POLITECNICO DI TORINO
Repository ISTITUZIONALE

Children and the Hybridised Threat of Online Radicalisation: Safeguarding in the Digital Age

Original
Children and the Hybridised Threat of Online Radicalisation: Safeguarding in the Digital Age / Monaci, S., Feta, B.. - (2025). (Conclusion Paper of Thematic Panel 3: New Technologies and the Online Dimension (3rd meeting), Working Group of EU Knowledge Hub on Prevention of Radicalisation Roma 16 -17 settembre 2025).

Availability:
This version is available at: 11583/3006282 since: 2026-01-06T11:48:07Z

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)

20 November 2026

CONCLUSION PAPER

Children and the Hybridised Threat of Online Radicalisation: Safeguarding in the Digital Age

Thematic Panel 3: New Technologies and the Online Dimension

EU Knowledge Hub on Prevention of Radicalisation (EUKH)

Third Meeting

Date: 17–18 September 2025
Location: Rome, Italy

EU Knowledge Hub on Prevention of Radicalisation

European Commission

1. Introduction

On 17–18 September 2025, the third meeting of the Thematic Panel on New Technologies and the Online Dimension (TP3) convened under the title "Children and the Hybridised Threat of Online Radicalisation: Safeguarding in the Digital Age." The gathering explored the escalating convergence of online harm, violent extremism, and child exploitation, with a specific focus on the radicalisation of children in digital environments. Day one centred on the hybrid nature of online threats as they affect children, examining how ideological manipulation, sexual coercion, and other forms of exploitation increasingly intersect across platforms. Discussions underscored the use of hybrid tactics, blending online subcultures, Child Sexual Abuse Material (CSAM), and Terrorist and Violent Extremist Content (TVEC), to target children[1], reinforcing the urgency of cross-sector collaboration and multidisciplinary engagement. Day two shifted toward solutions and spotlighting current and emerging interventions to protect children from online harm. The meeting's central conclusion was unequivocal: the growing involvement[2] of children in violent extremism as well as them being exploited online presents a rapidly evolving challenge for European institutions and EU Member States. Participants stressed the need for inclusive, disaggregated data collection, capturing age, ideology, and context, as a foundation for evidence-based policymaking and effective cross-sectoral responses. Another key outcome was the call for clearer practitioner mandates, simplified frontline guidance, and updated prevention content that addresses digital blind spots and the realities of child exploitation online. Panel members emphasised the pivotal role of parents in prevention and proposed the **Parents' Guide to Protecting Young Minds** as a practical outcome of TP3, an accessible resource designed to support digital awareness and early safeguarding through an ecosystem lens.

2. Key Insights and Takeaways: Children and the Hybridised Threat of Online Radicalisation

Between Victimhood and Agency: Rethinking Childhood in the Age of Digital Extremism: The hybridised threat of online radicalisation has exposed critical gaps in how childhood is defined, understood, and protected across jurisdictions. Terms like "child," "minor," "teen," and "youth" vary legally and culturally, complicating policy responses and safeguarding efforts. With terrorism-related prosecutions increasingly involving adolescents, even as young as 13 in recent cases in the United Kingdom (UK), the line between victimhood and agency is becoming blurred. Historical patterns of child involvement in extremist violence are now amplified by digital platforms, where grooming, exploitation, and instrumentalisation converge. This evolving landscape demands a recalibrated approach that recognises children as vulnerable targets, manipulated actors, and, crucially, still as victims within complex radicalisation ecosystems.

[1] For the purposes of TP3 meeting in Rome and this conclusion paper, the term 'children' refers to individuals under the age of 18. This terminology was adopted to ensure consistency within the panel's work and to navigate variations in national legislation across EU Member States regarding the definition of 'minors'. It is used here exclusively in the context of TP3 work and does not imply a recommendation for wider use.

[2] This growing trend is substantiated by the 2025 TE-SAT Report from Europol, which found that 133 individuals aged 12–20, over 29% of all terrorism-related arrests in Europe, were apprehended in 2024. Further evidence is provided by the UN CTED Trends Alert "Growing alarm as terrorist exploitation of children rapidly evolves", which highlights Member States' increasing concern over sophisticated online recruitment strategies targeting children and the challenges in mounting effective responses.

Key Takeaway: Re-evaluating the Definition of "Child" Across Legal, Policy, and Safeguarding Frameworks - Panel members stressed the urgent need to recalibrate safeguarding strategies in response to the growing involvement of children in terrorism-related cases. This shift highlights the limitations of current legal and policy definitions of childhood, which often fail to capture the complex interplay between vulnerability and agency in online radicalisation. To address this, participants proposed the development of a harmonised EU-wide framework that distinguishes between children, minors, and adolescents, aligning legal thresholds with developmental psychology and digital risk exposure. They also recommended age-appropriate intervention protocols that prioritise rehabilitation and tailored support over punitive measures, alongside specialised training for law enforcement, educators, and social workers to help them respond to adolescent radicalisation with informed, context-sensitive approaches.

