schools as primary prevention arenas, recognising their dual role as both risk and protective environments. Digital platforms should be treated as active risk environments rather than neutral infrastructure, requiring policy attention to recommendation systems, visibility dynamics, and peer driven reinforcement of violence.

**“Addressing nihilistic and lone actor violence requires moving beyond narrowly content focused ideological models and integrating perspectives that account for psychological needs, developmental dynamics and digitally mediated environments.”**

Prevention metrics should shift towards psychosocial functioning and wellbeing, including parenting quality, relationships, and externalising behaviour. Trauma informed, reintegration focused, and cross sectoral approaches are essential to address distress and social disconnection before violent trajectories consolidate.

**Conclusion**

Nihilistic violence and digitally mediated lone actor trajectories challenge conventional understandings of violent extremism. For many adolescents, violence represents less a political statement than an attempt to manage distress, grievance, and identity fragmentation in online environments that reward transgression and notoriety. Bridging the gap between mental health services and PCVE requires recognising these developmental and psychological realities. Grounding prevention in trauma informed care, digital understanding, and ethical cross sector collaboration offers a more proportionate and humane response to one of Europe’s most complex emerging security challenges.

**Aissa Bah**

Chief administrative medical officer, HUS Helsinki University Hospital | HUS Psychiatry

"Trauma informed, reintegration focused, and cross sectoral approaches are essential to address distress and social disconnection before violent trajectories consolidate."

## Library


1. Arain, M., Haque, M., Johal, L., Mathur, P., Nel, W., Rais, A., Sandhu, R., & Sharma, S. (2013). **Maturation of the adolescent brain**. *Neuropsychiatric Disease and Treatment*, 9, 449–461. https://doi.org/10.2147/NDT.S39776
2. Bah, A., & Lindberg, J. (2025). **Minustako terroristi? [I, a terrorist?]**. Helsinki: Warelia kustannus.
3. European Commission. (2026). **Digital Services Act (DSA)**. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act
4. EU Counter Terrorism Coordinator. (2025). **Nihilistic extremist violence: An emerging threat** (Council document 15477/25, LIMITE). Brussels: Council of the European Union.
5. Europol. (2025). **Intelligence Notification: The rise of online cult communities dedicated to extremely violent child abuse**. Europol Operations Directorate.
6. Europol. (2026). **Project Compass: First operational results against The Com network**. European Counter Terrorism Centre (ECTC).
7. Haghish, E. F., Obaidi, M., Strømme, T., Bjørgo, T., & Grønnerød, C. (2023). **Mental health, well being, and adolescent extremism: A machine learning study on risk and protective factors**. *Research on Child and Adolescent Psychopathology*, 51, 1699–1714. https://doi.org/10.1007/s10802-023-01105-5
8. Neumann, F. (2026). **Terrorism without a goal? The development of nihilistic violence**. Berlin: Konrad Adenauer Stiftung.
9. Rousseau, C., Miconi, D., Ngov, C., & Hassan, G. (2025). **Ideological and nihilistic violence in adolescents referred to a specialized clinic for violent extremism**. *Canadian Journal of Criminology and Criminal Justice,* 67(2), 30–48. https://doi.org/10.3138/cjccj-2024-0057
10. Windisch, S., Logan, M. K., & Simi, P. (2022). **Trauma, adversity and violent extremism: A systematic review**. *Behavioral Sciences of Terrorism and Political Aggression*, 14(2), 1–23.

# THE TRADE-OFF: ALGORITHMIC RADICALISATION FOR ECONOMIC GAINS

**“From a preventing violent extremism (PVE) lens, treating algorithmic radicalisation as a trade-off for economic gains could undermine the core principles of early intervention, resilience-building, and structural prevention that define effective counter-extremism strategies.”**

Algorithmic radicalisation—the subtle steering of digital citizens toward increasingly polarising or extreme content through engagement-driven systems—is a structural and predictable contributor of radicalisation. While platforms do not officially endorse algorithmic radicalisation as a trade-off—their (in)actions might effectively normalise it. From a preventing violent extremism (PVE) lens, treating algorithmic radicalisation as a trade-off for economic gains could undermine the core principles of early intervention, resilience-building, and structural prevention that define effective counter-extremism strategies. This insight argues that platforms might be aware of the dangers of radicalisation but deprioritise safety to protect profits. Finally, the article provides recommendations to address algorithmically driven pathways to radicalisation.

### Engineered Engagement and (Algorithmic) Radicalisation

Most platforms are economically incentivised to be addictive and their algorithms are engineered for engagement. Researchers observed, YouTube’s recommender systems “paint an alarming picture of online radicalisation: **not only Incel activity is increasing over time**, but platforms may also play an active role in steering [digital citizens] towards such extreme content.”

Researchers also indicate that, TikTok's recommender system is culpable of "pushing increasingly extreme content into the feed of new [digital citizens] after they've used the app for just 10 minutes." These examples reflect a structural pattern consistent with the definition of algorithmic radicalisation. Most concerningly, this *process mirrors established radicalisation pathways* and individuals with pre-existing grievances, identity insecurities, or social isolation are particularly vulnerable. Algorithms are influencing individuals, as platforms reinforce and normalise narratives, while isolating digital citizens from dissenting views and fostering echo chambers where extremist ideologies can take root and be exploited. Empirical studies show social media platforms could quarantine legal-but-harmful content, but are reluctant to deploy this type of intervention, as it could reduce engagement at the expense of commercial losses. Platforms' prioritisation of financial incentives over safety leaves individuals trapped on addictive content loops that enable radicalisation. So, if engagement and profiteering is prioritised over safety, then algorithmic radicalisation is a feature which can and should be appropriately addressed by platforms.

**Reactive Moderation: Limitations and Consequences**

Across both AI and social media platforms, "free speech" and "freedom of expression" are sometimes used to justify limited intervention, often serving as armor to shield algorithmic radicalisation. Harmful content is moderated only after dissemination, prioritising engagement and revenue over proactive safeguards

**"So, if engagement and profiteering is prioritised over safety, then algorithmic radicalisation is a feature which can and should be appropriately addressed by platforms."**

This creates a structural bias toward late-stage intervention, resulting in a conflict of interest: recommender systems fuel radicalisation, while transparency and accountability are treated as economic liabilities rather than ethical obligations. Institutional oversight is weakened, reducing content moderation to a trade-off between public safety and platform growth. For instance, some platforms participate in the Global Internet Forum to Counter-Terrorism - GIFCT's hash-sharing databases to manage Terrorist and Violent Extremist Content (TVEC), as part of a crisis response protocol, but these efforts focus on overt explicitly designated terrorist materials rather than a broader range of TVEC content that fuels upstream radicalisation. Scholars have documented, "The hash-sharing database doesn't regulate 'TVEC' by trying to change harmful online behaviour—it intervenes in global data flows infrastructurally to make sure '*things don't even hit the surface*'." From an optics perspective, this visually manages enforcement by targeting symptoms; however, it is not effectively addressing the normalisation of violent and extreme content stemming from algorithmic radicalization. From a PVE lens, reactive moderation fails to address the upstream drivers of radicalisation, such as: misogyny, conspiracy theories, and grievance narratives. It does not build resilience, promote critical thinking, nor provide alternative narratives. Instead, it reinforces a cycle of suppression and backlash, and does little to prevent individuals from entering extremist pipelines in the first place.

**"From a PVE lens, reactive moderation fails to address the upstream drivers of radicalisation, such as: misogyny, conspiracy theories, and grievance narratives."**

**Power Asymmetry: Reduced Agency is Operationally Convenient**

From a structural standpoint, platforms rarely treat the risk of radicalisation as a core business failure because monetising engagement is their primary objective. Platforms implement piecemeal interventions but do not challenge incentive structures or power imbalances, implicitly tolerating harms to vulnerable digital citizens as long as engagement and revenue remain strong. For platforms, the millions of people vulnerable to algorithmic radicalisation are still an *unquantifiable minority*, thus, seen as a trade-off. This estimate fails to account for the compounding harms caused to numerous individuals and communities impacted by actual real-world violence. Moreover, generative AI systems introduce similar risks, where researchers have raised concerns about how AI chatbots respond to self-harm or violence-related prompts, particularly during extended interactions where safety guardrails degrade. Since billions of people use social media and hundreds of millions interact regularly with generative AI systems, even a small fraction exposed to radicalisation pathways translates into *millions of at-risk individuals*. Yet, these digital citizens are often treated as *statistically negligible*—rendered invisible within profit-driven calculations.

Platforms create asymmetric dynamics due to structural imbalances. For example, digital citizens rarely see how algorithmic radicalisation functions in real-time or how their data influences exposure to harmful content. By controlling recommender systems that are responsible for algorithmic radicalisation, platforms gain significant power to influence the information digital citizens see and interact with online. On the other hand, digital citizens have no-to-low transparency or control over how their data is used, creating an imbalance between platforms' decision-making and individual autonomy. Regrettably, this is further exacerbated as "opt-out" mechanisms, (when they exist) are buried or require substantial digital literacy.

This power imbalance is further heightened by two interrelated factors: first, algorithmic radicalisation is structural and second, algorithmically driven systems contribute to making radicalisation feasible, as it continuously exposes digital citizens to influence-oriented information, undermining space for genuine deliberation and reflection. Here, the power dynamic is subtle: platforms do not assume digital citizens lack agency, but where agency exists, it is systematically weakened by default settings, opaque personalisation, and asymmetric knowledge. The problem is that platforms make reduced agency operationally convenient, choice, is formally preserved while being structurally sidelined. Recognising this distinction avoids technological determinism while highlighting power imbalances in curated digital ecosystems.

"The problem is that platforms make reduced agency operationally convenient, choice, is formally preserved while being structurally sidelined."

**Recalibrating Economic Trade-offs and Algorithmic Radicalisation**
Platforms must recalibrate from economic trade-offs and algorithmic radicalisation to true accountability, to disrupt this cycle. For example, platforms insinuate radicalisation is a result of individual choice, susceptibility, or moral failure, when it should be recognised as a predictable outcome stemming from an algorithmic radicalisation. Because platforms transfer responsibility onto digital citizens and away from algorithmic radicalisation, this narrative preserves the legitimacy of platforms' business models by casting radicalisation as exceptional and individualised. This status quo allows platforms to be both culprit and comforter, simultaneously.

"Platforms must recalibrate from economic trade-offs and algorithmic radicalisation to true accountability, to disrupt this cycle."

**Conclusion**
Economic trade-offs have real consequences: radicalised individuals, fractured communities, and weakened democracies. PVE demands rejecting the notion of algorithmic radicalisation as an unavoidable harm. It means building resilience, fostering safer communities, and embracing a future where digital citizens are endowed with agency, not stripped of it. Algorithmic radicalisation is not inevitable, and platforms can be reshaped for societal cohesion and safe(r) digital ecosystems.

Gazbiah Sans
Founding CEO, PVE Works

# THE HIDDEN INFLUENCE ON AI: WHY LLM GROOMING MATTERS FOR EUROPE

Artificial intelligence is rapidly becoming a central gateway to information for policymakers, institutions, and citizens alike. Large language models (LLMs) are increasingly used to summarise, interpret, and generate knowledge. At the same time, they are contributing to a growing "epistemic crisis": a gradual weakening of our collective ability to distinguish reliable knowledge from misleading or manipulated information.

A new and still underexplored driver of this development is **LLM grooming** — the deliberate shaping of the online information environment to influence what AI systems learn and communicate. Research shows that these systems are vulnerable across their entire lifecycle, from training data to external knowledge sources.

> "Artificial intelligence is no longer something on the sidelines – it is part of how people communicate, access information, and form opinions, especially in areas linked to public debate and democratic resilience."

In my work at Textgain, a spin-off from the University of Antwerp, I see these dynamics playing out more and more clearly. Artificial intelligence is no longer something on the sidelines – it is part of how people communicate, access information, and form opinions, especially in areas linked to public debate and democratic resilience.

At Textgain, we develop AI systems to detect hate speech, disinformation, and harmful narratives across all EU languages. This work spans both major platforms and more fringe online spaces, and is closely aligned with European frameworks such as the Digital Services Act (DSA), the AI Act, and the GDPR.

