POLITECNICO DI TORINO
Repository ISTITUZIONALE

Bridging Technology Ecosystems: Navigating Emerging & Persisting Dimensions in the Digital Landscape

Original
Bridging Technology Ecosystems: Navigating Emerging & Persisting Dimensions in the Digital Landscape / Monaci, S., Feta, B.. - (2025). (Conclusion Paper of Thematic Panel 3: New Technologies and the Online Dimension (2nd meeting), Working Group of EU Knowledge Hub on Prevention of Radicalisation online 4 Giugno 2025).

Availability:
This version is available at: 11583/3006281 since: 2026-01-06T11:43:25Z

Publisher:

Published
DOI:

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

18 November 2026

CONCLUSION PAPER

Bridging Technology Ecosystems: Navigating Emerging & Persisting Dimensions in the Digital Landscape

Thematic Panel 3: New Technologies and the Online Dimension

Working Group of EU Knowledge Hub on Prevention of Radicalisation

Thematic Panel Members' Second Meeting
04 June 2025
Online

EU Knowledge Hub on Prevention of Radicalisation

European Commission

1. Introduction

The **second gathering** of the **Thematic Panel on New Technologies and the Online Dimension of the EU Knowledge Hub on the Prevention of Radicalisation (EUKH)** provided a critical opportunity to delve deeper into the priority topics identified earlier. The first meeting of this Panel made clear that without adopting an **ecosystem-wide approach**, efforts preventing and countering violent extremism and terrorism online will remain **fragmented and ineffective**. Building on that foundation, the second meeting focused on "Navigating Emerging and Persisting Dimensions in the Digital Landscape". Participants analysed the **specific technologies and platforms involved** and how the platforms' specific features and interactions shape the evolving threat landscape. In particular, the meeting was focused on generative AI, looking at the potential exploitation by terrorists and violent extremists, as well as focusing on opportunities to counter extremism and terrorism, and on the complex decentralised platforms ecosystem.

This conclusion paper presents the **key insights**, **takeaways**, and **best practices** that emerged from this second gathering.

2. Key Insights: Understanding the Digital Ecosystem to Strengthen Prevention

The Complex and Highly Interconnected Digital Ecosystem: The digital landscape that facilitates extremist activities is **highly interconnected**, spanning mainstream, niche, and fringe social media platforms, stand-alone extremist websites, digital archives, encrypted messaging services, and decentralised web infrastructure. While niche[1] platforms serve specific functionalities—often catering to particular interests or communities—fringe platforms provide more open, less regulated environments that support broader interactions and content sharing, making them more susceptible to exploitation by extremist actors. These digital domains **do not function in isolation**—tactics, content, and users move fluidly between them, reinforcing extremist ideologies and aiding recruitment and propaganda efforts. This cross-platform movement allows extremist actors to evade moderation, to amplify their messaging across diverse audiences, and to maintain ideological continuity despite disruptions, thus strengthening the overall ecosystem's

[1] **Niche platforms** are digital spaces that openly and purposefully cater to a specific, often extreme, audience. They are typically smaller, tightly focused communities that may revolve around particular ideologies or interests. **Fringe platforms**, on the other hand, host a mix of mainstream and extreme content. Users might encounter coded or obscured extremist material, and these platforms often position themselves as alternatives to mainstream services, offering fewer content restrictions and more ideological freedom. See more here: https://www.rand.org/pubs/perspectives/PEA1458-1.html.

resilience and reach. In addition, the **decentralised and encrypted nature** of many of these platforms hinders detection and intervention significantly, presenting critical challenges for security efforts and investigations. **Open-source platforms** like NextCloud for example have been exploited to store and distribute large volumes of malicious content.