From Historical Involvement to Digital Immersion: How the Internet Has Reshaped Children's Role in Terrorism: While children's involvement in terrorism is not new, the digital age has transformed how they are exposed, recruited, and instrumentalised. The internet is no longer separate from young people's lives; it shapes their identity and behaviour from an early age. This immersive environment allows easy access to violent, extremist, terrorist, and sexually exploitative content, including via mobile devices and often via encrypted platforms. Harmful digital cultures, ranging from gore communities to jihadi and neo-Nazi forums, blur the lines between ideology, entertainment, and abuse. In this hybridised threat landscape, children are not only victims but also manipulated participants, groomed into sextortion, self-harm, and both ideological and non-ideological forms of violence.

Parents' Guide to Protecting Young Minds
Supporting Digital Awareness and Empowerment through an Ecosystem Lens

As a practical outcome of the Thematic Panel 3, this guidance will offer a clear, accessible resource to help caregivers understand where and how children engage online, and to recognise early signs of radicalisation and exploitation. Unlike previous initiatives that primarily described risks and proposed control measures in isolation, this guidance takes a more holistic approach. It considers the broader context in which threats emerge, including emotional, social, and technological dynamics, and supports parents in communicating effectively with their children. By building on caregivers' lived experience, it empowers them to act as digital mentors, fostering confident, informed, and resilient engagement.

The guidance will explain the affordances of commonly used platforms, such as anonymity, private messaging, and algorithmic exposure, and how these features can facilitate risks including TVEC, CSAM, sextortion, 764-coded content, and grooming. Framed through an ecosystem lens, it positions parents within a wider network of schools, communities, and support services, recognising that safeguarding is a shared responsibility. Designed for real-world use, the guidance is a non-technical, accessible resource that would aim to fill a critical gap in current prevention efforts. As part of our Thematic Panel and a parallel structured voluntary cooperation among several Member States on the online dimension, it will also include practical advise on how to have meaningful conversations with children about these risks, supporting caregivers in their role as digital mentors.

To ensure relevance and impact, the panel recommended:
• Involving parents in testing and refining the resource through stakeholder consultation • Aligning with EU-level child protection efforts via the Working Group of the Procurator of Digital Services • Engaging the European Commission to support policy uptake and institutional coherence • Developing a chatbot to provide real-time, country-specific guidance and connect families to verified support services • Partnering with schools, using educators as trusted intermediaries to share the guide and raise awareness.

Key Takeaway: Safeguarding in the Age of Digital Immersion - The online-offline continuum of radicalisation requires a safeguarding response that reflects the speed, scale, and psychological depth of children's online engagement with harmful content. During the meeting, participants emphasised the vital role of families and schools in prevention. They proposed establishing cross-sector Digital Resilience Hubs in schools and youth centres, with structured parental involvement through training and support. These hubs would offer workshops, confidential sessions, and tailored digital literacy resources to help families

recognise risks and engage in open dialogue with children. This collaborative model embeds safeguarding into daily life, linking educators, practitioners, and parents. Participants also raised concerns about parental influence in youth radicalisation, noting that some parents may dismiss or even share extremist views. This highlights the need for sensitive outreach strategies that help practitioners navigate complex family dynamics while prioritising engagement and harm prevention. Recognising the central role of parents in prevention, panel members stressed the importance of informed and empowered caregiving and proposed the **Parents' Guide to Protecting Young Minds** as a practical tool to support digital awareness and early safeguarding.

Key Takeaway: Supporting Parents at the Critical Moment: Local Strategies to Enable Discreet, Non-Stigmatising Intervention - Panel members identified a pivotal moment in the radicalisation process: when parents first suspect their child's engagement with terrorist and violent extremist content online. This stage is often marked by fear, uncertainty, and hesitation, especially when families lack clear reporting pathways or fear stigma. Research shows many parents choose not to report concerns due to social pressure or institutional ambiguity. To address this, participants proposed developing localised strategies that clearly identify trusted institutions, such as youth services, social workers, or prevention officers, equipped to offer discreet support. These should include awareness campaigns, referral protocols, and training for frontline staff. Crucially, reporting mechanisms must protect family privacy and foster trust, enable early intervention and help prevent deeper radicalisation.

From Sextortion to Extremism: Mapping the Pipeline of Digital Harm Among Children: Participants raised serious concerns about the convergence of online child sexual abuse, violent extremism, and quasi-ideological digital subcultures. Online communities such as 764 and O9A[3] were cited as part of loosely connected networks where teens are both victims and perpetrators of livestreamed sextortion, self-harm, and abuse. A key concern was the pipeline from interpersonal exploitation to public violence, often driven by a complex mix of factors, including a desire for notoriety, emotional distress, and fragmented ideological influences, rather than a coherent belief system. Many children engage with ideology in fragmented, personalised ways, so-called micro-ideological formations, assembled from disparate online influences and tailored to peer-group identities. This challenges traditional models of radicalisation and calls for prevention strategies that reflect the fluid nature of digital belief systems. The meeting also highlighted gendered dynamics in online grooming, with anecdotal evidence suggesting that perpetrators are often young, heterosexual males targeting girls, some under 11, under the guise of romantic interest. Gender emerged as a critical factor in children radicalisation, with evidence from Spain showing boys gravitating toward extreme right ideologies and girls toward extreme left[4]. These patterns underscore the need for prevention approaches tailored not only by age but also by gender, recognising distinct vulnerabilities and pathways into radical narratives.