What becomes clear in practice is that the challenge is shifting. It is not just about analysing individual posts anymore. The real question is how narratives take shape, gain traction, and continue to circulate – and how those same dynamics increasingly influence the information environments that AI systems rely on.

**From Influencing People to Shaping AI-Driven Information**

Misinformation has long been recognised as a societal challenge. Its impact on public opinion and democratic processes is well documented. What is changing is where this takes place. Instead of targeting individuals directly, actors increasingly shape the broader information environment on which AI systems rely. By producing large volumes of coordinated and search-optimised content – often presented in credible formats – they increase the likelihood that these narratives are reflected in AI-generated outputs. Recent investigations illustrate how such ecosystems operate in practice.

**The Shift to Narrative Shaping**

Misinformation does not need to be clearly false to be effective. Repetition, familiarity, and internal consistency can make information appear credible, even when it is misleading.

LLM grooming builds on these mechanisms. Rather than spreading isolated false claims, it gradually shapes how topics are framed. Certain perspectives become more visible, others less so, and over time a particular narrative can begin to feel dominant.

**"It is not just about analysing individual posts anymore. The real question is how narratives take shape, gain traction, and continue to circulate – and how those same dynamics increasingly influence the information environments that AI systems rely on."**

For AI systems, this creates a more subtle risk. Outputs may be fluent and balanced in tone, while still reflecting a skewed representation of reality. For policymakers, this makes the challenge more complex: it is no longer only about identifying incorrect information, but about recognising when knowledge itself is being (re)shaped in a systematic way.

**New Vulnerabilities in Retrieval-Based AI Systems**

These risks become more pronounced with the rise of systems that retrieve information in real time. Retrieval-augmented generation (RAG) allows AI models to draw on external sources while generating responses. While this improves relevance, it also introduces new dependencies.

If those sources are manipulated, the model can reproduce that manipulation without any change to its internal design. Research on "knowledge poisoning" demonstrates how such interventions can influence outputs by targeting the information supply chain itself. In that sense, RAG systems can enable faster and more scalable forms of manipulation, as influence shifts upstream to the sources being retrieved.

At the same time, RAG introduces an important structural advantage over traditional LLMs. Because responses can be linked to the specific sources they are derived from, these systems are inherently more transparent.

Unlike standalone models – which can generate fluent outputs without any visibility into why certain information is presented as true – RAG-based systems can provide traceability and source-level accountability to the end user. This creates a critical opportunity: while the attack surface increases, so does the capacity for verification and auditability.

More broadly, studies indicate that digital information environments are already linked to increased polarisation and declining trust in institutions. AI systems that draw on these environments risk amplifying these dynamics further – making it essential not only to secure the information supply chain, but also to ensure that transparency mechanisms are meaningfully exposed to users.

**Implications for Policy and Governance**
For policymakers, this points to a gradual but important shift. The focus can no longer be limited to individual pieces of content or isolated incidents. Instead, attention needs to move towards the conditions under which knowledge is produced and circulated.

Solutions suggest that addressing misinformation requires a combination of analytical methods, contextual understanding, and institutional safeguards. This aligns with the need for structured monitoring of information environments.

**"For policymakers, this makes the challenge more complex: it is no longer only about identifying incorrect information, but about recognising when knowledge itself is being (re)shaped in a systematic way."**

In this context, specialised and transparent AI approaches become increasingly relevant. Initiatives such as the European Observatory of Online Hate (EOOH) and Textgain's CaLICO Large Language Model focus on multilingual analysis, expert-informed annotation, and the detection of patterns rather than isolated content. The emphasis is on identifying trends, coordinated behaviour, and emerging risks at an early stage.

This approach aligns with European priorities, including the Digital Services Act, and broader efforts to address disinformation and foreign information manipulation and interference (FIMI) while maintaining strong standards for data protection and transparency.

**Lessons Learned**

- Influence is no longer aimed only at people, but increasingly at the AI systems they rely on.
- The process is subtle: narratives are shaped over time rather than through obvious falsehoods.
- Real-time AI systems depend on external information sources, which introduces new vulnerabilities.
- Outputs may sound convincing without being reliable.
- Mitigation depends on structured, transparent, and accountable AI design.

**"LLM grooming can be understood as a next step in the evolution of disinformation. It does not replace earlier forms but adds a new layer by targeting the systems that increasingly mediate knowledge."**

**Conclusion**
LLM grooming can be understood as a next step in the evolution of disinformation. It does not replace earlier forms but adds a new layer by targeting the systems that increasingly mediate knowledge.

Research shows that misinformation is persistent and that digital environments can affect trust and cohesion. The addition of AI systems introduces new pathways through which these effects can spread and scale.

For Europe, the challenge is therefore not only to manage information risks, but to ensure that AI systems remain reliable and trustworthy intermediaries. This requires attention to governance, transparency, and the design of systems that are fit for purpose in sensitive domains.

With information widely available but trust and certainty under pressure, improving how knowledge is produced and interpreted is a key policy challenge.

**Gijs Van Beek**
Co-Founder and researcher, CBDO

“For Europe, the challenge is therefore not only to manage information risks, but to ensure that AI systems remain reliable and trustworthy intermediaries.”

## Library

1. Tianzhe Zhao, Jiaoyan Chen, Yanchi Ru, Haiping Zhu, Nan Hu, Jun Liu, Qika Lin, Exploring knowledge poisoning attacks to retrieval-augmented generation, Information Fusion,Volume 127, Part C, 2026, 103900, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2025.103900.
2. Zhao, T., Chen, J., Ru, Y., Zhu, H., Hu, N., Liu, J., & Lin, Q. (2025). RAG Safety: Exploring Knowledge Poisoning Attacks to Retrieval-Augmented Generation. ArXiv. https://arxiv.org/abs/2507.08862
3. Anthropic reveals that as few as '250 malicious documents' are all it takes to poison an LLM's training data, regardless of model size, by Jess Kinghorn published 16 December 2025 on PC Gamer. Link here
4. Textgain website, www.textgain.com
5. European Observatory of Online Hate Link here
6. CaLICO: The world’s first multilingual foundation model to track harmful content, Textgain Link here

# WIKIPEDIA, AI AND DISINFORMATION: STRATEGIC NARRATIVE CONTROL IN A DIGITAL BATTLE OF IDEAS

In today's digital age, knowledge is power—and platforms like Wikipedia play a central role in shaping how that knowledge is formed and consumed. It serves as a first point of reference for journalists, policymakers, researchers, and the public. At the same time, it has become increasingly influential in shaping artificial intelligence systems (AI), which rely on widely available online content to generate knowledge and interpretations.

This centrality has turned Wikipedia into a strategic target. In politically sensitive fields—particularly those related to political Islam (Islamism) and extremism research—the platform is no longer just an encyclopaedia. It has become a contested space in a broader "battle of ideas," where narratives are shaped, challenged, and strategically influenced. In some cases, these dynamics are not random but reflect structured methods that can be exploited by determined actors.

For example, in the Arabian Peninsula, the United Arab Emirates has emerged as a leading actor in confronting extremist Islamist movements such as the Muslim Brotherhood. Within this broader ideological conflict, research on Political Islam has increasingly become part of a highly polarised online environment in which UAE-affiliated think tanks and scholars—as well as other researchers working on related topics—are frequently exposed to reputational attacks and hostile digital campaigns.

Activist-oriented platforms such as the Bridge Initiative's "Fact Sheets" illustrate how respected researchers on Islamism can be portrayed alongside known far-right extremists in ways that blur fundamental intellectual and political distinctions and shape public perceptions. Those "Fact Sheets" have also found their way into the "Sources" section of various Wikipedia articles, books or online content, despite their patent framing.

**A Hybrid Battlefield of Narratives**
Wikipedia's open editing model allows broad participation, but it also enables small groups of highly active editors to exert disproportionate influence over how topics are framed. Direct falsehoods are relatively rare. Instead, influence typically operates through more subtle and methodical techniques.
These include:

- selective use of sources,
- omission of contextual information,
- strategic quotation of material that supports a preferred interpretation.

This practice—often described as "cherry-picking"—does not necessarily violate formal rules.[1] However, when applied consistently over time, it can gradually reshape how a topic is understood.

[1] See Wikipedia Guidelines on „Reliable Sources", "Neutral Point of View" or "Verifiability": https://en.wikipedia.org/wiki/Wikipedia:Reliable_sources?utm_source=chatgpt.com as well as https://en.wikipedia.org/wiki/Wikipedia:Neutral_point_of_view?utm_source=chatgpt.com and https://en.wikipedia.org/wiki/Wikipedia:Verifiability?utm_source=chatgpt.com

The result is not a single act of disinformation, but a cumulative reframing of knowledge. Such patterns are particularly effective because they remain below the threshold of obvious manipulation. They reflect a method: incremental, persistent, and difficult to detect in isolation.

**Terminology as a Strategic Tool**
One of the most consequential battlegrounds is terminology. In it of itself, terminological debates around concepts and phenomena are core to academia and a necessary discussion. However, there is a clear distinction between Islam as a religion and Islamism (or political Islam) as a political ideology. This distinction is essential for analytical clarity. Editorial disputes often revolve around attempts to blur this boundary regardless.

Replacing references to "Islamism" with broader references to "Islam" may appear minor, but it fundamentally alters the framing. It shifts the discussion from a specific ideological movement to a general religious context. These shifts are rarely accidental. They reflect a broader struggle over definitions—one in which language becomes a strategic instrument for shaping perception. Researchers examining extremist Islamist movements may therefore find their work reframed or their public profile repositioned within an entirely different ideological context.

This has further significant implications. For example, describing the Muslim Brotherhood primarily as an 'Islamic' rather than an 'Islamist' movement changes how the organisation is perceived.

**"The result is not a single act of disinformation, but a cumulative reframing of knowledge."**

The Brotherhood is commonly regarded as an extremist Islamist movement that may take different forms—violent or non-violent—depending on national context. While scholarly interpretations vary, in most interpretations it remains a highly problematic, anti-pluralistic and anti-democratic actor that has often times sought to shape 'Muslim life' in Europe according to its own ideological views. Reframing it from an Islamist to a broader Islamic movement fundamentally weakens the analytical distinction between religion and extremist ideology—an outcome that certainly aligns with the strategic interests of the Brotherhood and its sympathisers, which may raise questions about the motivations behind.

**Discrediting Researchers in the Battle of Ideas**

The contest is not limited to concepts and terminology. It also extends to the portrayal of researchers and institutions working on political Islam and extremism. In some cases, scholars are framed less through their research and more through accusations of bias or labels such as "Islamophobic", "controversial", or "far-right" and so forth. While academic critique is legitimate and necessary, the systematic foregrounding of such labels can function as a reputational strategy.

The effect is a shift in focus: away from empirical findings and toward questions of legitimacy. In a digital environment where Wikipedia entries rank highly in search results, this framing can influence how journalists, policymakers, and the public perceive entire research fields. From the perspective of information dynamics, this resembles a classic tactic in ideological conflict: not only contesting ideas, but also undermining those who produce them.

"The effect is a shift in focus: away from empirical findings and toward questions of legitimacy. In a digital environment where Wikipedia entries rank highly in search results, this framing can influence how journalists, policymakers, and the public perceive entire research fields."

**Method, Not Coincidence: Incremental Influence Campaigns**

Research on digital influence operations suggests that effective campaigns rarely rely on overt manipulation. Instead, they follow gradual, methodical approaches.

Typical characteristics include:

- small, incremental edits that avoid attention,
- reliance on formally acceptable sources, even if highly selectively used,
- persistence over time to stabilise specific framings.

Such strategies can be employed by a range of actors, including politically motivated groups, advocacy networks, or professional communication actors. The key point is not necessarily coordination in every instance, but the existence of a method that can be used to shape knowledge environments. Once a particular framing becomes established—supported by citations and repeated across articles—it gains resilience. Correcting it becomes increasingly difficult, especially as it is perceived as "consensus knowledge."

**Amplification Through Artificial Intelligence**

The rise of artificial intelligence adds a new dimension to these dynamics. AI systems increasingly act as intermediaries between users and information. Their outputs are shaped by patterns found in widely accessible sources—among which Wikipedia plays a central role. This creates a multiplier effect. Narratives that become dominant within Wikipedia are not confined to the platform.