Decentralised Platforms: Security Risks vs. Counter-Extremism Potential: Decentralised social media platforms such as BitChute, Gab, 8kun or Parler pose serious threats: the lack of centralised moderation, encryption, and anonymity allows extremist content to spread unchecked, making detection and intervention more challenging. The panel discussions highlighted the **dual use of decentralised platforms**, with 67% of participants viewing them more as a threat than an opportunity for building resilience because of their potential role in facilitating extremist activity (*see figure 1*). Meanwhile, 33% of participants recognised decentralised platforms as a **valuable tool in countering violent extremism (CVE)**, emphasising their potential to foster open dialogue, support alternative narratives, and empower marginalised voices. Despite differing perspectives, there was **broad consensus** that developing supportive mechanisms to enable a more centralised form of moderation is essential, as this could allow decentralised platforms to shift from **vulnerability factors to resilience-building tools**—reinforcing the need for **strategic, well-informed approaches** to leverage their strengths while mitigating security risks. While decentralised platforms lack a single governing authority, centralised moderation can still be introduced through **modular or opt-in systems** that preserve user autonomy while enhancing content governance. As proposed by TP members, one promising approach involves **protocol-level safeguards**, such as moderation middleware[2]—third-party services that filter or flag content across federated servers. These services can be centrally managed but activated at the discretion of server administrators or individual users. This model demonstrates that centralised moderation within decentralised networks can be **feasible, flexible, scalable**, and aligned with the principles of decentralisation.

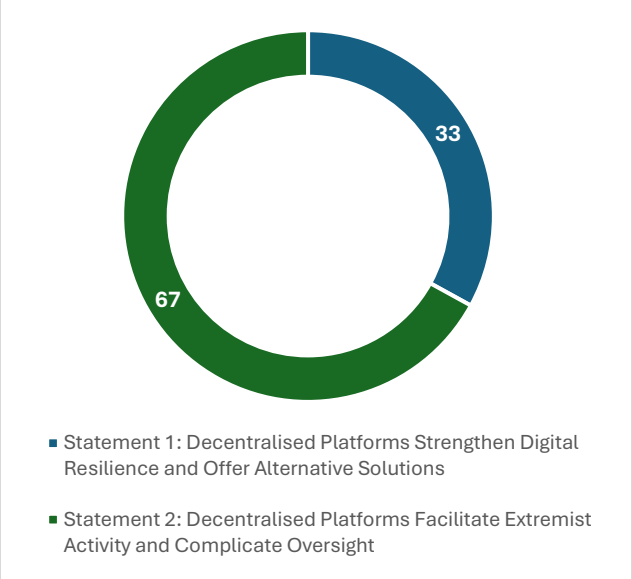


Figure 1

[2] The Integrity Institute discusses moderation middleware as a customizable layer that empowers users to filter content independently of platform-level decisions. See more here: https://integrityinstitute.org/blog/middleware-and-the-customization.

Bridging the Knowledge Gap on How Terrorists Exploit the Decentralised Platforms: The complexity of decentralised platforms presents a significant challenge in countering radicalisation, as their structures, interactions, and content dissemination mechanisms remain difficult to monitor and to moderate. Decentralised platforms operate on a **distributed network rather than relying on a central authority or server**. Because content is hosted across multiple independent nodes—often operated by anonymous or loosely affiliated individuals—there is no single point of control, making it extremely challenging to track activity, enforce moderation policies, or remove harmful content at scale. A key insight from the panel discussions was the presence of a significant **knowledge gap concerning how terrorists and violent extremist actors exploit these platforms**. A poll conducted during the session highlighted this gap, underscoring the urgent need for knowledge, targeted training, and awareness initiatives (*see figure 2*). Panel members emphasised that this lack of awareness might be even more pronounced among those with primary responsibility for supporting youth—particularly parents. As such, they recognised the urgent need to equip them with a better understanding of how decentralised platforms function and what the major threats posed by their exploitation are.