Key Takeaway: Beyond Counter-Narratives: Addressing the Emotional and Social Drivers of Children in Radicalisation - Prevention strategies must go beyond ideological counter-narratives to tackle the

[3] 764 is a decentralised online network known for its involvement in livestreamed sextortion, CSAM, and psychological manipulation of children. It is ideologically aligned with O9A, the Order of Nine Angles, a militant accelerationist group rooted in neo-Nazi and occultist beliefs. Both networks exploit digital platforms and gaming environments to radicalise and abuse teens, who are often simultaneously victims and perpetrators. Their activities illustrate the convergence of violent extremism and child exploitation within the hybridised threat landscape.

[4] Pilar Rodriguez Martinez, Christian Roith, Antonio Jesús Segura Sánchez & Ana Maria López Narbona (2023) Extremist and pro-violence attitudes of Spanish adolescents in secondary schools, Cogent Social Sciences, 9:1, 2239542. Available at: https://www.tandfonline.com/doi/pdf/10.1080/23311886.2023.2239542

emotional, social, and performative factors that draw adolescents into harmful digital cultures. Many children engage with extremist spaces through peer validation, notoriety-seeking, and emotional vulnerability rather than ideology alone. To address this, participants proposed child-led digital peer support programmes in schools and community hubs, combining mental health support, online culture literacy, and safe spaces for dialogue. These initiatives should be facilitated by trained child protection mentors and supported by psychologists and educators. EUKH could play a key role by curating best practices, coordinating cross-country pilots, and offering evidence-based guidance to ensure interventions are scalable, context-sensitive, and rooted in the lived realities of digitally immersed children.

Key Takeaway: Bridging the Data Gap and Strengthening Data Foundations for Children-Involved Extremism and Child Protection - Participants stressed the urgent need to better conceptualise and disaggregate emerging forms of children-involved violence and extremism in the digital age. They called for the systematic development of comprehensive datasets that map groups, incidents, ideological markers, and behavioural patterns, including overlaps with school shooters, new religious movements, and gendered dynamics. A broad, inclusive data strategy is essential to detect trends, test hypotheses, and avoid premature conclusions. At the same time, participants highlighted the lack of accessible, systematic data on children's involvement in online harm and radicalisation cases, particularly in Western Europe, where child protection laws restrict public records. They advocated for a secure, anonymised, and transnational data-sharing framework to enable joint analysis by law enforcement and trusted researchers while safeguarding children's identities. The panel also emphasised the importance of integrating gender-sensitive analysis into counter-terrorism and Continuing Professional Development (CPD) frameworks[5], recognising the roles of girls not only as victims but also as active participants in radicalisation ecosystems. Addressing major gaps in data linking mental health, family background (including substance use), and online behaviour was seen as critical to improving vulnerability assessments and targeted responses. Finally, participants noted a definitional gap around forms of violence rooted in nihilism or identity denial, which often fall outside existing policy frameworks and require a public health approach. The EUKH was identified as a key facilitator to coordinate practitioner-led data collection, uphold ethical standards, and address urgent knowledge gaps in child protection and radicalisation research.

Institutional Mandate Gaps in Addressing Online Threats to Children: A key challenge within international organisations is the absence of clear mandates to address online threats targeting children. Many organisations are limited in their ability to engage with child-related digital issues, resulting in fragmented responses and insufficient support for Member States. Coordination is further undermined by siloed expertise: not only among international organisations, but also within national institutions. Child-focused entities like the United Nations International Children's Emergency Fund (UNICEF) or national child protection authorities, often lack specialised knowledge on online radicalisation, while cyber-focused bodies may hesitate to collaborate with child protection actors. This structural disconnect hampers the development of comprehensive, cross-sectoral strategies needed to safeguard children in digital environments.

[5] Continuing Professional Development (CPD) frameworks refer to structured approaches that support professionals in maintaining, enhancing, and expanding their knowledge, skills, and competencies throughout their careers. In the context of counter-terrorism and safeguarding, CPD frameworks ensure that practitioners, including educators, law enforcement, social workers, and civil society actors, are equipped with up-to-date training, ethical guidance, and interdisciplinary tools to respond effectively to evolving threats, including online radicalisation and gendered dynamics of extremism. These frameworks often include accredited learning modules, peer exchange, scenario-based exercises, and reflective practice tailored to specific roles and regional contexts.

Key Takeaway: Building Ethical Research Frameworks Through Cross-Sector Collaboration - Conducting research with children across EU Member States remains complex due to varying legal and ethical requirements. Restrictions, such as mandatory parental or staff presence, can compromise the authenticity of children's responses. To address this, researchers should collaborate with international and child-focused organisations like UNICEF to co-develop ethical protocols tailored to digital environments. Such partnerships would offer mutual benefits: researchers gain guidance for sensitive engagement, while child protection bodies, often lacking expertise in online radicalisation, can use insights to strengthen policy responses. Structured collaboration ensures that research with children produces high-quality data to inform effective child protection strategies.