"The rise of artificial intelligence adds a new dimension to these dynamics."

They can influence how AI systems:
- summarise political movements,
- explain ideological concepts,
- contextualise researchers and institutions.

In this sense, influencing Wikipedia is no longer just about shaping a single article. It is about shaping the informational ecosystem itself—including how both humans and machines understand complex issues.

**Lessons Learned**
- **Digital platforms are strategic battlegrounds:** Wikipedia's influence makes it a key site for ideological contestation.
- **Subtle methods are highly effective:** Incremental edits and selective sourcing can reshape narratives without obvious rule violations.
- **Terminology matters:** Small linguistic shifts can fundamentally alter how complex issues are understood.
- **Reputation is a target:** Discrediting researchers is a strategic tool in broader information conflicts.
- **AI amplifies narratives:** Once established, dominant framings are reinforced and scaled through artificial intelligence systems.
- **Method over coincidence:** These dynamics often follow structured, repeatable patterns rather than isolated actions.

**The Struggle Over Knowledge**
Wikipedia remains a remarkable and indispensable knowledge project. Yet its importance also makes it vulnerable to strategic influence.

"Influencing Wikipedia is no longer just about shaping a single article. It is about shaping the informational ecosystem itself—including how both humans and machines understand complex issues."

In contested fields such as political Islam, the platform has become part of a broader arena in a conflict of ideas.

What emerges is not a simple story of misinformation, but a more complex reality: a structured and ongoing contest over how knowledge is framed. Terminology, source selection and reputational narratives become tools in a wider struggle—one that includes attempts to discredit researchers and institutions alongside efforts to reshape conceptual understanding.

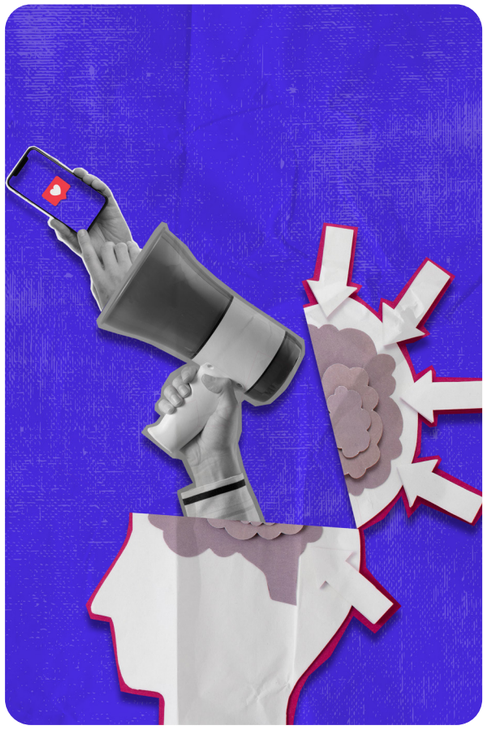
In an era where both human audiences and artificial intelligence rely heavily on digital knowledge platforms, these dynamics carry far-reaching consequences. Understanding Wikipedia as part of an information battlefield is therefore essential. Safeguarding plurality, transparency, and methodological integrity is not only a technical challenge, but a central task in preserving open and informed democratic discourse.

"Safeguarding plurality, transparency, and methodological integrity is not only a technical challenge, but a central task in preserving open and informed democratic discourse."

**Ferdinand J. Haberl**
Deputy Director, Documentation Centre Political Islam and Thematic Panel 4 on "Local Dimension, Polarisation and Resilience" Co-Leader

## Library

1. NATO Innovation Hub. (2020). Cognitive Warfare. Norfolk, VA: Allied Command Transformation.
2. Hikes-Wurm, D., & Sagawa-Krasny, M. (2025). Hybride Bedrohungen. In: ISS Lagebild 3/25. Wien: BMLV.
3. Reagle, J. M. (2010). Good Faith Collaboration: The Culture of Wikipedia. Cambridge, MA: MIT Press.
4. Österreichischer Fonds zur Dokumentation von religiös motiviertem politischen Extremismus (Dokumentationsstelle Politischer Islam). (2025). Jahresbericht 2024. Wien.



# THE STRATEGIC ADVANTAGE OF 'STUPID': WHAT PCVE PRACTITIONERS SHOULD LEARN FROM LOW-TECH EXTREMIST CONTENT ONLINE

**“For PCVE practitioners, the key question is not whether content is technologically advanced. It is whether the message, messenger, format, and platform fit the target group closely enough to resonate.”**

*Current debates on extremism online often focus on AI and deepfakes. These matter. But much extremist communication is effective for simpler reasons: it signals authenticity, belonging, and accessibility to the target group. It is the online version of a schoolyard or town square conversation. For PCVE practitioners, the key question is not whether content is technologically advanced. It is whether the message, messenger, format, and platform fit the target group closely enough to resonate. Policymakers should consider supporting agile Strategic Communications laboratories and networks.*

**“We do not see things as they are, we see them as we are.”**
Anaïs Nin’s line captures a core difficulty for prevention and countering violent extremism (PCVE): people rarely respond to “objective facts” as such. Especially when values are concerned, we respond to information as filtered through identity, emotion, and group loyalty. Research on motivated reasoning suggests that we often defend the views that protect our group and our sense of self. Extremist and terrorist propaganda exploits these dynamics. It defines what is wrong, identifies who is to blame, and frames what must be done and who should act. In doing so, it draws a sharp line between “us” and “them” and then offers the individual a role within that struggle: to belong, to defend the group, and, potentially, to become a hero. In that sense, such propaganda can function as a tribal call to arms.

**The Online Version of a Schoolyard Conversation**
If people interpret information through identity and group loyalty, content that signals in-group authenticity may be as, or even more, persuasive than polished but socially distant communication. That helps explain why “stupid”- looking, low-fidelity (low production value) content can work so well. A post with spelling mistakes, a shaky clip, or a crude meme may not look impressive. But it lowers the perceived barrier to entry. It suggests that belonging does not require expertise. And it makes the messenger appear to be one of “us,” not above the audience. In that sense, low-tech and low-fidelity can be an advantage. It can make content feel more real and relatable.


Example of a recruitment post by an extreme-right youth group in Germany, containing numerous spelling and grammatical errors while calling for others to join and disparaging the “competition.” (TikTok, November 2025)

Simple slogans like “*join us, we are 50 comrades*” or “be one of us” with spelling errors **implicitly** say:

- **Low entry barrier** (“you don’t have to be special to join”),
- **No ideological exam required**
- **Low-fidelity** aesthetics can **signal** *“We are like you!”*
- **Authenticity, relatability** and **quantity** can matter more than production **quality**

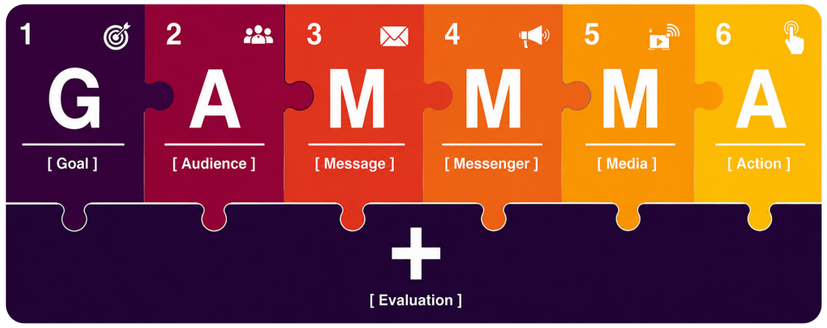

Screenshot from a recruitment video of an extreme-right youth group in Germany, signaling identities including an extreme-right party (AfD), a football hooligan group, East-German (Flag of former socialist Germany), “Fuck (Chancellor) Merz” (FCKMRZ), Good night left-side (anti-Antifa violence), with calls to action such as: You Only Live Once (YOLO), Now or Never, as well as companionship. (TikTok, November 2025)

The most important role of high-tech in such low-tech and low-fidelity cases is that of algorithmic amplification by social media platforms. Once a person really looks at such content, the algorithm will suggest more of the same. The business-model, which is designed to keep people engaged as long as possible so the social media companies can sell targeted advertisements, also helps extremists and terrorist to reach their target groups online. Low-tech and low-fidelity meet low-cost.

**Learnings for Effective PCVE Strategic Communication Efforts**

Many PCVE strategic communication (Strategic Communications) efforts have missed the mark because they tried to learn from professional advertising or to compete with some of the high-fidelity extremist or terrorist propaganda. Extremist or terrorist propagandists, however, do not need every piece of content to be good. They need good-enough pieces, pushed often enough, with the right emotional tone, authentic, relevant, and accessible. Low-tech and low-fidelity content can be produced fast, tested fast, and changed fast. Over time, a steady stream can normalise grievances, othering, and calls to action, long before a formal campaign by PCVE Strategic Communications project has started production.

The EU GAMMMA+ toolkit highlights that narrative effectiveness does not start with the most sophisticated tool, but with fit: fit between *the goal, the audience, the message, the messenger, the medium*, and the action you want people to take.




The toolkit is explicit that campaigns can work when they understand the target audience in depth, use messages that resonate with that audience's needs, rely on messengers the audience sees as credible, and communicate on the platforms the audience actually uses. It also states that StratCom needs to be co-created with members of the target groups. Finally, a constant stream of good-enough content can matter more than polished production, and authenticity and quantity may be more relevant than high-fidelity technical quality.

In other words, the key question for effective narratives is not really whether something is high-tech and high-fidelity, or low-tech and low-fidelity, but whether the chosen level of technology and sophistication matches the audience's language, habits, grievances, and social environment closely enough to reach and move them.

**Develop the Planner, not Only the Plan**

There is a planning and operational challenge here. If the extremist and terrorist environment is fluid and opportunistic, PCVE Strategic Communications needs a lighter and faster rhythm. Research on narrative creativity suggests that in volatile and uncertain environments, effective action depends less on refining static plans than on strengthening the practitioner's capacity to scan for what seems to work right-now: Test pieces of content. Adapt fast. Repeat. Develop the planner, not only the plan.

**"The business-model, which is designed to keep people engaged as long as possible so the social media companies can sell targeted advertisements, also helps extremists and terrorist to reach their target groups online."**

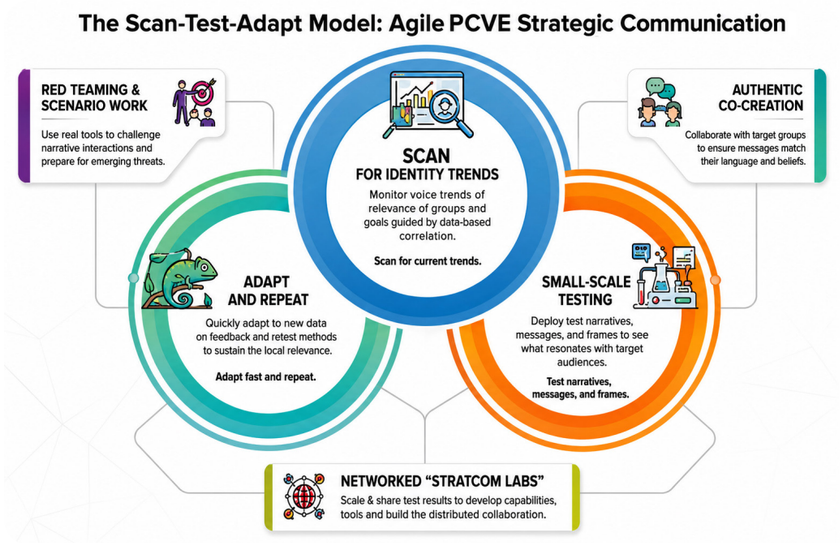
Such a scan–test–adapt model is not just a slogan. It would change what many PCVE Strategic Communications teams do day to day. It means live-monitoring new blends of grievance and identity, and testing narratives, messengers, and formats on a small scale. It means using red teaming and scenario work, so that PCVE Strategic Communications practitioners are continuously engaged and prepared for novelty and ambiguity, not just yesterday's narratives. This could be done through agile Strategic Communications "laboratories". In practice, these could take the form of multidisciplinary units that monitor trends, run limited message tests, review results in short cycles, and distribute their findings to practitioners and policymakers in a timely manner.