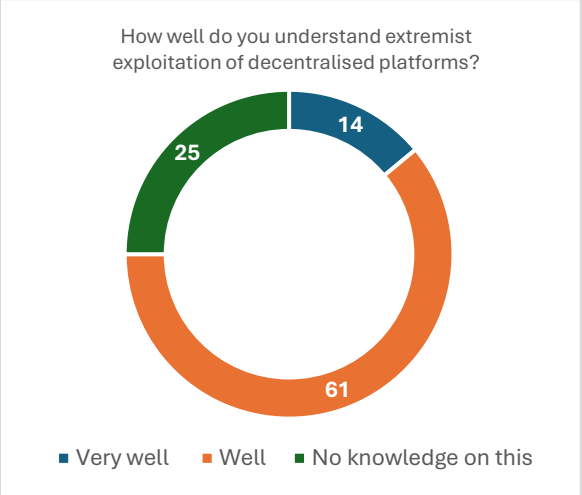


Figure 2

Extremist Platform Migration and Decentralised Platforms as Adaptive Safe Havens: The panel highlighted the **continuous migration of extremist groups** from monitored platforms to less-regulated digital spaces, allowing them to evade detection and maintain operational security. This landscape remains **highly fluid**: when specific platforms are subject to content takedowns or increased moderation pressure, extremist actors often **shift their activity to alternative, less visible environments**. This constant cycle of adaptation complicates monitoring efforts, as extremist content becomes increasingly dispersed and it is difficult for authorities to identify and track across shifting online territories. For example, the decentralised nature of platforms like **SimpleX and Rocket.Chat** makes them more attractive alternatives, offering encryption and anonymity that hinder intervention efforts. Extremist groups use these platforms strategically for **communication, recruitment, and financial transactions**, including crypto wallets like Monero. The absence of **centralised oversight and subsequent challenges to consistently enforce regulation** facilitates their resilience, reinforcing the need for **adaptive countermeasures, cross-sector collaboration, and deeper intelligence-sharing** to address emerging threats in the evolving digital landscape. Decentralised platforms can be temporarily deplatformed and later reinstated, and new digital spaces continue to emerge at a rapid pace. For example, following the U.S. Capitol

riot in January 2021, Parler[3]—a platform favoured by far-right users—was removed from Apple and Google app stores and dropped by Amazon Web Services due to concerns over violent content and lack of moderation. This effectively took the platform offline for several weeks until it secured alternative hosting.

Balancing Online Security Measures with Open-Source Accessibility: Efforts to address terrorist content online have primarily focused on **mainstream social media platforms and public-facing digital spaces**, but deeper engagement with **internet service providers (ISPs) and server hosts** remains inconsistent. While entities like Cloudflare have implemented crackdowns, the extent and effectiveness of such measures vary. A critical challenge is that **open-source platforms can play a vital role in enabling free access to information**, particularly in **repressive environments, while being susceptible to exploitation by malicious actors**. Striking a **balance between security interventions and the protection of open digital spaces** is essential to ensure platforms remain **safe, yet accessible**, without undermining their legitimate uses. To achieve this balance, panel members highlighted the importance of developing proportionate and transparent online regulations—including the protection of privacy and freedom of expression—while also encouraging transparency reporting to promote accountability and informed public debate. Panel members considered this basis as a fundamental requirement for any future regulation.

Balancing Age Restrictions and Digital Literacy: The discussion underscored the importance of **targeted protective measures** to limit terrorist and violent extremist content exposure among minors and other vulnerable groups. The discussion explored the topic of age restrictions and digital literacy for minors as a possible measure to be implemented by large and small platforms, to limit extremist content exposure among these targeted groups. Participants expressed a range of views—including concerns about effectiveness, enforceability, and potential impacts on privacy and rights. Overall, many participants expressed reservations about strict bans or age-based restrictions, emphasising the need for more nuanced, education-focused approaches instead. Some participants advocated **stricter age identification mechanisms**, such as **mandatory verification systems**, to prevent minors from accessing violent extremist content. Others emphasised the importance of **educating society** to develop and respect voluntary guidelines like the PEGI system applied in the video-gaming sector[4], arguing that **digital literacy and parental guidance** are more effective than rigid enforcement. Some participants expressed a preference for media literacy over strict age restrictions or coercive regulatory measures, arguing that heavy-handed approaches could backfire and potentially alienate younger users. Instead, they

[3] For more information see here: https://www.cnbc.com/2021/01/16/how-parler-deplatforming-shows-power-of-cloud-providers.html?msockid=12649ff8e3e760ec3dc489eae2fb61d4

[4] PEGI (Pan European Game Information) provides age classifications for video games in 38 European countries. The age rating confirms that the game content is appropriate for players of certain age. PEGI considers the age suitability of a game, not the level of difficulty. Cfr. https://pegi.info/.

advocated for educational strategies that empower youth to critically engage with digital content and understand the risks posed by violent extremist material. By promoting awareness and encouraging respect for online safety guidelines, these approaches aim to foster self-protection and responsible behaviour among young people—making them active agents in their own digital resilience. As a concrete example, TP members highlighted **community-based digital mentorship programs** as an effective and inclusive way to enhance digital literacy, particularly among young people. Furthermore, the panel also highlighted how age verification, a way to restrict access to platforms based on age, oftentimes is easy to evade, and also has the ability to infringe on human rights, with many civil society organisations highlighting privacy concerns. The debate highlighted a broader challenge: while **age restrictions can help limit exposure**, they are **not a standalone solution**.