From Virality to Responsibility - Rethinking Influencer Engagement for Online Child Safety: Panellists explored the increasingly complex role of influencers in shaping children's online experiences. While not all influencers promote terrorist and violent extremist content, their direct engagement with children, often through emotionally resonant storytelling, challenges, or lifestyle content, can subtly guide young audiences in ways that mirror grooming or radicalisation dynamics. An example came from Bulgaria's Safer Internet Centre, which launched a voluntary certification scheme for "responsible influencers."[6] Creators who meet child safety criteria across various harm categories receive a digital label, though uptake remains limited and skewed toward non-viral female influencers. Some of the panel members proposed scaling such initiatives through EU-level coordination, visibility, and incentive structures, such as increased reach, promotional boosts, or platform benefits, to encourage broader participation. The discussion also referenced YouTube's former Creators for Change initiative, which offered visibility, credibility, and access to high-profile collaborations for influencers promoting pro-social messaging. This model demonstrates how platforms can leverage their creator engagement departments to reward safety-conscious behaviour and foster inclusive online cultures. However, panel members expressed mixed views on the strategic use of influencers in counter-extremism and digital safety campaigns. While some saw potential in leveraging influencers for disinformation literacy and children empowerment, others warned of serious pitfalls. A counter-extremism initiative in Australia backfired when influencers were unaware of the government funding source, leading to community backlash and reputational damage. Scepticism was also voiced toward tech companies that promise large-scale support, such as free content creation resources, but fail to deliver, leaving civil society and governments underfunded and unsupported.

3. Key Insights and Takeaways: Navigating Digital Vulnerabilities Across Online Spaces and At-Risk Groups

Socialisation Over Content: Rethinking Radicalisation Pathways in Youth Gaming Ecosystems: Participants noted that in gaming environments, the risk of radicalisation stems not only from terrorist and violent extremist content but also and even more from the social dynamics embedded in gameplay. Rapid trust-building among co-players fosters tight-knit communities where peer influence can shape worldviews. Experts cautioned against overinterpreting provocative behaviour, as children often act out of curiosity or peer pressure without ideological intent. The absence of child-targeted propaganda suggests that gaming culture itself may serve as a conduit for ideological messaging. This calls for nuanced assessments that distinguish between provocation and genuine radicalisation, as well as for interventions

[6] See more information here: https://safefluencers.bg/

that address relational dynamics driving youth vulnerability. Observational research from the GEMS project in Athens showed that children, some under 11, frequent gaming cafés and migrate across platforms like Discord, Telegram, and YouTube, where they may encounter glorified depictions of violence. Teachers, though aware of the risks, often avoid engaging with gaming spaces due to discomfort or fear of legitimising them as entertainment venues.

Key Takeaway: Mapping Gaming Spaces and Threat Surfaces: A Prerequisite for Targeted Online Harm Prevention - Participants emphasised the need to develop clear typologies of digital environments where gaming-related harms emerge, including in-game spaces, gaming platforms (e.g. Steam, Roblox), adjacent platforms (e.g. Twitch, Discord), and broader social media ecosystems. Each presents distinct risks requiring tailored moderation strategies. Communication modes, text, voice, and video, create complex "threat surfaces" for extremist content, especially through user-generated material. Participants noted that users can build ideologically charged environments and share content, such as reenactments of violent attacks, across platforms like TikTok and YouTube. Limited searchability within games like Minecraft or Roblox complicates detection. This highlights the need for cross-platform monitoring and context-aware tools to distinguish gameplay from genuine harm, particularly in spaces frequented by children.

Key Takeaway: Building Trust-Based Alternatives and Strengthening Media Literacy in Gaming Ecosystems - Panel members emphasised the urgent need to create alternative, trust-based communities within gaming spaces to counter harmful peer dynamics and online radicalisation. Examples such as the Dutch "Gaming with the Police" initiative and Denmark's formal police patrols in gaming environments demonstrate how law enforcement can build rapport with minors and offer safe reporting channels. These models work best in close-knit societies with high institutional trust and highlight the potential of proactive engagement. In contrast, the EU-funded EPIC-WE project offered a different model, using games as a cultural amplifier to foster bottom-up, child-led interaction. It demonstrated how creative, non-policing approaches can also build trust and promote positive engagement among children.

Key Takeaway: Mobilising Parents as Active Participants in Gaming Spaces to Strengthen Child Safety and Awareness - Participants stressed the importance of moving beyond fear-based narratives and recognising gaming as a largely positive social environment, while acknowledging the presence of harmful actors who exploit these spaces. A key recommendation was to involve parents as active participants in their children's gaming lives. Inspired by Nordic Street patrol models, one proposed solution is to organise community-based gaming sessions where children and parents play together, helping families understand the dynamics and risks firsthand. EU-funded initiatives could also support online environments that foster trust, media literacy, and early detection of harm through intergenerational gameplay. Rather than rigid platform lists, experts advocated for focusing on moderation practices, transparency, and reporting tools, equipping families to navigate digital spaces safely and collaboratively.