### We See Things as We Are

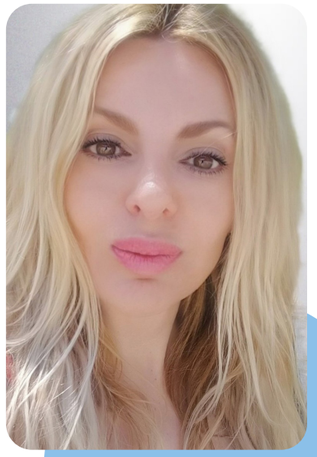
And there is another challenge. If people see the world through identity and group loyalty, institutions and CSOs do too. PCVE policy makers and practitioners are not outside the problem. Professional habits, threat categories, and political incentives shape what gets noticed and what gets missed. That is why self-reflection matters. For policy makers this means: PCVE StratCom teams need space to challenge assumptions with enough freedom to question their own perspectives.

**"If people see the world through identity and group loyalty, institutions and CSOs do too. PCVE policy makers and practitioners are not outside the problem."**

A network of PCVE StratCom "laboratories" on the national and EU level could be a way to facilitate that. They could reflect assumptions, share tools, warning indicators, and tested formats, while preserving flexibility for different hyper-local contexts. Many extremists and terrorists think in networks. It takes a one to beat one.




**Alexander Ritzmann**
Senior Advisor and researcher with the Counter Extremism Project (CEP)



# NEW TRENDS IN ONLINE RADICALISATION

A chat with

**Eva María Jiménez González**

Head of Department / Doctor of Clinical and Forensic Psychology, Forensic Psychology Institute (Ministry of Justice)

**1. Introduce yourself and your work in the fields of radicalisation, and PVE.**

I am a Psychologist with a PhD in Clinical-Forensic Psychology and two Masters specialised in International Security and Counterterrorism. My work sits at the intersection of mental health, security, and prevention of violent extremism (PVE), with a strong focus on translating research into practical tools for policymakers and frontline practitioners.

I currently serve as Head of the Institute of Forensic Psychology at the Spanish Ministry of Justice and work as a senior expert in prevention and countering of violent extremism (PCVE) for several European Union and Council of Europe initiatives. In this capacity, I have led and contributed to projects across a wide range of regions, including the Western Balkans, Türkiye, Central Asia, the MENA region, the Sahel, and Latin America. My work primarily involves supporting national authorities and local stakeholders in developing evidence-based policies, as well as delivering specialised trainings.

A central component of my professional trajectory has been the integration of mental health perspectives into PCVE. Through my involvement with international organisations, including also contributions to United Nations (from the Psychological Support Unit and Peacekeeping-related initiatives), I have worked to strengthen the understanding of how psychological vulnerabilities, trauma, and psychosocial factors intersect with radicalisation processes. This approach is particularly relevant for improving early detection, risk management, and tailored interventions for individuals at risk.

In addition to my policy and operational work, I am actively engaged in academia. I direct and teach in postgraduate programmes on forensic psychology and terrorism at international universities, where I focus on bridging the gap between research, policy, and practice. This dual role allows me to contribute to capacity-building efforts while also ensuring that emerging evidence and field-based insights inform training and strategic development.

Over the years, I have collaborated closely with European Commission initiatives, including practitioner networks and policy support frameworks, where I have contributed to advancing knowledge exchange and the development of practitioner/policymaker-oriented guidance

My experience has also included the positions of Co-Chair and Ambassador from RAN Practitioners, and Task Leader from RAN Policy Support, and senior expert/trainer for the EU Knowledge Hub, covering work on mental health within PCVE settings and supporting multidisciplinary approaches that bring together law enforcement, judicial actors, stratcomms, mental health professionals, and social services.

Overall, my work is driven by the objective of enhancing the effectiveness, coherence, and sustainability of PCVE responses. This involves promoting integrated approaches that are sensitive to local contexts, grounded in human rights, and responsive to the increasingly complex and hybrid nature of radicalisation dynamics. I am particularly committed to ensuring that P/CVE experts are equipped with the tools, knowledge, and frameworks needed to address evolving risks in both offline and digital environments.

**2. What experiences inspired you to do this work?**
My interest in prevention and countering violent extremism (PCVE) originates from my doctoral research, which focused on the evaluation and potential intervention with individuals involved in terrorism and radicalised populations, primarily in the context of ETA-related and early jihadist threats in Spain.

Being Spanish, it was a phenomenon with which, unfortunately, we were very familiar, and from my perspective as a forensic psychologist, I really wanted to understand why individuals engaged in terrorism and extreme violence behaved the way they did, including the factors that led them to adopt radical views, how they came to dehumanise and attack those who did not share those views, and what motivations drove them to act. From that point, I became deeply engaged with the PCVE field, recognising early on the importance of combining rigorous psychological assessment with broader security and policy perspectives.

Since 2014, I have been fully dedicated to PCVE. That year, I had the opportunity to lead a European Union-funded project in Türkiye (DEPAR), which allowed me to engage directly with operational challenges and policy development in a highly complex context. This experience reinforced my commitment to advancing evidence-based approaches that can be applied both at strategic and operational levels.

Over the years, I have witnessed how global crises, particularly since the COVID-19 pandemic, have amplified populist and extremist positions.

I consider myself privileged to have contributed to national initiatives (such as the Spanish's most recent ENCOT-The National Counterterrorism Strategy), as well as to international work under the United Nations, the Council of Europe, and the European Commission. My participation in multidisciplinary working groups addressing crises such as foreign terrorist fighters in Syria, designing preventive psychosocial policies to combat polarisation in the face of the Russian invasion of Ukraine or the Israeli-Palestinian conflict, and regional challenges in MENA region and the Western Balkans, have strongly impacted my understanding on the importance of multiprofessional perspectives, the exchange of operational insights, and the inclusion of psychosocial variables as integral components of P/CVE policies and frameworks.

Working with victims of terrorism has also been profoundly influential in shaping my perspective. It has allowed me to understand violent extremism not solely through a security lens, but also in terms of prevention, resilience, and repair. This three-pronged approach (on perpetrators, at-risk populations, and those affected by violence), has solidified my conviction that effective PCVE

strategies must be holistic, context-sensitive, and inclusive of vulnerable populations, particularly minors and those previously affected-induced by deficiencies, unmet needs, or a wide variety of unresolved issues, who remain central to any preventive efforts.

In essence, my motivation to engage in this work stems from a combination of research inquiry, operational engagement, policy development, and human-centred practice. Each of these experiences has reinforced my belief in the necessity of integrating psychological, social, and security considerations into comprehensive and tailored PCVE approaches that are both practical for frontline practitioners and actionable for policymakers.

**3. In "The Hub. Voices" podcast episode on Minors and Radicalisation, you spoke about "emotional pain" as a driver. In the 2026 digital landscape, how are extremist groups weaponising the "loneliness epidemic" or personal grievances to offer a false sense of "belonging" online?**

In the current digital landscape, what we are observing is a very sophisticated evolution in how extremist actors identify, approach, and engage vulnerable individuals, particularly young people experiencing loneliness, frustration, social disconnection, identity uncertainty, an unmet need for validation, or a lack of recognition.

So, what I referred to as “emotional pain” is not incidental; it is increasingly being used as a deliberate entry point.

Extremist groups are highly adept at identifying and exploiting these vulnerabilities. Rather than starting with ideology, they often begin with emotion. Through online platforms, they observe and target expressions of grievance, isolation, or perceived injustice. Once these signals are detected, engagement becomes highly personalised. Individuals are approached, directly or indirectly, with messages that validate their feelings: that their loneliness is understandable, that their frustration is justified, and that their sense of being “different” or “excluded” is not only real, but shared.

This is where the manipulation becomes particularly effective. These groups offer what can be described as a “false belonging”, a constructed sense of community that appears to respond directly to the individual’s unmet needs. The messaging often includes narratives such as “we have been where you are”, “we understand you”, or “here, you will not be ignored”. For someone in a vulnerable state, this form of recognition and fellowship can be extremely powerful.

At the same time, technological dynamics significantly amplify this process. In these environments, individuals are not only consuming content but also receiving social reinforcement from perceived peers, which accelerates identity formation around these narratives. I mean, a critical element of this process is the reframing of personal grievances as collective or systemic injustices. For example, feelings of rejection or isolation may be reinterpreted through misogynistic narratives, as seen in incel-related environments, or through broader conspiracy frameworks that attribute personal difficulties to societal or political structures. This reframing provides not only a sense of belonging, but also a moral justification for violence against those who are not like me.

Importantly, extremist actors do not simply validate grievances, they offer “solutions”. These are often simplistic, immediate, and unrealistic, but they are presented in a way that is emotionally compelling. They function as what could be described as “siren calls”: promises of belonging, recognition, purpose, and even status. For individuals experiencing vulnerability, such offers can be very difficult to resist, precisely because they appear to address both emotional and existential needs in a direct and accessible way.

Over time, this dynamic can lead to a progressive narrowing of perspective. The individual becomes more embedded in a community that reinforces their worldview, reduces exposure to alternative narratives, and strengthens in-group identification. What began as a search for connection can evolve into deeper ideological alignment, and in some cases, into acceptance of harmful or violent positions

**4. In the digital space, where slang and memes evolve daily, how can practitioners distinguish between "edgy" adolescent rebellion and a genuine descent into extremist ideology?**
It is important to underline that these two phenomena are not entirely separate. In fact, the first one often builds upon the second. The search for alternative narratives, the rejection of a world perceived as not understanding them, and the tendency to adopt more extreme or oppositional positions are all characteristic of adolescence. These behaviours and attitudes can also represent the early stages of radicalisation processes, both in minors and adults. In this sense, expressions that are transgressive or fall outside what is considered normative should not automatically be interpreted as problematic; they are often part of natural identity development and social positioning.

The key distinction lies in when these behaviours shift from being a “means” of expression to becoming an “end” in themselves. Adolescent rebellion is typically exploratory, situational, and often temporary. However, when the objective evolves into a sustained effort to destabilise, attack, or oppose perceived “others” (whether individuals, groups, or entire systems), this may signal a transition towards more concerning dynamics. At this stage, grievances are no longer episodic or context-dependent, but rather become central to the individual’s worldview, often framed in rigid, polarised terms.

Another important differentiating factor is the pattern of manifestation over time. Adolescent rebellious behaviours tend to fluctuate in intensity and frequency; they are episodic, context-driven, and often inconsistent. In contrast, engagement with extremist ideologies typically shows a gradual but consistent increase in both intensity and frequency. The individual’s narratives, attitudes, behaviours, and online activity become more structured, repetitive, and ideologically aligned over time.

The modality of these expressions also differs significantly. Adolescent rebellion is often highly individualised and personal. Conversely, processes of radicalisation are strongly shaped by group dynamics, particularly in online environments. These are not spontaneous developments, but rather processes that are actively facilitated, modelled, and reinforced within digital communities, forums, and networks. Peer validation, group consensus, and algorithmically amplified content all play a critical role in consolidating these trajectories.

Memes and digital language are a particularly relevant example in this context. Today, a wide range of actors, including brands and political campaigns, use memes as tools to engage audiences, simplify narratives, and increase relatability. Their effectiveness lies in their accessibility, humour, and cultural resonance. However, these same characteristics also make them powerful instruments for manipulation. Extremist groups strategically adopt meme culture to normalise harmful narratives, gradually introduce ideological content, and lower the threshold for engagement, particularly among younger audiences.

For practitioners, the challenge is therefore not to focus solely on the presence of certain symbols, language, or humour, but rather on their function and trajectory. When such content serves to progressively isolate individuals from their immediate environments (family, peers, community), reinforce “us versus them” mentalities, legitimise hatred, or encourage mobilisation, it moves beyond the realm of normative adolescent behaviour and psychology (emotions, reactions, etc.). At that point, it becomes indicative of structured recruitment and indoctrination processes.