Bridging the Regulatory Asymmetry Between VLOPs (Very Large Online Platforms according to Digital Service Act) **and Decentralised Platforms:** A key observation is that decentralised **platforms** face a greater challenge when it comes to content moderation, security measures, and transparency obligations. Decentralised social media platforms have normally more tolerant Terms of Service (ToS) compared to VLOPs: they ensure more tolerant forms of free expression and, as a result, often risk becoming “hot beds” for terrorist content. In consideration of that, decentralised platforms are more vulnerable to exploitation by malicious actors. Nevertheless, even decentralised and small platforms (in terms of number of users compared to the VLOPs) must comply with the Digital Services Act. As the panel pointed out, the legislative asymmetry emerges not so much in relation to the DSA and how it regulates small platforms, but in relation to the ToS of decentralised platforms compared to the ToS of VLOPs, which are much more attentive to content moderation and countering terrorism. In this sense, the participants highlighted this “regulation asymmetry” and called for a strengthening of existing ToS on moderation by decentralised platforms.

3. Key Takeaways: Strengthening Policies and Practitioner Strategies for a Resilient Digital Ecosystem

This chapter presents the key points that emerged from the roundtable discussion on policies and strategies aimed at strengthening the resilience of the digital ecosystem.

Strengthening Digital Counter-Extremism Strategies: To effectively combat evolving online threats, policymakers and first-line practitioners must embrace a **multi-layered, adaptive approach** that reflects the interconnected nature of extremist activity. Stronger collaboration between governments, tech providers, and civil society is crucial to **enhancing content moderation, disrupting extremist ecosystems, and preventing misuse of decentralised platforms**. Policymakers should ensure regulatory frameworks keep pace with AI-driven technologies, while first-line practitioners need specialised training to navigate emerging threats. A data-driven approach—grounded in structured data such as online activity patterns, content trends, user behaviour analytics, and threat intelligence— can enable first line practitioners to track extremist activity and inform effective responses. This includes identifying emerging threats through real-time monitoring and evaluating the impact of interventions using measurable outcomes.

Certification Framework for Decentralised Platforms: A recommendation was made to develop a safety certification system for decentralised platforms that could include a **robust set of standards and tools** designed to enhance accountability and reduce the risk of extremist exploitation. At its core, the framework would establish **baseline moderation and user safety standards**, such as mandatory AI-driven content detection, minimum thresholds for human oversight, and transparent reporting mechanisms. To support implementation, **an EU-backed technical toolkit** could offer deployable solutions like content-scanning APIs, database flagging models, and real-time moderation dashboards tailored to decentralised environments. The framework could also introduce a multi-tier compliance system, rewarding certified platforms with increased visibility, access to funding incentives, and participation in cross-platform signal-sharing networks. Crucially, the certification would be accompanied by clear guidance on balancing moderation with privacy and decentralisation values, **ensuring that governance remains democratic, rights-compliant, and aligned with the ethos of decentralised**

technologies. Together, these measures would foster responsible innovation while safeguarding digital ecosystems from extremist misuse.

Empowering Parents with Digital Safety Guidelines: Frontline practitioners and those involved in the protection of minors such as teachers, therapists, mental health teams, and parents must be practically and accessibly informed about **how the whole digital ecosystem functions**, the **channels it provides for extremist exploitation, and the protective mechanisms that exist**. To address this gap, the panel **recommended the development of dedicated material for parents**, offering clear insight into the risks children face online, while adopting an ecosystem-based approach. By mapping different platforms and their associated risks, this material aims to **empower parents with accessible knowledge** about how extremist content spreads across digital spaces. It will provide tools to help identify potential risks and supports parents in developing digital citizenship skills, thereby enhancing their ability to protect children from engaging with harmful content.