From Avatars to Porn Portals: Unseen Pathways of Children Vulnerability: Participants emphasised the role of anonymity and avatar-based identities in enabling radicalisation, exploitation, and harmful content in online spaces frequented by children. While these features support self-expression, they also obscure accountability and facilitate grooming and extremist messaging. A pressing concern was the ease with which children access pornography platforms, where age verification is often ineffective. Research shows that much mainstream content depicts violence against women and girls, raising serious concerns about desensitisation among children. The overlap between pornographic and gore websites suggests a broader ecosystem of digital harm. Participants called for a more integrated understanding of these environments,

recognising that radicalisation risks extend beyond traditional platforms into entertainment, social, and adult content domains.

Key Takeaway: Empowering Children as Digital Upstanders: A Scalable Model for Countering Online Hate and Extremism - Participants agreed that while content moderation is vital, it cannot address the complex dynamics of online hate alone. A pilot initiative in the Netherlands trains youth to act as bystanders and upstanders, empowering them to intervene and then train their peers, creating a ripple effect of resilience. Meanwhile, grassroots efforts are emerging beyond formal structures, with youth workers becoming influencers on platforms like Discord, engaging young audiences and responding to tensions in real time. These approaches underscore the value of children-led, peer-driven strategies in building safer digital ecosystems.

Key Takeaway: Language Matters - Avoiding Stigmatisation in Reintegration Efforts - The terminology used by authorities plays a critical role in shaping public perception and supporting the reintegration of radicalised children. Labelling children as "extremists" or "terrorists" risks vilification and undermines rehabilitation. Countries like Albania offer a more constructive approach, referring to children of foreign fighters as "returnees," recognising them as survivors of conflict and manipulation. Neutral, non-stigmatising language fosters trust, reduces shame, and supports recovery. Panel members emphasised that frontline practitioners must be trained not only in deradicalisation but also in the careful use of language to enable healing and inclusion.

Bridging the Gaps in Online Content Removal and Youth Radicalisation: Traditional approaches are often too slow to address online extremist content. ATKM - Authority for the Prevention of online Terrorist Content and Child Sexual Abuse Material, as the entity mandated to implement the TCO in the Netherlands and enforce national CSAM legislation, stands out as an interesting model. Due to its unique mandate, it has the capacity to respond to hybrid threats that span both terrorism and child exploitation. In the Netherlands, persistent jihadi content and emerging threats like nihilistic accelerationism reflect the evolving nature of child radicalisation. Experts from ATKM, the International Centre for Counter-Terrorism (ICCT), and Leiden University warn of COM/GORE[7] networks circulating violent and harmful material, including CSAM, within closed communities. While terrorist content is limited, it remains easily accessible and contributes to the desensitisation of children. The rise of "awful but lawful" content, extreme material outside current legal frameworks, poses new challenges for regulation. Although AI offers scalable moderation, its use is constrained by legislation, ethical and technical concerns, and the need for human oversight.

[7] COM/GORE networks are transnational online ecosystems that fuse competitive abuse with ultraviolent content, where users gain status through acts of harm, degradation, or shock media. COM spaces often overlap with misogynistic and nihilistic subcultures, while GORE platforms circulate graphic extremist material to desensitise and radicalise. Together, they create a hybridised threat landscape that exploits youth vulnerability and drives radicalisation through notoriety and peer validation rather than coherent ideology.

4. Law Enforcement Response to Online Radicalisation of Minors

Law Enforcement Struggles to Keep Pace with Children in Decentralised Digital Ecosystems - As radicalisation shifts into decentralised digital ecosystems, powered by encrypted platforms, blockchain technologies, federated networks, pseudonymous identities, and cross-border hosting, law enforcement agencies (LEAs) face growing challenges in protecting children. Legal frameworks such as the TCO regulation are difficult to apply in these fragmented environments, while technical barriers like encryption, anonymity, and distributed hosting obstruct investigation and takedown efforts, even when referrals are made by police authorities. Critically, children often adopt and navigate these technologies faster than enforcement can respond, immersing themselves in digital subcultures shaped by older peers. This generational and operational gap demands urgent investment in multidisciplinary expertise, proactive digital literacy, and child-specific safeguarding strategies tailored to decentralised ecosystems.

Key Takeaway: Reframing Collaboration as a Prerequisite for Effective Prevention - While public-private cooperation remains central to counter-radicalisation, the Rome meeting underscored a deeper gap: the lack of consistent public-to-public coordination especially among police authorities. Without trust and structured information-sharing, both across borders and within individual states, efforts remain fragmented. This includes coordination between ministries, among law enforcement units, and across institutions operating within the same national context as well as across units that operated under the same institution. When these public actors fail to align, private sector engagement risks losing impact and sustainability. This is especially critical for safeguarding children, where fragmented mandates and siloed data hinder early intervention. Multidisciplinary task forces and cyber-society partnerships must be grounded in strong internal alignment, both within individual institutions and across collaborating public authorities. Operationalising public-to-public collaboration is not optional, it is essential.