Ultimately, distinguishing between these phenomena requires a longitudinal and contextualised assessment. It is less about isolated behaviours or rebellious attitudes, and more about patterns, intent, and the broader psychosocial dynamics surrounding the individual (whether minor, adolescent or adult).

**5. The EUKH recently highlighted the "crucial role of families." If you could give one piece of advice to a parent whose child is spending 10+ hours a day in unregulated "gaming" chatrooms, what would it be?**
If I had to offer one central piece of advice, it would be this: do not underestimate your role, but also do not face it alone. Families are not only a protective environment; they are often the primary space where both vulnerability and resilience are shaped.

This makes them pivotal not only in early prevention, but also in disengagement processes. In practical terms, this begins with equipping families with the tools to recognise early indicators of concern. Spending long hours in unregulated online environments is not, in itself, a definitive sign of radicalisation. However, when combined with other factors, such as social withdrawal, sudden changes in language or attitudes, increased secrecy, rigid or polarised thinking, or a growing hostility towards perceived “others”, it may indicate underlying vulnerabilities that require attention. The focus should not be on isolated behaviours, but on patterns and changes over time.

At the same time, it is essential to understand and address both risk and protective factors. Risk factors may include emotional distress, loneliness, identity struggles, or exposure to harmful online networks. Protective factors, on the other hand, are often rooted in the family environment itself: stable relationships, emotional support, clear boundaries, critical thinking skills, and a sense of belonging that reduces the appeal of external validation. Strengthening these protective elements from families is one of the most effective ways to prevent harmful trajectories.

Open and non-judgemental communication is another key component. Adolescents, even when they appear disengaged, need spaces where they feel heard and understood. A purely restrictive or punitive approach may reinforce secrecy and push them further towards external communities. Instead, parents should aim to create an environment where difficult topics, including online experiences, can be discussed without fear of immediate sanction. This does not mean the absence of limits, but rather that limits are accompanied by dialogue and trust.

Equally important is the need to educate and empower parents themselves. The digital environment evolves rapidly, and many families feel overwhelmed by platforms, language, and dynamics that are unfamiliar to them. Providing parents with accessible knowledge about online cultures, including gaming spaces and meme-based communication, is essential for them to interpret what they are observing and respond effectively.

In some cases, additional support may be necessary. Family-based interventions, including family therapy, can play a crucial role in addressing underlying relational dynamics, improving communication, and supporting both parents and young people in navigating complex situations. Seeking help should not be perceived as a failure, but rather as a responsible and proactive step.

More broadly, families should be understood within a wider social and policy context. They are the primary environment where values, identity, and belonging are formed, and as such, they play a fundamental role in social cohesion. However, they cannot and should not be expected to carry this responsibility alone. Supportive ecosystems, including schools, community services, and public policies that promote family well-being, are essential to enable them to fulfil this role effectively.

Ultimately, what may seem like a simple recommendation is often the most difficult to implement: when parents feel overwhelmed or uncertain about how to manage a situation, they should not remain isolated. Reaching out for support, whether from professionals, schools, or community resources, is not a sign of inadequacy, but of awareness and concern. While feelings of personal blame, guilt, or a perceived sense of ultimate responsibility may arise, it is important to recognise that no family has all the answers, particularly in the face of rapidly evolving digital challenges, and that acknowledging this is, in itself, a key protective factor. I mean, this possible sense of sole responsibility can be limiting as it prevents families from seeking solutions. This is why it is essential to equip parents with the skills to recognise risk factors early and to encourage them to engage with professionals at the first signs of concern.

# NOT MY CHILD! WHAT ARE SOME OF THE EARLY SIGNS OF RADICALISATION AMONG ADOLESCENTS AND TEENAGERS, AND HOW TO DETECT THEM?

**“Crucially, the absence of a clear ideology is increasingly common. Ideology is no longer the primary driver.”**

“I did not see this coming.” “I had no idea that he was involved in such things…” “There were no warning signs – he just did it.”

These are phrases often voiced by parents and caregivers whose children have been radicalised (primarily online) and become involved in extreme violence, violent extremism, or even terrorism.

One may ask: How is it possible that the early signs went undetected? How could a child become radicalised without visibly adopting a clear ideology or suddenly converting to a belief system? And how is it that those closest to them often did not see it happening right before their eyes?
Without judgment, the answer is simple: it is easy to miss.

Today, across EU member states, radicalisation among children is shaped by a complex intersection of ideological, psychological, and technological factors. Crucially, the absence of a clear ideology is increasingly common. Ideology is no longer the primary driver.

In March 2026, two minors attempted to plant a bomb at a Bank of America office in Paris. Their actions were not driven by a coherent ideology, but by a mix of financial incentives, online manipulation, and broader geopolitical influences. In 2025, in Slovakia, Norway, and Germany, several children were arrested in connection with attacks motivated by racism, misogyny, or anti-Muslim hatred. In Germany, five teenagers (some as young as 14 years) were arrested for planning attacks on migrants and attempting to destabilise the state as part of the neo-Nazi group "Last Defence Wave."

Minors are no longer peripheral in such cases; they are increasingly central.
Looking back, early warning signs are often identifiable. But in the moment, they are rarely recognised. Only after arrests do patterns become clear. By distinguishing these early indicators, especially in schools and family environments, we can better understand what to look for.

In schools, a previously engaged boy may become argumentative or absolutist, insisting that "there is only one truth" and rejecting nuance.[1] This may appear as withdrawal from participation, increased confrontation with classmates or teachers, and disproportionate emotional reactions such as anger or defensiveness. These behaviours are often more visible in boys than in girls.[2]

[1] Campelo et al. (2022), A Clinical and Psychopathological Approach to Radicalization Among Adolescents
[2] Susan Nolen-Hoeksema (2012). Emotion regulation and psychopathology: The role of gender.
[3] Connell, R. W., & Messerschmidt, J. W. (2005). "Hegemonic Masculinity: Rethinking the Concept." Gender & Society, 19(6), 829–859.
Way, N. (2019). Deep Secrets: Boys' Friendships and the Crisis of Connection. Harvard University Press.

In many societies, boys are socialised to follow specific masculine values, dominance, rationality, and emotional control, while vulnerability or ambiguity is associated with weakness and lack of control.[3] In this context, rigid or absolutist thinking and acting can function as a way of performing masculinity and protecting social status or identity. What appears as aggression or ideological certainty may therefore hide underlying insecurity, confusion, or emotional distress that boys feel unable to express openly in the offline world.

Girls, by contrast, are often socialised toward relational harmony and emotional self-monitoring, meaning distress may be expressed in less externally confrontational ways.[4] As a result, schools may notice polarised or disruptive behaviours more readily in boys because they align with culturally recognised forms of masculine acting-out. These patterns are not biologically fixed, but shaped by wider social norms, peer cultures, and institutional expectations.

A growing sense of intolerance and the justification of violence are also key warning signs. Around the dining table, this may sound like blaming entire groups or using dehumanising language. An intense fixation on perceived injustice framed in extreme or conspiratorial ways can be another indicator.

"An intense fixation on perceived injustice framed in extreme or conspiratorial ways can be another indicator."

Anderson, E. (2020). Inclusive Masculinity Theory: Overview, Reflection and Refinement. Journal of Gender Studies, 29(6), 677–689.
[4] Gilligan, C. (1982). In a Different Voice: Psychological Theory and Women's Development. Harvard University Press.

Parents and caregivers may notice a developing fascination with weapons, attacks, or perpetrators among boys. A child may begin to glorify individuals previously unknown to the family. Drawing in sketchbooks, napkins, or in notebooks may increasingly depict violence, destruction, or weapons.

Social changes are equally important. Caregivers and parents may notice that old friends are no longer coming around, or that no one comes around at all. Their son or daughter spends increasing amounts of time online. The child tries to convince the people around them of their 'only and unique' conviction without real dialogue, instead pressuring them. Conflicts with classmates from particular backgrounds may intensify, reflecting a growing "us versus them" mindset.

Conversely, girls in many cases display less disruptive or visible behaviour.[5] Their pathways into radicalisation may be more relational in nature. Online contacts, romantic relationships, and friendship networks can play a significant role in influencing their radicalisation. This process is often more subtle and less immediately recognisable.

The online environment remains the primary space where radicalisation unfolds. For parents, caregivers, and teachers, it is also the hardest to monitor both because of privacy concerns and a lack of insight into digital subcultures. However, warning signs may still surface indirectly.

[5] Rose, A. J., & Rudolph, K. D. (2006). "A Review of Sex Differences in Peer Relationship Processes: Potential Trade-offs for the Emotional and Behavioral Development of Girls and Boys." Psychological Bulletin, 132(1), 98–131.

"The online environment remains the primary space where radicalisation unfolds."

Adolescents may use irony, coded language, or dark humour in schoolwork. They may reference niche online figures, networks, or extremist memes. These signals, though subtle, should not be ignored.

Adolescence is naturally a period of identity exploration, which makes it particularly difficult to distinguish between normal development and early radicalisation. Political activism, religious interest, and identity formation are not inherently problematic. The challenge lies in recognising when these shift toward rigidity, exclusion, and the acceptance of violence.

Ultimately, there are five key domains that parents, caregivers, and teachers should pay close attention to: number one rapid behavioural change, that may be characterised by sudden shifts in personality, mood, routines, appearance, or interests that seem disproportionate or difficult to explain. Second a shift from nuanced thinking to black-and-white views by increasing rigidity in beliefs, intolerance of ambiguity, and insistence that complex issues have only one correct answer. Third explicit or implicit justification of violence by expressing admiration for violence, framing harm as necessary or heroic, or normalising aggression against perceived enemies or out-groups. Fourth social isolation from family, friends, or previously valued activities and only substituted by loneliness, resentment, or alienation. And fifth. involvement in closed networks and increased secrecy, especially in online activity where the minor spends increasing amounts of time in insular digital spaces, concealing online interactions, or engaging with communities that reinforce grievance, hostility, or extremist narratives.

Recognising these patterns early is essential to preventing the "I did not see it coming" scenario.

**Lilla Schumicky-Logan**
Deputy Executive Director and Head of Portfolio Management Unit, GCERF (Global Community Engagement and Resilience Fund)
EU Knowledge Hub Special Advisor on Minors

# "DIGITAL STREET WORKER" (DENMARK): ONLINE PATROLLING

**Mikkel Bøgeskov Eriksen**
Senior Advisor SCU, Special Crime Unit Danish Online Police Patrol

The Danish Online Police Patrol (POP), known as POP in Denmark, was established in 2022. It comprises seven uniformed officers, three civilians, and one Superintendent dedicated to addressing a spectrum of online criminal activities, from fraud with skins, grooming, to extremism. Operating on a 'Prevent, Disrupt, and Investigate' framework, the POP builds an 'eye-level' approach to engender trust within online communities, especially among young people. Wearing uniforms online, the unit is visible on platforms like Discord, Twitch, TikTok, and Instagram, engaging with users and investigating concerning behaviours, emerging online trends, and threats.

The Patrol conducts weekly online patrols on social media platforms and within online games, where they interact with Danish users through verified profiles. This can take place, for example, on Reddit or in Roblox.

More recently, during the latest Danish parliamentary election, the Patrol monitored the comment sections on Danish politicians' social media pages – such as Facebook – focusing on identifying threats and engaging in dialogue with citizens.

In other cases, the Patrol operates within various Discord servers, where they use webcams and microphones to engage directly with children and young people on specific topics such as hacking or sextortion.

The POP adopts the language of the users online, primarily younger audiences, with the licence to deploy social media engagement, such as TikTok videos or supplementary use of memes and GIFs to establish effective communication. Last year, the Patrol published a TikTok video that was viewed more than 168 million times. The Patrol's TikTok account is among the largest in Denmark.

Through online gaming platforms like Twitch streaming Fortnite and Minecraft, they actively participate, gaining trust through visibility and participation. It can investigate and refer cases involving, for example, dealing drugs or fireworks to sharing inappropriate content.

They also conduct online parent empowerment campaigns regarding online safety, choosing content for busy and stressed parents to meet them on platforms they use, like YouTube and Facebook. The POP exemplifies a strategic communication approach by understanding its audience at an ‘eye level’. This approach allows for a soft intervention, fostering a sense of community while confronting the audience’s needs and concerns.