Navigating the Privacy Risks of AI-Powered Moderation on Decentralised Platforms: The panel raised concerns about **the use of AI-powered tools in Preventing and Countering Violent Extremism (PCVE)**, particularly when applied to decentralised platforms. While these tools—such as automated content moderation, behavioural analytics, and threat detection systems—can enhance security, they also carry **risks of infringing on privacy and amplifying algorithmic bias**. Without proper oversight, AI-driven moderation may lead to mass surveillance or discriminatory outcomes, potentially undermining fundamental rights and public trust. These risks could hinder the broader adoption of AI in CVE strategies, especially in decentralised environments where governance is more complex and transparency is limited.

Strengthening Oversight Through Public-Private Cooperation in Decentralised Technologies: Emerging challenges—such as the rapid evolution of decentralised technologies, inconsistent definitions of harmful content across jurisdictions, and limited transparency in algorithmic moderation—continue to complicate enforcement and oversight. In this context, **public-private cooperation** can play a transformative role by enabling timely information-sharing, co-developing ethical moderation tools, and aligning risk indicators and response protocols. Effective collaboration should be grounded in **mutual trust**, **clearly defined responsibilities**, and **shared accountability**, supported by mechanisms that uphold privacy, freedom of expression, and due process. Participants emphasised the need for cautious, transparent approaches that prioritise digital rights, alongside responsible self-regulation. Rather than restricting decentralised technologies, policymakers should focus on **intervention models** that balance security with privacy by promoting **transparency**, **proportionality**, and **accountability** in their design and deployment. To enhance this framework, some measures were proposed: **piloting real-time threat intelligence hubs** that enable decentralised platforms to flag and respond to coordinated

abuse; and **launching EU-supported capacity-building programmes** to help smaller platforms meet baseline moderation and safety standards.

Digital Resilience Through Local Engagement and Counter-Narratives: Addressing extremist misuse of decentralised platforms **cannot rely solely on legal and securitised measures**—it also requires countering terrorist and violent extremist narratives. **Engagement between practitioners, institutions, and platform end-users should be enhanced** by fostering meaningful interactions, building trust-based relationships, and supporting the delivery of counter-narratives that challenge extremist messaging in an authentic and accessible manner. By equipping users—especially young people—with the knowledge to critically navigate these digital spaces, decentralised platforms can shift from **vulnerability factors to resilience-building tools**, reinforcing prevention efforts while safeguarding open dialogue and innovation. It was, however, highlighted that counternarratives can be difficult to create, and that our industry can do better when it comes to creating entertaining counter messages.

Measures to Counter Extremist Platform Migration: To counter extremist migration to decentralised platforms, stakeholders should prioritise **early-warning systems that use AI** to detect shifts in content dissemination and user coordination across platforms. For example, by using systems devoted to "inauthentic coordinated online behaviour detection" as the one realized by the EU funded project VERA.ai[5], machine learning models can flag emerging migration trends by **analysing metadata, link-sharing patterns, and encrypted traffic indicators**. Public-private partnerships should focus on **standardising risk indicators, sharing threat intelligence**, and supporting smaller platforms with moderation tools.

Evaluating how the Lantern Coalition can provide lessons learned to counter TVEC Platform Migration: The **Lantern Coalition**, launched by the **Tech Coalition**, is an innovative cross-platform signal-sharing initiative designed to combat **child sexual abuse material (CSAM)** by preventing offenders from evading detection across different digital ecosystems without infringing on the right to privacy and GDPR. Understanding how this model does so without infringing on GDPR may aid efforts to counter **violent extremist content.** This could provide a powerful mechanism to counter **platform migration**, a tactic often used by extremist groups to circumvent moderation. By adapting Lantern's **signal-sharing framework**, tech companies could collaborate to track and disrupt extremist activity across platforms. However, while CSAM is universally illegal and clearly defined, the classification of extremist content is more complex—definitions vary across jurisdictions, and not all forms of such content are unlawful. This **legal and contextual ambiguity**

[5] The EU-funded project VERA.ai has developed a system known as the Coordinated Inauthentic Behaviour (CIB) Detection Tree, which is designed to identify and assess inauthentic coordinated activity online. This framework was revisited in a report authored by EU DisinfoLab as part of the project's deliverables. You can explore the full report and methodology on VERA.ai's official website here: https://www.veraai.eu/posts/report-revisit-coordinated-inauthentic-behaviour-detection-tree.

presents additional challenges when considering the adaptation of Lantern's framework to the TVEC space. Nonetheless, by exploring how Lantern facilitates responsible collaboration, tech companies may find pathways to disrupt extremist activity across platforms without compromising fundamental rights.