Key Takeaway: Avoiding the Overextension of Counterterrorism Measures - Some panel members expressed concern over the growing tendency among some European law enforcement bodies to label certain online communities as terrorist entities, primarily to facilitate content removal under TCO regulation. While this approach may offer short-term operational benefits, researchers warned that terrorism designations must not be used as a convenience tool. Such labels carry serious legal and ethical consequences and must be grounded in rigorous, rights-based standards. Law enforcement representatives acknowledged the pressure to act swiftly, often relying on broad terrorism definitions to enable rapid intervention. However, this practice risks stretching legal boundaries and redefining terrorism in ways that may be disproportionate, especially when applied to children. Some panel members strongly cautioned against expanding counterterrorism frameworks to address online harms involving children. Instead, they called for the development of a distinct legal and welfare-based approach, separate from counterterrorism, that reflects the realities of emerging digital threats and outdated CSAM legislation. This shift is essential to ensure proportionate, child-sensitive responses that uphold fundamental rights and avoid the criminalisation of vulnerable groups.

5. Civil Society Approaches to Online Radicalisation of Children

Clarifying and Strengthening Civil Society's Role in Preventing Online Radicalisation of Children - Participants affirmed the vital role of Civil Society Organisations (CSOs) in countering online radicalisation among children, particularly through media literacy, community engagement, and early prevention. However, the discussion stressed the need to clearly define CSOs responsibilities in relation to state institutions, given the sensitive nature of working with children. To ensure safe and rights-based engagement, CSOs must be trained in child protection strategies by expert bodies such as UNICEF. Interventions must also reflect the realities of a post-truth era, where misinformation and emotional manipulation are widespread. Effective programming requires cultural competence, strict adherence to privacy standards, and alignment with frameworks like the United Nations Convention on the Rights of the Child (UNCRC). Moreover, initiatives should address structural grievances and include child-informed feedback loops that connect practitioners, researchers, and policymakers. A public health approach, viewing radicalisation as a behavioural and social issue, can help build protective factors and offer confidential support, avoiding the pitfalls of securitisation.

Key Takeaway: Empowering Civil Society Through Data-Driven Oversight of Online Platform Accountability - A key recommendation from the panel was to leverage the DSA transparency database as a strategic tool for civil society organisations and researchers working to counter online radicalisation, particularly among children. This database provides structured access to information on how Very Large Online Platforms (VLOPs) moderate illegal content, including the types of measures taken, frequency of enforcement, and algorithmic interventions. For civil society actors, this offers a valuable opportunity to move from reactive advocacy to evidence-based engagement, supporting policy development, platform accountability, and the design of more targeted interventions. When integrated into child-focused programming, the database can help CSOs better understand platform dynamics, identify gaps in content moderation, and advocate for stronger protections for children online. It also reinforces the need for civil society to be equipped not only with ethical and safeguarding training, but also with analytical tools that enable meaningful participation in digital governance.

6. Addressing Chatbot Influence in Child-Focused Online Radicalisation

Risks of Child - Targeted Chatbots in Radicalisation Contexts - Panel members warned that AI chatbots, especially those simulating digital personas, pose a growing risk in the online radicalisation of children. By acting as trusted companions, these bots can foster emotional dependency and expose children to ideological grooming. The threat is amplified by weak age safeguards, manipulative designs, lack of regulation in decentralised environments, and major detection gaps for law enforcement, particularly when chatbots operate within gaming or social platforms. The discussion also highlighted two critical challenges: the legal and ethical ambiguity surrounding chatbot-related research under the Digital Services Act (DSA), and the absence of transparency mechanisms to monitor their deployment and potential harms. A proposed solution is to include chatbots in the DSA's transparency reporting obligations, enhancing oversight and aligning with broader efforts to incorporate terrorist-operated websites into the

Terrorist Content List (TCL). Without ethical standards, transparent design protocols, and a multi-stakeholder watchdog framework, these systems may become covert vectors of influence. Addressing this issue must be a priority in future safeguarding strategies.

Key Takeaway: Safeguarding Children from Chatbot - Facilitated Radicalisation Through Ethical AI Governance - To counter the risks posed by conversational AI, governments, CSOs, and tech developers must co-create child-specific ethical standards and regulatory protocols. These should include mandatory privacy-by-design safeguards, robust age verification tools/mechanisms, and transparent data handling practices. A multi-stakeholder watchdog, comprising educators, child psychologists, and digital rights experts, should be established to audit chatbot deployments targeting children. Awareness campaigns for parents and schools must explicitly address chatbot-related risks, ensuring that digital literacy encompasses not only platforms, but also the AI systems embedded within them. However, these efforts must also acknowledge the technical limitations in controlling chatbot behaviour, particularly in decentralised or rapidly evolving environments, underscoring the need for adaptive, layered safeguards rather than reliance on static regulation alone.

Annex

1. Recommendations and Actionable Solutions

The table below presents key recommendations and actionable solutions proposed by members of the TP3 during their meeting in Rome.