By engaging with young people, the POP recognises that kids may not confide in their parents about online experiences due to fear of device confiscation, guilt, and shame. The unit meets the kids where they are and fosters a supportive environment, offering clear routes for investigation without punishment and building a rapport along the way. Their success extends beyond online platforms, with POP members sometimes being recognised and approached in public. POP has also been nominated for awards and is often featured on scenes during award presentations across various social media platforms and gaming award shows.

# FOREIGN AND RETURNING TERRORIST FIGHTERS: A COMPREHENSIVE REVIEW OF POLICY AND PRACTICE

**Viktória Kuszi**

Assistant lecturer, Ludovika University of Public Service Law Enforcement Faculty Counter Terrorism Department.

**Terézia Ruff**

Academic staff member / MSc student of the Department of Counter-Terrorism, Ludovika University of Public Service Law Enforcement Faculty Counter Terrorism Department.

The phenomenon of Foreign Terrorist Fighters (FTFs) has become one of the most complex challenges in global security policy over the past decade and a half. Issues of international terrorism, armed conflicts, migration, and state sovereignty are all intertwined within this problem area. The volume *Document Collection on Foreign and Returning Terrorist Fighters* aims to present this multifaceted phenomenon in a comprehensive manner through a thematically structured selection of relevant literature.

Rather than promoting a single analytical perspective, the collection brings together documents representing diverse academic, policy-oriented, and practical approaches, thus offering a complex picture of the security, social, and legal dimensions of the issue.

This document collection was prepared at the Department of Counter Terrorism of the Faculty of Law Enforcement, Ludovika University of Public Service, Budapest. The Department serves as one of Hungary's leading institutional platforms for research and education in the field of counter-terrorism and security studies.

**Dániel Rémai**

Assistant Professor, Ludovika University of Public Service Law Enforcement Faculty Counter Terrorism Department.
TP6 on "Management of Foreign Terrorist Fighters (FTFs), Volunteers, and their Families" Co-Leader.

Its work is characterised by an interdisciplinary approach, integrating perspectives from law enforcement, international relations, and security policy, while maintaining close links with practitioners and governmental stakeholders. Through its teaching, research, and international collaborations, the Department contributes to the development of both academic knowledge and practical responses to evolving security challenges. The authors of the volume are Viktória Kuszi, Terézia Ruff, and Dániel Rémai.

It is important to highlight that the document collection was prepared in Hungarian, which in itself represents a valuable and gap-filling initiative. In Hungary, the issue of foreign terrorist fighters is not among the most prominent topics on the national security agenda; nevertheless, given ongoing international developments, it remains important for the professional and academic community to engage with the subject. The relevance of the topic is also reinforced by European policy frameworks. Recent strategic directions of the European Union in the field of counter-terrorism – most notably the EU Agenda on Preventing and Countering Terrorism –place particular emphasis on preventing radicalisation and addressing the security and societal challenges posed by foreign and returning terrorist fighters.

One of the greatest strengths of the volume lies in its clear structure. The authors organise the material into three major sections. The first part provides a brief geopolitical overview that situates the phenomenon of foreign terrorist fighters within a global and regional context. The second section discusses conceptual and theoretical foundations, paying particular attention to the definition of FTFs, the dynamics of radicalisation, and the security and social challenges posed by returning fighters. The third and most extensive part is a thematically structured collection of texts that introduces the work of various international organisations, research institutes, and experts.

The opening section of the volume highlights that the phenomenon of foreign fighters is not new; however, it gained a new dimension during the 2010s. During the conflicts in Syria and Iraq, international jihadist mobilisation reached an unprecedented scale: according to estimates, between 2011 and 2016 more than 42,000 individuals travelled from different countries to conflict zones in order to join terrorist organisations. The global character of the phenomenon underscores the role of modern communication technologies and online propaganda. Radical groups were able to establish transnational recruitment networks that generated rapid, cross-continental mobilisation.[1]

[1] Hamming, Tore Refslund (2019): Global Jihadism after the Syria War. In: Perspectives on Terrorism. VOL. XIII, Issue 3. p.8.

The geopolitical analysis emphasises that the FTF phenomenon is closely linked to the fragmentation of the international system. Contrary to the optimistic expectations that followed the end of the Cold War, the security environment of the early twenty-first century has increasingly been shaped by non-state actors and asymmetric threats. Armed conflicts often become protracted and create long-term instability, which in turn provides a mobilisation space for radical groups. In this environment, the emergence of foreign fighters is not an isolated development but rather a recurring feature of the global security landscape.

The regional overview in the volume pays particular attention to the situation of the European Union. Europe occupies a specific position within the FTF phenomenon: while it is not a primary conflict zone, it represents both a significant point of departure and a destination for returning fighters. During the Syrian and Iraqi conflicts, more than five thousand European citizens joined terrorist organisations.[2] European security policy initially relied primarily on reactive and law-enforcement-centred measures, including stricter criminal legislation, enhanced border controls, expanded intelligence cooperation, and financial surveillance mechanisms introduced after the 2004 Madrid and 2005 London attacks.

[2] European Fighters in Syria and Iraq: Assessments, Responses, and Issues for the United States. (2015) https://www.everycrsreport.com/reports/R44003.html

Over time, however, increasing emphasis has been placed on preventing radicalisation through community-based programmes, online content regulation, education initiatives, and the reintegration of returning foreign terrorist fighters and their families, particularly following the rise of ISIS after 2014.

The chapter focusing on the Western Balkans is particularly noteworthy, as it illustrates the region's specific context. Although fewer fighters in absolute numbers travelled from this region to Middle Eastern conflicts, proportionally the Western Balkans was among the largest source regions in Europe. The phenomenon may be linked to the challenges faced by post-conflict societies, the lack of economic opportunities, and persistent political and identity-related tensions. At the same time, the experiences of the region demonstrate that dealing with returnees is not solely a security issue but also a long-term societal challenge.

The volume also addresses in detail the dilemmas associated with returning fighters. Returning FTFs represent both a national security risk and a challenge of social integration. Some individuals continue to adhere to radical ideologies and may pose a potential threat, while others return disillusioned and require support for successful reintegration. The documents highlight that policies addressing returnees often involve tensions between security considerations and human rights or child protection perspectives.

One of the most important themes of the volume is the situation of women among returning individuals from former conflict zones. Following the end of the Syrian and Iraqi conflicts, a significant proportion of returnees are no longer male combatants but women. In the case of female returnees, it is particularly difficult to determine the boundaries between responsibility and victimhood: some women played active roles in the functioning of terrorist organisations, while others arrived in conflict zones under coercive or vulnerable circumstances.
The situation of children constitutes a separate and increasingly important challenge. Many minors were exposed to violence, ideological indoctrination, or severe psychological trauma during their time in conflict zones. Consequently, policy responses increasingly focus on psychological rehabilitation, safeguarding, education, and long-term social reintegration.

The document collection also devotes significant attention to policy responses. The volume presents the guidelines of the United Nations, the European Union, and various international organisations, as well as practical experiences from several countries. The different case studies – such as the policies of Belgium, Germany, or the Netherlands – demonstrate that there is no single model for managing returning fighters. Some states rely primarily on criminal justice tools, while others place greater emphasis on rehabilitation and deradicalisation programmes.

An important message of the volume is that the phenomenon of foreign terrorist fighters is a multidimensional problem that cannot be addressed solely through security policy instruments. Preventing radicalisation, strengthening societal resilience, and implementing reintegration programmes are all key components of long-term solutions. Taken together, the documents suggest that effective policy requires an integrated approach in which law enforcement, social policy, education, and civil society cooperate.

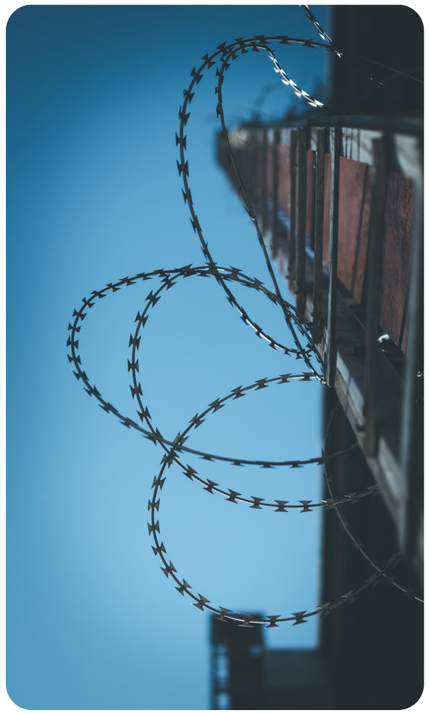
Overall, Document Collection on Foreign and Returning Terrorist Fighters represents a valuable resource for anyone dealing with issues related to terrorism, radicalisation, or international security. The volume may be particularly useful for researchers, students, security policy professionals, and decision-makers, as it brings together key academic and policy documents on the topic within a single framework. The thematic structure enables readers not only to explore individual studies but also to gain a comprehensive understanding of the various aspects of the FTF phenomenon.
A notable strength of the document collection is that it presents diverse analytical perspectives rather than prescriptive conclusions. Instead, it presents different perspectives and analytical frameworks that help readers understand an extremely complex security policy issue. This diversity of approaches makes the volume especially valuable for both academic research and policy-making.

**Lessons Learned**
The collected materials highlight several broader lessons regarding the management of foreign terrorist fighters (FTFs) and returnees:

- Effective reintegration requires long-term cooperation between security institutions, social services, schools, and local communities.
- Women and minors require differentiated assessment frameworks reflecting distinct pathways of radicalisation, victimisation, and agency.
- Online radicalisation and encrypted communication increasingly complicate early detection and intervention efforts.
- Sustainable prevention strategies depend not only on law-enforcement measures but also on trust-building, education, and local resilience.
- The lack of harmonised European reintegration standards continues to create operational and legal fragmentation across Member States.

The authors plan to compile additional document collections on similar themes in the future, addressing other current issues related to terrorism, radicalisation, and security policy. The authors therefore welcome suggestions for studies, reports, or policy documents that could serve as a basis for future selections.

**Conclusion**
The aim of this initiative is to create a continuously expanding professional resource base that supports professional discourse and facilitates access to relevant international literature. By collecting and contextualising key studies, policy documents, and empirical analyses, the initiative seeks to assist researchers, practitioners, and policymakers working in the fields of counter-terrorism, radicalisation prevention, and security studies. It also aims to strengthen knowledge transfer between academic research and operational practice.



# FINAL DESTINATION? EUROPEAN FOREIGN TERRORIST FIGHTERS IN IRAQI PRISONS

*Since January 2026, there has been a significant change in the situation regarding the detainment of male individuals suspected of being members of Daesh (ISIL), including numerous European foreign terrorist fighters (FTFs). Firstly, Syrian transitional president Ahmed al-Sharaa's troops routed the Kurdish-dominated Syrian Democratic Forces (SDF) and advanced to the northeast region, where Daesh suspects have been detained in prisons for almost ten years. The United States, which had previously supported the SDF, then transferred almost 6,000 male Daesh prisoners to neighbouring Iraq; about 3,500 of them are Syrian nationals. The Iraqi government has called on other nations to repatriate their own citizens. Following the start of the U.S.–Israeli war against Iran, the Al-Karkh prison housing individuals affiliated with Daesh has become a target of attacks. European states that have so far been reluctant to repatriate male FTFs now face difficult decisions.*

In mid-January 2026, the domestic political situation in Syria escalated markedly, following the withdrawal of US military forces from northeast Syria. The armed conflict between the army of the transitional Syrian government and its allies, on the one hand, and the SDF, on the other, spread to the country's northeast. On 19 January, the SDF was forced to hand over control of the Shaddadi prison in the Hasaka region, allowing 120 prisoners to escape, according to the Syrian central government. Eighty-one of the prisoners were recaptured. However, Kurdish sources have reported that as many as 1,500 Daesh prisoners may have escaped.