Shifting Toward Opportunity Framing and Feature-Based Taxonomy for Safer Digital Spaces: The panel suggested **moving beyond solely risk-centric approaches** and encouraged intervention strategies that leverage the potential of digital spaces in advancing prevention efforts. A key recommendation was **the development of a typology of platforms** based on their **design features rather than content**, offering a clearer understanding of the **risks users may encounter online**. This approach—emphasising platform architecture, moderation capacity, and structural characteristics—allows for a meaningful distinction between **open and closed online spaces**. Panellists noted that such a framework would help practitioners tailor responses with greater precision, leading to more **targeted, scalable, and effective interventions**.

Tailoring Interventions Based on Platform Differences: Participants stressed that **effective digital safety strategies must also recognise the distinct characteristics of different platform types**, as interventions, regulatory measures, and collaboration approaches must be adapted accordingly. Governments, tech companies, and civil society should distinguish between mainstream, niche, and decentralised platforms to ensure responses are targeted, scalable, and rights-respecting, since a **one-size-fits-all approach is insufficient**. A concrete way to achieve this would be to establish a **platform-specific risk assessment framework** that evaluates structural features, moderation capacity, user demographics, and governance models—enabling stakeholders to design tailored interventions and regulatory responses that reflect each platform's unique risk profile and operational context.

Beyond Borders: Advancing Scalable and Structured Collaboration in CVE: Given the borderless nature of the internet, panellists stressed that digital safety and countering violent extremism (CVE) efforts must be grounded in global collaboration rather than confined to an EU-centric lens. Concerns were raised about the **impact and structure of existing collaborative initiatives**. Some panellists argued that despite the existing efforts, we are still far from establishing a common framework for addressing digital safety challenges. The discussion highlighted the need for **more structured and outcome-oriented formats of cooperation**, both within existing mechanisms and through the creation of new ones. These efforts should be supported by scalable infrastructures—**such as modular design, cloud-based systems, and shared standards**—that allow tools and practices to be replicated, adapted, and deployed across diverse contexts while maintaining core functionality and compliance.

Annex

Existing Practices

Several successful programs have already been implemented in different areas of P/CVE which can be considered as "**reference models**" or "**best practices**". It is particularly useful to build from past and existing initiatives and to take advantage of the positive outcomes of the different experiences. What follows represents a non-exhaustive list of cases discussed by the participants during the panel discussion.

Lantern is a **cross-platform signal-sharing initiative** launched by the **Tech Coalition** to enhance child safety online**.** Cross-platform collaboration in the **Child Sexual Abuse Material (CSAM)** field has seen more structured and effective best practices compared to **Terrorist and Violent Extremist Content (TVEC).** This is largely due to the longer history of coordinated efforts in tackling CSAM, the existence of strong legal frameworks, and the widespread industry commitment to combating child exploitation online. Platforms combating CSAM benefit from **cross-platform hash-sharing databases**, such as those provided by NCMEC, IWF, and Google, which allow companies to detect and remove known CSAM content efficiently. **TVEC efforts have made significant strides**, particularly through **GIFCT's HSDB**. However, some panellists and experts have noted that **the level of integration, standardisation, and global adoption** of TVEC hash-sharing still lags behind the more mature and widely institutionalised systems used for CSAM. Strengthening GIFCT's taxonomy, expanding participation, and improving interoperability could help close that gap.

The **Danish Police Online Patrol** (*Politiets Online Patrulje*) was established in April 2022 to strengthen law enforcement's **digital presence and engage with citizens online**, much like traditional street patrols. This unit actively monitors social media and gaming platforms, including Discord, Facebook, Instagram, and Twitch, to prevent crime, intervene in offenses, and promote safe online behaviour. Officers also **play online games** such as Counter-Strike: Global Offensive, Fortnite, and Minecraft, interacting with young users to **build trust, preventing fraud, hate speech, and grooming**. Citizens can **contact the patrol directly** via messaging apps to report suspicious activity or seek advice on digital safety.