Recommendation/Actionable Solution	Brief Description
Address Data Gaps and Funding Instability	Invest in inclusive datasets disaggregated by age and ideology to inform child-focused interventions, and secure stable funding for online initiatives that operate beyond local geographies. This data gap, compounded by unstable funding for digitally focused initiatives that lack local anchoring, poses a significant barrier to sustained impact and evidence-based intervention.
Establish Local Points of Contact for Parents and Teachers	Establish accessible support structures at the local or municipal level to assist educators, parents, and peers in navigating online risks, complemented by EU-wide knowledge sharing and contextual adaptation. These contact points should function as one-stop hubs where individuals can report concerns about children engaging with problematic content, access clear guidance, and receive information on available alternatives and support mechanisms.
Support EU-Level Tooling for Member States and IRUs	Facilitate the joint development of digital tools, AI-based or otherwise, across EU Member States and Internet Referral Units (IRUs) to strengthen the prevention, detection, and coordination of online threats involving minors. These tools should specifically support efforts to identify and respond to child-targeted radicalisation, exploitation, and harmful content, ensuring that interventions are timely, rights-based, and aligned with child protection standards.
Improve Platform Design for Child Safety	Encourage platforms to go beyond basic age verification by exploring features that anticipate circumvention tactics (e.g., VPN use), and by integrating insights from abuse prevention and behavioural analysis to better protect children in persistent digital environments.
Expand Detection Capabilities of LEAs	Strengthen the technical capacity of law enforcement authorities to detect and respond to online radicalisation of children, particularly within decentralised platforms and emerging digital ecosystems. This includes enhancing tools and methods for identifying harmful content, extremist grooming tactics, and cross-platform coordination signals, while ensuring child-sensitive protocols and alignment with EU child protection standards.
Foster Public–to-Public Cooperation	Prioritise collaboration between national and international public sector entities, such as police forces, child protection agencies, and

	Internet Referral Units (IRUs), to strengthen coordination and response mechanisms. Particular emphasis should be placed on improving the sharing of knowledge and operational information related to children, especially in jurisdictions where such cooperation is currently limited or fragmented. Establishing secure, child-sensitive channels for cross-border data exchange can help identify emerging threats, support timely interventions, and ensure that law enforcement efforts are aligned with child protection standards across the EU.
Build Multidisciplinary Teams within Law Enforcement	Establish dedicated multidisciplinary teams within law enforcement agencies, particularly in departments working with children and monitoring complex online content. These teams should bring together experts from child protection, digital forensics, psychology, and counter-extremism to better understand the nuanced risks behind the content children consume online. Such integrated structures will enable more informed, coordinated, and child-sensitive responses to emerging digital threats.
Strengthen Cooperation Between Civil Society and Tech Companies	Foster meaningful, sustained partnerships between CSOs and technology companies to address algorithmic harms affecting children, particularly in search environments, recommendation systems, and content discovery pathways. CSOs can contribute valuable insights from frontline experience, helping platforms understand how radicalisation, emotional manipulation, and misinformation reach children through algorithmic amplification.
Collaborate on AI and Chatbot Safety	Promote structured collaboration between companies, researchers, and child protection experts to test and monitor AI systems, particularly chatbots and generative tools that interact with or are accessible to children. This includes conducting safety audits, behavioural testing, and misuse simulations to identify risks such as grooming, emotional manipulation, exposure to extremist content, or inappropriate advice. Developers should be encouraged to implement child-sensitive safeguards, including age gating, content filters, and escalation protocols. CSOs and educators should be involved in co-designing these systems to ensure they reflect real-world parenting and child engagement needs.
Develop Red-Teaming Protocols for AI Systems	Support the structured involvement of civil society organisations in red-teaming exercises to stress-test AI systems, particularly those interacting with or accessible to children. These protocols should simulate real-world scenarios to uncover vulnerabilities related to radicalisation, emotional manipulation, and exposure to harmful content. Civil society actors, especially those with expertise in child protection, psychology, and digital literacy, can help identify edge cases and unintended consequences that may not be visible through technical audits alone. Red-teaming should be conducted in coordination with platform developers, regulators, and child rights experts, ensuring that findings lead to actionable safeguards, improved moderation, and ethical design standards.

Leverage Transparency Tools (e.g., DSA Database)	Use regulatory datasets, such as the Digital Services Act (DSA) Transparency Database, to monitor platform behaviour, inform advocacy efforts, and design evidence-based interventions targeting online risks to children. To maximise impact, train relevant stakeholders, including civil society actors, educators, and child protection professionals, on how to access, interpret, and apply these tools effectively within their local and national contexts.
Adapt Literacy Tools to Local and Cultural Contexts	Ensure that digital literacy efforts are tailored not only to regional trust levels, policy environments, and community needs, but also to the specific realities of minors. This includes age-appropriate content, culturally sensitive messaging, and formats that resonate with children across diverse settings.
Build Trust in Interventions	Design civil society-led initiatives that avoid perceptions of censorship and instead focus on behavioural understanding and the empowerment of children. These interventions should foster open dialogue, promote critical thinking, and equip children with tools to navigate online risks confidently.
Develop Age-Specific Messaging Strategies	Create tailored communication and counter-narratives that reflect the developmental needs and emotional realities of children, avoiding generic or blended approaches.
Engage Children in Message Creation	Involve children directly in designing digital literacy and prevention content to ensure relevance, authenticity, and emotional resonance.
Strengthen AI and Chatbot Safeguards	Implement strict ethical standards and privacy-by-design protocols for AI systems interacting with children, including red-teaming to test for manipulation or harm.
Promote Critical Thinking Through AI Tools	Support development of child-friendly AI applications that build resilience and critical thinking, while continuously assessing risks and limitations.
Train Practitioners in Child Protection	Offer specialised training for online practitioners and civil society actors working with children, grounded in child rights frameworks such as the UNCRC.
Leverage EUKH Training Opportunities	Use the EU Knowledge Hub to request and design tailored trainings focused on child protection in digital environments and ethical engagement with children.
Integrate Online Safety into School Curricula	Encourage the European Commission to update key competence frameworks and promote national adaptation of curricula that include digital literacy, media literacy, online risks, and well-being, supported by mentoring and community role models. Integrate digital literacy into core education curricula as a foundational skill, equivalent in importance to native language education, to ensure that children understand the risks, responsibilities, and dynamics of the online world before harm occurs.
Introduce Bystander Training for Youth and Caregivers	Adapt tools like Australia's bystander training to empower children and caregivers to recognise, respond to, and report online risks, fostering a culture of shared responsibility and early intervention.

