Erasmus School of Social and Behavioural Sciences

Autoriteit online Terroristisch en Kinderpornografisch Materiaal

From Online Terrorist Content Exposure to Real-World Mobilisation: Understanding Susceptibility, Assessing Risk, and Informing Interventions

summary

Stavroula Spernovasili, Dominika Grudzień, Neelav Novo Parashar
Erasmus University Rotterdam

Executive Summary

The Authority for the prevention of Online Terrorist Content and Child Sexual Abuse Material (ATKM) assesses whether online material meets the legal criteria for terrorist content under Regulation (EU) 2021/784 and may therefore require removal. Within this mandate, the present report examines how behavioural and psychological evidence can provide context for identifying characteristics of terrorist content that may carry a greater potential to facilitate radicalisation or movement towards real-world mobilisation. The report does not seek to assess or profile the individuals sharing such material. Instead, it considers how different forms and functions of content, including ideological expression, violent imagery, recruitment material, gamified participation, and operational or tactical information, may be interpreted and prioritised.

The report first describes how the contemporary online environment differs from the centralised propaganda systems traditionally examined in radicalisation research. Extremist content is now frequently distributed through decentralised and participatory spaces in which humour, memes, gaming references, competition, social recognition, and peer interaction can contribute to engagement. These dynamics are also visible in loosely organised networks that reward escalating acts of violence or self-harm. Children and adolescents may be particularly exposed to this environment because violent material can be encountered through social media, video games, streaming platforms, and algorithmic recommendation systems, including without being actively sought.

The report then reviews the psychological, behavioural, and neurological evidence concerning exposure to violent digital content. Repeated exposure may contribute to desensitisation, reduced empathic responding, moral disengagement, aggressive priming, and more permissive attitudes towards violence. Some studies also associate violent-media exposure with increased aggression and other adverse outcomes. However, these effects are generally modest, findings are not fully consistent, and much of the evidence is correlational or based on laboratory measures that do not reflect serious real-world violence. The evidence therefore does not support treating exposure to, or sharing of, violent content as a direct predictor of mobilisation. Rather, exposure should be understood as one probabilistic influence whose effects depend on the interaction between individual vulnerabilities, social circumstances, and protective factors.

The report subsequently examines factors that may increase susceptibility to gamified extremist environments. These include psychological strain, social isolation, unmet needs for belonging and recognition, identity uncertainty, sensation-seeking, and limited family or community support. Gamified structures may reinforce engagement by rewarding participation, status, competition, and behavioural escalation. Conversely, parental involvement, supportive relationships, digital literacy, community belonging, and access to alternative sources of identity and meaning may reduce susceptibility. These factors are presented as contextual explanations rather than as a checklist or a basis for ATKM to infer an individual's psychological characteristics from content.

The operational section considers how content and, where lawfully available, associated behavioural signals may be interpreted more systematically. It discusses four heuristic types of content-sharing behaviour: ideological-operational content, status-driven network content, performative shock content, and incidentally redistributed content. Building on this distinction, the report proposes a provisional risk-tiered framework organised around four dimensions: escalation, network, ideology, and capability and operational behaviour. Operational indicators, such as tactical learning, logistical planning, weapon acquisition, target selection, reconnaissance, or attack preparation, are weighted most heavily because they may distinguish movement towards mobilisation more reliably than ideological expression alone.

The framework assigns content to minimal, lower, medium, or high-risk tiers to support prioritisation, but it remains conceptual rather than diagnostic and requires piloting, inter-rater reliability testing, legal safeguards, and calibration against relevant case outcomes.

Finally, the report presents recommendations across three levels of prevention. Primary prevention focuses on parental awareness, media literacy, digital resilience, and education for young people. Secondary prevention includes search-based redirection, credible-messenger interventions, counter-narratives, active-inoculation games, and referral to psychosocial support by stakeholders with the appropriate mandate and access to user-level information. Tertiary and operational measures include prioritising content containing operational or tactical indicators, strengthening trained human review of coded or ambiguous material, introducing technical friction into platform design, and supporting cross-platform hash-sharing for known extremist content. Together, these recommendations aim to strengthen prevention and content prioritisation without treating ideological or provocative expression alone as evidence of an individual’s progression towards violence.