Germany's **Task Force to Prevent Islamist Radicalisation**, launched by Federal Ministry of the Interior in October 2024, aims to combat **online radicalisation**, particularly among **young people**. The initiative was introduced following deadly attacks in Mannheim and Solingen, highlighting the urgent need for preventative measures against extremist recruitment. The task force brings together academics, civil society representatives, and government authorities to develop

recommendations for de-radicalisation and prevention, ensuring a collaborative approach to tackling Islamist extremism. The initiative recognises that extremist recruitment often occurs through chat groups, social media platforms, and encrypted messaging services, **making digital ecosystems a critical battleground for prevention**.

Civil society fact-checking initiatives have made commendable strides in strategic communication campaigns to counter extremist narratives and in establishing **fact-checking platforms to combat disinformation** and counter violent extremism (CVE). One such example is the **SEE Check network**, a collaborative effort among fact-checking organisations in South-Eastern Europe that works to debunk misinformation and extremist propaganda. The network includes organisations from Serbia, Croatia, Bosnia and Herzegovina, Montenegro, and Slovenia, focusing on media accountability and improving public resilience against disinformation. Their work involves verifying claims, exposing manipulative narratives, and fostering media literacy to **counter the spread of extremist ideologies online**.

Tech Against Terrorism is a global initiative dedicated to disrupting terrorist activity online while upholding human rights. The organisation collaborates with tech companies, policymakers, and experts to develop effective counterterrorism strategies. A key component of its work is the **Terrorist Content Analytics Platform (TCAP)**, which automates the detection and removal of verified terrorist content across digital platforms. TCAP leverages **open-source intelligence and AI-driven processes** to swiftly identify and alert tech companies about harmful material, ensuring a proactive approach to combating online extremism.

The **European Observatory of Online Hate (EOOH)** is an AI-powered platform dedicated to identifying and analysing **illegal online hate speech** across multiple languages, including **22 EU languages, Arabic, and Russian**. By supporting **real-time tracking and reporting**, EOOH helps detect harmful content on both mainstream and fringe platforms, contributing to a safer and more inclusive digital space. The initiative plays a crucial role in monitoring evolving **hate speech narratives, such as sexism, antisemitism, anti-LGBTQ+, anti-Muslim hate, and anti-refugee rhetoric**.

Further Readings

This curated list of materials has been carefully selected by the co-leaders and secretariat of **Thematic Panel 3** to equip readers of this conclusion paper with essential knowledge on how extremists exploit the digital ecosystem.

Peer reviewed articles:

- **Far-right conspiracy groups on fringe platforms: a longitudinal analysis of radicalisation dynamics on Telegram** (2022) - examines the long-term radicalisation patterns of far-right conspiracy groups on fringe platforms, specifically analysing their dynamics on Telegram over time.
- **From Anti-Muslim to Anti-Jewish: Target Substitution on Fringe Social Media Platforms and the Persistence of Online and Offline Hate** (2023) - explores the shift in target groups within fringe social media platforms, analysing how anti-Muslim sentiment transitions into anti-Jewish narratives while examining the enduring impact of online hate on real-world behaviours.
- **Visual Generative AI in Warfare and Terrorism: Risk Mitigation through Technical Requirements and Regulatory Insights (2024)** - explores the role of visual generative AI in warfare and terrorism, examining risk mitigation strategies through technical requirements and regulatory insights.

Analyses:

- **The Radicalisation (and Counter-radicalisation) Potential of Artificial Intelligence** (2024) – explores how AI-driven chatbots can both enable and counter radicalisation.
- **Digital Pathways to Violence: the Tech Ecosystem Behind the Antioch Shooting** (2025) – examines how digital platforms facilitated the radicalisation of the Antioch shooter, highlighting the transnational spread of extremist narratives, the role of multiplatform engagement, and failures in AI-based security systems that contributed to the attack.
- **Automated Recruitment: Artificial Intelligence, ISKP, and Extremist Radicalisation** (2025) – explores how Islamic State Khorasan Province (ISKP) leverages AI-driven recruitment strategies, using generative AI, deepfake technology, and autonomous chatbots to amplify propaganda, personalise radicalisation efforts, and evade counter-terrorism monitoring.
- **Exploitation of Generative AI by Terrorist Groups** (2024) - examines how terrorist groups are increasingly exploiting generative AI, using automated content creation, deepfake technology, and AI-driven propaganda to enhance recruitment, spread misinformation, and evade detection.
- **The Great TikTok Migration: Western Extremists Flock to RedNote** (2025) - examines how Western extremists migrated to RedNote, a Chinese social media platform, following the TikTok ban in the U.S., highlighting how far-right groups adapted their tactics, engaged with Chinese audiences, and navigated content moderation challenges on the platform.