Establish Age-Sensitive Guidelines for Device Use	Develop national frameworks that set age-appropriate thresholds for phone and digital device exposure among children, grounded in educational and developmental research, building on models like Spain's expert-led approach. Support independent, cross-country research to map and evaluate national approaches to regulating device use and online safety for children, identifying gaps and good practices.
Ensure Parental Awareness and Engagement	Design outreach and training programmes to help parents understand digital risks, age-appropriate boundaries, and how to support healthy digital habits at home. Panel members emphasised the importance of promoting digital citizenship by educating parents about the internet, its risks, dynamics, and opportunities, so they can better support and protect their children online.

2. 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". They would be particularly useful in helping to build from past and current initiatives and to take advantage of the positive outcomes of the different experiences. What follows represents a non-exhaustive list of cases addressed by the participants during the panel discussion.

Better Internet for Kids (BIK): A Comprehensive European Resource for Safer Digital Engagement

The Better Internet for Kids initiative is a flagship European effort designed to support safer and more empowering online experiences for children and adolescents. It offers a rich suite of resources, including targeted campaigns which promote critical thinking and responsible digital behaviour. BIK also provides practical tools such as an app guide with search functionalities, helping users identify appropriate applications based on age, purpose, and safety features. Its extensive library includes thematic guides on online video games, positive online content, and parental control strategies, making it a valuable reference for families, educators, and practitioners.

Australia's New Industry Codes for Child Online Safety

On 9 September 2025, the Australian eSafety Commissioner registered six new industry codes designed to strengthen child protection across the digital ecosystem. These codes target exposure to 'class 2' material under the Online Safety Act, including online pornography, high-impact violence, and self-harm content, and introduces specific rules for AI companion chatbots capable of generating explicit material. Developed in collaboration with industry, the codes enshrine safety obligations across the technology stack, including app stores, social media platforms, equipment providers, and messaging services. Notably, they introduce new age assurance requirements to reduce children's access to harmful content and promote proactive safety measures.

Playing IT Safe - A play-based initiative designed to teach children online safety through interactive activities

Developed by the eSafety Commissioner in collaboration with the Alannah & Madeline Foundation and the Australian Federal Police, Playing IT Safe offers a suite of engaging resources for families and educators. These include online games, classroom activities, and conversation starters that help children understand key safety concepts, such as asking for help, making good choices, and sharing digital content responsibly. The platform encourages co-play between parents and children, fostering trust and early digital literacy in a safe, age-appropriate environment.

Meta's Updated AI Chatbot Guardrails for Child Safety

Meta's revised AI chatbot guardrails introduce stricter protections to prevent inappropriate interactions with children. The approach prohibits romantic or sexual roleplay involving children, restricts advice on intimacy, and ensures sensitive topics are addressed only in educational or clinical contexts. This approach aims to reduce exploitation risks and promote safer, age-appropriate chatbot engagement.

Aldous: AI-Driven Dialogue for Targeted Deradicalisation

Aldous, Mythos Labs' AI-powered chatbot, supports deradicalisation efforts by engaging at-risk individuals in personalised conversations that guide them away from extremist ideologies. Beyond dialogue, Aldous tailors psychosocial interventions based on user responses, helping practitioners assess risk levels, offer targeted support, and scale prevention efforts across diverse contexts.

Spain's Expert Committee Report on Safe Digital Environments for Children and Adolescents

Commissioned by the Ministry of Youth and Children and presented to the Council of Ministers in December 2024, this report (in Spanish) outlines a comprehensive roadmap for safeguarding minors in digital spaces. Developed by a multidisciplinary committee of 50 independent experts, the 150-page document offers an in-depth diagnosis of the technological risks facing children and adolescents, including industry responsibility, social media exposure, and the role of families and schools. It proposes 107 actionable measures grouped into short, medium, and long-term implementation phases. Key recommendations include age-specific device use guidelines, mandatory parental controls, regulation of content creators and sharenting, and strengthened industry obligations.

Campamento Digital: Empowering Children and Families for Safe Online Engagement

Campamento Digital is a Spanish initiative dedicated to promoting digital safety, media literacy, and responsible technology use among children, families, and educators. Through interactive resources, workshops, and educational campaigns, it helps young users navigate the online world with confidence and awareness. The platform offers practical guidance on topics such as privacy, cyberbullying, and healthy screen habits, while also encouraging co-learning between parents and children.