Despite the transitional Syrian government and the SDF signing an agreement at the end of January (which included the transfer of control of detention centres housing Daesh suspects to the Syrian central government), the US government appeared to assume that the al-Sharaa government would be unable to ensure the safe custody of these prisoners. Fearing further prison breaks and a potential Daesh resurgence, the U.S. government opted to initiate a military operation to facilitate the transfer of the detainees to Iraq. By mid-February 5,704 male Daesh suspects had been transferred to prisons in Iraq. They are reported to come from more than 27 countries, including France, Germany, Turkey, China, and Russia.

Though Iraqi Justice Minister Khaled Shwani has highlighted prison overcrowding as a significant challenge for the Iraqi justice system, he also emphasised that accommodating a substantial number of Daesh prisoners appears to be a necessary measure to ensure regional security. He stated that it requires "human resources to run this prison, infrastructure, additional manpower, military and security forces for protection, as well as the costs of housing, maintenance, and providing services to 5,704 prisoners. This is not easy."

Iraqi officials have repeatedly demanded that countries of origin repatriate their citizens. The Iraqi Prime Minister, Shia al-Sudani, recently called on EU states to repatriate their nationals among the captured Daesh suspects and try these individuals in their respective countries. During a call with EU Commission President Ursula von der Leyen, he emphasised that these repatriations are fundamental to ensuring long-term regional security. According to the Iraqi Justice Minister, only detainees "who fought Iraq, killed Iraqis or participated in terrorist activities inside Iraq" would be tried in Iraq.

Recent developments suggest that the joint efforts of Iraq and the United States have led to some movement regarding the repatriation of FTFs. Morocco, Tunisia, Turkmenistan, and Egypt are anticipated to be the first countries to begin repatriating their citizens from Iraq. An agreement has been reached with Turkey for the repatriation of Turkish citizens. Furthermore, the Russian government has indicated its willingness to return around 130 of its citizens. However, European states currently do not display the same degree of willingness, referring to potential prosecutions through Iraqi authorities.

According to the Iraqi Anti-Terrorism Law, foreign nationals cannot be prosecuted for acts committed outside of the country's territorial jurisdiction. However, an exception is made for the prosecution of Daesh members. Daesh is widely regarded as a terrorist organisation that poses a threat to the Iraqi state and its people. Since Daesh began gaining control of significant portions of Iraqi territory in 2014, it has been asserted that affiliation with or membership of this group constitutes an ongoing threat to Iraq's national security and state stability. Consequently, this act is not automatically regarded as purely "foreign", but rather as participation in an organisation whose main place of crime and activity was Iraq.

The trials of these individuals are further complicated by differing approaches to international law and human rights, putting additional pressure on their home countries. Take Germany for example. If the Iraqi government were to try German Daesh suspects in Baghdad according to this line of argumentation, Germany would be prohibited from providing investigative information to support the Iraqi criminal proceedings, since the death penalty is imposed in Iraq. In accordance with § 8 of the Act on International Mutual Assistance in Criminal Matters (IRG), mutual legal assistance (and consequently the transmission of evidence) is inadmissible if its purpose is to impose or execute the death penalty. In the event of a state requesting legal assistance, an exception is permitted should they guarantee "that the death penalty will not be imposed or not carried out".

The extent to which these trials coincide with international human rights and constitutional law remains questionable. This is evidenced by previous counterterrorism proceedings in Iraq. Furthermore, Iraq's Anti-Terror Law is also insufficiently differentiating between different types of membership and affiliation. A confidential situation report from the Federal Foreign Office dated October 2022, further demonstrates the prevalence of confessions that are obtained through coercion, torture, and arbitrary arrests. Often, capital punishment is imposed following a trial that lasts for a mere 10-minutes.

Short and unjust trials not only fail to provide a satisfactory resolution for the victims of Daesh. They also have the potential to be exploited and disseminated by extremist groups as a 'martyrdom' narrative. The fact that prisoners are housed in mass cells results in the creation of a milieu that neither dismantles nor challenges existing radical world views but rather serves to consolidate and re-activate them. This phenomenon has been impressively highlighted by studies conducted by the Counter Extremism Project, reports of the UN Special Rapporteur on the Promotion and Protection of Human Rights in the Fight against Terrorism, and eyewitness accounts.

**“The fact that prisoners are housed in mass cells results in the creation of a milieu that neither dismantles nor challenges existing radical world views but rather serves to consolidate and re-activate them.”**

### The Effects of the Iran War

Although the initial relocation seemed to be a step forward in securing Daesh prisoners, the already fragile security situation in Iraq has worsened further as a result of the US-Israeli war on Iran. The killing of Ali Khamenei and members of his family has also triggered visible anger within Iraq. As the US and Iran are Iraq's most important bilateral partners, a prolonged war could massively impact the country's security situation, with political fragmentation and sectarian divisions already growing.

U.S. and coalition bases and facilities, as well as Iraqi prisons holding Islamic State fighters, have been repeatedly targeted by Iranian-backed militias. Some Daesh suspects recently transferred from Syria are being held in Baghdad's al-Karkh prison, located within Baghdad airport complex. In a recent statement, the Justice Ministry expressed concern about the impact of these attacks on the security of the prison. Daesh's continued presence in both Iraq and Syria remains a further source of concern for the Iraqi authorities. Daesh stands to gain from political fragmentation and the weakening of the Iraqi security forces caused by the Iran war.

### Potential Pathways

When considering the potential courses of action for European countries, two main options emerge. The first option is to continue the current course of action, letting Iraq and the U.S. handle European FTFs, while providing financial compensation. The Iraqi justice system would determine the appropriate course of action. The second option is repatriation, whereby responsibility for the citizens in question is assumed after they have been left in a legal and consular grey area in Syria for years, a fact that has been the subject of ongoing criticism from numerous organisations, including the United Nations and Human Rights Watch.

Developments from January to March 2026 have demonstrated that European states would benefit from contingency planning. If the current war continues and the Iraqi government and its international supporters are unable to withstand attacks from Iran-backed Shia militias and the Islamic State itself, it is conceivable that European FTFs in Iraqi prisons might escape. If European states opt for repatriation, the timeframe is relevant, as it is anticipated that FTFs could be released ahead of schedule. This is because they may be granted a credit factor of 1:3 for their time spent in Iraqi prisons under respective national law.

**Conclusion**
The return of European FTFs presents a highly complex issue involving numerous stakeholders and interests at various international and national levels. European governments are facing a challenging situation that requires careful management. Unlike the repatriation of numerous female Daesh supporters and their children by several European countries in the past, there is less political willingness to return male FTFs.

Iraq could well be their final destination. However, continued political instability, the announced end of the U.S.-led anti-Daesh coalition in Iraq, as well as ongoing attacks by Iran-aligned militias could increase the likelihood of prison escapes and an Daesh resurgence. A coordinated return and removal of the burden from Iraq could constitute a beneficial strategy for ensuring long-term regional and international security, given the highly fragile situation on the ground.

**“The return of European FTFs presents a highly complex issue involving numerous stakeholders and interests at various international and national levels.”**

**Hanno Schedler**
Case Manager, Grüner Vogel e.V.

**Julia Berczyk**
Case Manager, Grüner Vogel e.V.

# FROM IDEOLOGY TO NETWORKED EXTREMISM AND INFLUENCE ECOSYSTEMS: WHY PCVE MUST EVOLVE

**Javier Ruipérez Canales**

Strategic Communications Manager of the EU Knowledge Hub. Director of Research and Projects at the Euro-Arab Foundation

For decades, violent extremism was largely understood through the lens of organised groups, coherent ideologies, and relatively linear radicalisation pathways, with prevention efforts focused on understanding ideological commitment, monitoring organisational structures, and disrupting recruitment processes. But is this model still sufficient? Across this 5th issue of the Digital Magazine, contributors describe a series of developments that may at first appear unrelated: the decentralisation of extremist propaganda production, the emergence of Violence-as-a-Service (VaaS), the rise of algorithmic radicalisation, the exploitation of artificial intelligence for grooming and manipulation, the growth of true crime communities, and the increasing circulation of transnational ideological narratives. Taken individually, each phenomenon represents an important challenge for prevention practitioners and policymakers. Taken together, however, they reveal something much more significant: **a profound transformation in the nature of extremism itself.**

SHARE

Radicalisation is no longer confined to clearly identifiable organisations or ideological movements. Instead, it unfolds across complex digital environments where narratives, identities, communities, technologies, and forms of violence intersect (Conway, 2017; Fielitz & Thurston, 2019). Individuals move fluidly between platforms, subcultures, conspiracy communities, gaming environments, extremist channels, and online networks where ideological content coexists with memes, entertainment, irony, and performative violence (Fielitz & Thurston, 2019). At the same time, **communication has become inseparable from radicalisation** with extremism and violence increasingly designed for digital audiences, extremist narratives circulate through networked information environments where influence often matters more than formal recruitment (Wardle & Derakhshan, 2017; European Commission, 2022). In many cases, the objective is no longer simply to convince individuals to join a particular movement, but to shape perceptions, amplify grievances, deepen polarisation, and mobilise audiences. What we are witnessing is therefore not simply a transformation of extremism, but the emergence of a new ecosystem of networked violence in which ideology, communication, digital infrastructures, and identity formation are deeply intertwined.

"Radicalisation is no longer confined to clearly identifiable organisations or ideological movements."

"In many cases, the objective is no longer simply to convince individuals to join a particular movement, but to shape perceptions, amplify grievances, deepen polarisation, and mobilise audiences."

Understanding this shift is essential if Prevention and Countering Violent Extremism (PCVE) is to remain effective. The challenge facing Europe is no longer only how to prevent individuals from joining extremist organisations, but how to build resilience within increasingly complex influence ecosystems that shape attitudes, identities, and behaviours long before formal radicalisation occurs.

### From Organisations to Ecosystems

One of the most significant transformations highlighted throughout this Digital Magazine is the gradual shift from organisation-centred extremism towards ecosystem-based forms of radicalisation and violence. This is particularly important in the case of Lone Actors, which, in the absence of an extremist group, tend to be analysed as individual and isolated products of radicalisation under the traditional model of prevention. However, if we pay attention to their online patterns and digital footprints, we could argue that the extremist organisation is currently replaced by extremism-related ecosystems of contents and networks available in multiple formats and platforms (GNET, 2024a; ISD, 2025).

As discussed in this issue, extremist propaganda is no longer produced exclusively by formal organisations. Digital technologies, social media platforms, creative software, and artificial intelligence have dramatically lowered the barriers to content production. Individuals can now create, adapt, remix, and distribute ideological material without belonging to any structured movement. Extremist communication has become decentralised, participatory, and increasingly embedded within everyday digital culture. Similarly, contemporary violence increasingly emerges from fluid online environments rather than isolated organisations (Malkki, Ali-Hokka & Benjamin, 2025; ISD, 2025). Violence-as-a-Service, accelerationist communities, online cultic networks, misogynistic ecosystems, violent fandoms, and nihilistic subcultures all illustrate how violence can circulate through interconnected networks where different actors, motivations, and ideologies overlap (GNET, 2024a; Malkki et al., 2025; ISD, 2025).

These ecosystems are characterised by permeability. Individuals can move between communities, platforms, and narratives, consuming contents from multiple sources simultaneously. Extremist propaganda coexists alongside conspiracy theories, gaming cultures, influencer content, political grievances, and entertainment.

In this environment, ideological purity becomes less important than participation in a shared digital milieu. The result is a radicalisation landscape that is increasingly decentralised, transnational, and difficult to categorise through traditional ideological labels (Europol, 2025).

The question, therefore, is no longer simply which group an individual belongs to, but which ecosystems they inhabit, which narratives they consume, and which digital communities shape their perceptions of reality. This shift has profound implications for prevention. Monitoring organisations alone is no longer sufficient when influence, socialisation, and mobilisation occur across fluid digital environments that transcend traditional organisational structures.

**“The result is a radicalisation landscape that is increasingly decentralised, transnational, and difficult to categorise through traditional ideological labels.”**

### Violence as Communication

A further characteristic of contemporary extremism is the growing convergence between violence and communication. Historically, violence was often understood primarily as a means to achieve political objectives. Today, violence increasingly performs an additional function: it communicates. Many contemporary attacks are designed not only to produce physical harm but also to generate visibility, attention, emotional impact, and symbolic resonance (Conway, 2017).