Reports:

- **The Next Paradigm-Shattering Threat? Right-Sizing the Potential Impacts of Generative AI on Terrorism** (2024) – examines how extremist groups experiment with AI tools for propaganda and recruitment.
- **Algorithms and Terrorism: the Malicious Use of Artificial Intelligence for Terrorist Purposes** (2021) – this UNCCT-UNICRI report explores the potential malicious uses of AI by terrorist organisations, highlighting risks such as automated propaganda, cyber threats, and AI-enabled attacks.
- **The Online Extremist Ecosystem-Its Evolution and a Framework for Separating Extreme from Mainstream** (2021) – introduces a framework for categorising online platforms based on their extremist content, distinguishing between mainstream, fringe, and niche spaces, as well as analysing how extremist narratives evolve within the digital ecosystem.
- **Early Terrorist Adoption of Generative AI** (2023) – examines the early adoption of generative AI by terrorist and extremist groups, highlighting how AI tools are being used to create propaganda, evade detection, and enhance operational security.
- **AI Extremism: Technology, Tactics, Actors** (2024) – provides new typologies and concepts to systematically chart AI-driven extremist tactics, offering insights for policymakers and practitioners in countering violent extremism.
- **Content moderation through removal of service: Content delivery networks and extremist websites** (2023) – examines the role of Content Delivery Networks (CDNs) in moderating extremist and terrorist content online, highlighting how platforms like Cloudflare influence the accessibility of such websites and the challenges in enforcing consistent content moderation policies.
- **Durably reducing conspiracy beliefs through dialogues with AI** (2023) – explores how AI-driven dialogues can effectively reduce belief in conspiracy theories, demonstrating that personalised, evidence-based interactions with AI can shift entrenched perspectives and promote critical thinking.
- **More is More: Scaling up Online Extremism and Terrorism Research with Computer Vision** (2025) – explores how computer vision techniques can enhance the analysis of online extremist ecosystems, demonstrating how automated image clustering and object identification can help researchers scale up investigations into extremist content.
- **The Impact of Technology on Radicalisation to Violent Extremism and Terrorism in the Contemporary Security Landscape** (2024) – examines how digital technologies, including the Internet, IoT, and social media platforms, have transformed the spread, recruitment, and operation of extremist movements, highlighting both security challenges and opportunities for countermeasures.

Webinars:

- **Radicalisation, Counter Radicalisation, and AI** – this webinar discusses how AI can amplify extremist messaging and how governments can use AI to combat radicalisation.
- **Artificial Intelligence and Radicalism: Risks and Opportunities** – this event features experts discussing how AI impacts radicalisation and terrorism, along with its potential benefits in countering extremism.
- **Generative AI's Counterterrorism Challenge and Opportunity** – highlights AI's disruptive impact on content moderation, online harms, and regulatory challenges.
- **Melodies of malice: Understanding how AI fuels the creation and spread of extremist music** – examining how far-right communities use AI platforms to create and spread extremist music propaganda across mainstream social media. It highlights the risks of AI-generated music in amplifying misinformation and offers policy recommendations for tech companies and regulators to counter this emerging threat.

Podcasts:

- **Digital Services Act (DSA) & TCO Regulation – A Comparison** – examines the differences, synergies, and enforcement mechanisms of these frameworks, highlighting their impact on online platforms—both large and small.
- **Small Platforms in the Spotlight: Complying with the TCO Regulation** – insights into the strategies these platforms use, and the support needed to navigate regulatory complexities.
- **The Fundamental Balance: Freedom of Expression and Online Safety** – delves into platform challenges, democratic discourse, and practical strategies for maintaining responsible content moderation in the digital space.
- **The TCAP: A Tool to Tackle Terrorist Content** – highlights how TCAP works, its impact on smaller platforms, and ongoing efforts to enhance transparency and functionality.

Product of the EU Knowledge Hub on Prevention of Radicalisation (EUKH)
Authored by Bledar Feta & Sara Monaci, Key P/CVE Experts
Secretariat of the Thematic Panel on New Technologies and the Online Dimension