Manifestos, livestreamed attacks, viral videos, memes, propaganda edits, digital archives, and post-attack communities ensure that violent acts continue to circulate long after the event itself (Fielitz & Thurston, 2019). In this context, violence becomes content.

The communicative dimension of violence is visible across multiple ideological and non-ideological environments. Jihadist organisations have long understood the importance of enhancing their own strategic communication capabilities. Contemporary accelerationist movements similarly seek to inspire copycat attacks and societal destabilisation through symbolic acts of violence. Nihilistic online communities often celebrate perpetrators as digital celebrities, transforming attacks into cultural reference points which circulate through memes, fan content, and online storytelling. The objective is frequently less about persuading audiences through rational argument and more about generating emotional reactions. Fear, outrage, admiration, humiliation, revenge, belonging, and excitement become central mechanisms through which violence acquires meaning.

**"Understanding violence as communication therefore becomes essential for understanding how contemporary radicalisation operates."**

Digital platforms significantly amplify these dynamics. Algorithms reward engagement, emotional content travels faster than factual information, and visual media often generates stronger reactions than traditional political messaging. As a result, the communicative impact of violence can extend far beyond the immediate victims and locations affected. This development reinforces the need to understand radicalisation not simply as a process of ideological persuasion but as a process of communication, social influence, and symbolic interaction. Extremist actors increasingly compete within attention economies where visibility, emotional resonance, and narrative dominance may be as important as operational capability. Understanding violence as communication therefore becomes essential for understanding how contemporary radicalisation operates.

### Agents of Chaos: From Recruitment to Influence

If the shift from organisations to ecosystems represents a structural transformation, a second equally significant change concerns the purpose of extremist communication itself. For many years, prevention efforts focused heavily on recruitment.

The dominant question was how extremist groups attracted, indoctrinated, and incorporated new members. While recruitment remains very important and should not be underestimated, contemporary digital environments reveal a broader and more complex reality: influence increasingly precedes recruitment and, in many cases, may even replace it as the primary objective.

Digital platforms allow extremist actors, conspiracy entrepreneurs, hostile influence networks, and ideologically motivated communities to reach audiences at unprecedented scale (Wardle & Derakhshan, 2017; European Commission, 2022). Rather than focusing exclusively on converting individuals into formal members, many actors seek to shape perceptions, emotions, and interpretations of reality. Their objective is not necessarily to recruit followers immediately, but to influence how people understand social problems, political events, identity conflicts, and perceived injustices (European Commission, 2022). Finally, this influence tends to broadly increase the likelihood of malicious actors weaponising social groups.

This transformation has profound implications. Individuals may become increasingly exposed to polarising narratives, grievance-based framings, conspiratorial worldviews, or exclusionary interpretations of social reality without ever joining an extremist organisation. The cumulative effect of this exposure can contribute to distrust, social fragmentation, and increased receptivity to extremist narratives over time (Wardle & Derakhshan, 2017). The distinction between influence and recruitment is particularly important in an environment characterised by algorithmic amplification, personalised recommendation systems, and information disorder. Content no longer needs to be explicitly extremist to contribute to radicalisation dynamics (European Commission, 2022; Conway, 2017). Narratives that deepen polarisation, undermine trust, reinforce victimhood identities, or normalise hostility towards out-groups may create cognitive and emotional conditions that facilitate later mobilisation.

This dynamic is further reinforced by emerging technologies. Artificial intelligence systems, automated content production, synthetic media, and personalised communication tools are increasingly capable of identifying vulnerabilities, adapting messages, and maintaining continuous engagement with users. In parallel, transnational ideological narratives now circulate rapidly across borders, adapting to local contexts while retaining common emotional and symbolic elements. The result is a radicalisation landscape in which influence operates continuously and often invisibly. Rather than moving individuals through clearly identifiable stages of recruitment, contemporary digital environments expose users to persistent streams of narratives, symbols, and emotional stimuli that shape attitudes and identities over time.

For PCVE practitioners, this means that understanding influence ecosystems is becoming as important as understanding extremist organisations themselves. Prevention can no longer focus exclusively on recruitment pipelines. It must also address the broader communication environments within which perceptions, grievances, and identities are formed.

**“Prevention can no longer focus exclusively on recruitment pipelines. It must also address the broader communication environments within which perceptions, grievances, and identities are formed.”**

### From Ideologies to narratives, aesthetics, and subcultures

Perhaps the most striking development emerging from recent research is the declining centrality of ideology as the primary organising principle of violent extremism. This does not mean that ideologies have disappeared. Jihadism, violent far-right extremism, ethno-nationalism, and other ideological movements remain significant security concerns. However, an increasing number of contemporary radicalisation processes do not fit neatly within traditional ideological categories.

Across multiple digital environments, violence itself increasingly functions as a source of attraction, identity, status, and belonging (Malkki et al., 2025). Online communities associated with nihilistic violence, violent fandoms, misogynistic subcultures, accelerationist milieus, and certain segments of the true crime community illustrate how individuals may become attracted to violence without demonstrating strong commitment to coherent political or religious projects (Malkki et al., 2025; ISD, 2025). In these environments, aesthetics often matter as much as ideology (Fielitz & Thurston, 2019). Memes, symbols, visual culture, online status, notoriety, and performative transgression frequently play a central role in shaping participation.

Violence may be admired not because it advances a particular cause, but because it generates attention, visibility, power, or symbolic recognition.

This shift is particularly visible among younger users who navigate highly interconnected digital environments where ideological content mixes seamlessly with entertainment, gaming culture, internet humour, influencer content, and social interaction. The boundaries separating political radicalisation, identity formation, online subcultures, and harmful digital communities are becoming increasingly blurred (GNET, 2024b; ISD, 2025). Hybridisation further complicates the picture (Europol, 2025). Individuals may simultaneously engage with extremist, conspiratorial, misogynistic, nihilistic, and anti-system narratives without demonstrating exclusive commitment to any one ideology. Fragments of different worldviews are combined, adapted, and personalised in ways that challenge traditional prevention frameworks.

As a result, ideology is no longer always the most useful starting point for understanding risk. In many cases, emotional drivers, social dynamics, identity needs, grievances, status-seeking behaviour, and digital socialisation processes may provide more meaningful insights into why individuals become attracted to violent environments. This evolution creates significant challenges for PCVE frameworks that remain heavily centred on ideological categories.

**“Violence may be admired not because it advances a particular cause, but because it generates attention, visibility, power, or symbolic recognition.”**

While ideology remains important, it increasingly represents only one dimension of a broader ecosystem in which violence, identity, communication, and social belonging intersect.

### What This Means for PCVE: From Countering Messages to Shaping Environments

In sum, and from a preventive point of view, many of the developments described throughout this 5th edition of the EU Knowledge Hub Digital Magazine point towards a common conclusion: many of the assumptions that have traditionally informed PCVE approaches require significant adaptation. The challenge facing practitioners today is that the environments within which radicalisation occurs have fundamentally changed. For policymakers and practitioners, the implications are significant. Prevention can no longer focus solely on identifying extremist beliefs or disrupting recruitment efforts. It must also address the broader environments in which vulnerabilities are exploited, narratives circulate, identities are formed, and influence is exercised.

A first implication is the **need to move from organisation-centred monitoring towards ecosystem-centred analysis**. Prevention efforts can no longer focus exclusively on extremist groups, formal memberships, or designated organisations. Increasingly, influence emerges from networks of communities, influencers, platforms, subcultures, and digital spaces that collectively shape perceptions and behaviours. Understanding how these ecosystems function, interact, and evolve is becoming as important as understanding the actors operating within them.

Second, **prevention frameworks must expand beyond ideology**. Ideological narratives remain important, but they increasingly coexist with emotional, social, and identity-based drivers that cut across traditional categories. Grievances, loneliness, status-seeking, humiliation, belonging, notoriety, and the search for meaning frequently act as more immediate drivers of engagement than doctrine itself. Effective prevention therefore requires a broader understanding of the psychological, social, and cultural dimensions of radicalisation.

Third, **greater attention must be devoted to communication environments**. Radicalisation increasingly occurs within digital ecosystems characterised by algorithmic amplification, personalised content, information disorder, and continuous exposure to emotionally charged narratives.

In such environments, harmful influence often precedes recruitment and may operate long before individuals encounter explicitly extremist content. Monitoring narratives, information flows, and audience dynamics is therefore becoming a core prevention requirement rather than a complementary activity.

This evolution also reinforces **the growing importance of Strategic Communications** within PCVE. Traditional approaches often focused on countering extremist narratives directly. While such efforts remain valuable, contemporary digital environments require a broader and more proactive approach. The challenge is no longer simply to respond to harmful messages, but to strengthen resilience, foster trust, promote social cohesion, and shape communication environments that are less conducive to manipulation and mobilisation.

In this context, **digital literacy becomes a prevention capability** rather than merely an educational objective. Individuals increasingly require the skills to navigate complex information environments, recognise manipulation, assess sources critically, understand algorithmic dynamics, and engage constructively with competing perspectives. These capacities are becoming central components of societal resilience against both extremism and broader forms of information manipulation.

At the same time, and after recognising the great importance of the online environment in radicalisation, it is paramount to consider that **prevention must remain rooted in local realities.** Families, schools, youth workers, civil society organisations, and local authorities continue to play a critical role in identifying vulnerabilities, building trust, and strengthening protective factors. Digital radicalisation may occur online, but resilience is often built offline through relationships, belonging, and community engagement.

Finally, **prevention frameworks must become more adaptive**. Emerging technologies, artificial intelligence, synthetic media, encrypted platforms, and rapidly evolving online cultures are continuously reshaping the radicalisation landscape. Static approaches risk becoming obsolete. Future PCVE efforts will require continuous learning, multidisciplinary cooperation, and greater integration between security, education, mental health, social policy, digital governance, and strategic communications.

Ultimately, and while radicalisation and extremism have evolved, **the objective of prevention remains unchanged: reducing the likelihood that individuals embrace violence**. However, achieving that objective increasingly requires understanding radicalisation as a systemic phenomenon that emerges from the interaction of technology, communication, identity, and social dynamics.

**"The challenge facing Europe is therefore not simply how to prevent individuals from joining extremist groups. It is how to strengthen resilience within increasingly interconnected information environments where influence, communication, identity, and violence have become deeply intertwined."**

In short, PCVE must move from organisations to ecosystems, from countering messages to shaping environments. The challenge facing Europe is therefore not simply how to prevent individuals from joining extremist groups. It is how to strengthen resilience within increasingly interconnected information environments where influence, communication, identity, and violence have become deeply intertwined.

## Library


1. Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98. https://www.tandfonline.com/doi/full-l/10.1080/1057610X.2016.1157408
2. European Commission. (2022). *Countering hybrid threats*. https://ec.europa.eu/newsroom/home/items/880571/en
3. Europol, (2025): EU Terrorism Situation and Trends TE-SAT2025. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf
4. Fielitz, M., & Thurston, N. (Eds.). (2019). *Post-digital cultures of the far right: Online actions and offline consequences in Europe and the US*. Transcript Verlag. https://doi.org/10.14361/9783839446706
5. Global Network on Extremism & Technology (GNET). (2024 a). *Accelerationism, active clubs and networked extremism.* https://gnet-research.org/wp-content/uploads/2024/07/GNET-44d-Accelerationism-Active-Club-Network_web.pdf
6. Global Network on Extremism & Technology (GNET). (2024 b). Extremist "chan" culture and online radicalisation. https://gnet-research.org/wp-content/uploads/2024/07/GNET-44f-Extremist-Chan-Culture_web.pdf
7. Institute for Strategic Dialogue (ISD Global). (2025). Networks of harm: Understanding online extremist ecosystems. https://www.isdglobal.org/wp-content/uploads/2025/09/764_Networks-of-Harm.pdf
8. Malkki, L. Ali-Hokka, H. and Benjamin, S. (2025). Violence-focused online communities. RADIA Brief. University of Helsinki https://www.helsinki.fi/assets/drupal/2025-11/RADIA-brief%201%20-%202025.pdf
9. Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c

BUILDING RESILIENT COMMUNITIES,
TOGETHER.

European Commission

EU Knowledge Hub on
Prevention of Radicalisation