Radicalisation Awareness Network
RAN Policy Support

Malign use of Algorithmic Amplification of Terrorist and Violent Extremist Content

Victoria Jordan, Kristin Thue & Jacopo Bellasio

RAND EUROPE

Study context and scope

How is algorithmic amplification used to promote terrorist and violent extremist content and how can the phenomenon be addressed?

1. What is algorithmic amplification and how is it or can it be used to promote terrorist and violent extremist content?
2. What is the extent of the current threat posed by the potential misuse of such algorithms?
3. What is the role of the private sector in addressing this challenge?
4. What actions have already been taken by private-sector actors to address the phenomenon of algorithmic amplification to promote terrorist and violent extremist content?
5. What gaps, opportunities and challenges should policymakers address and consider?

Methodology and caveats

Literature review

Key informant interviews

Internal analysis workshops

Defining algorithmic amplification

Several algorithms with amplification functions

A structural feature of digital platforms

Working definition:
Process of automated content promotion online for engagement-driving purposes

Contextual understanding

Inadvertent amplification of terrorist and violent extremism content can happen as a result of recommender algorithms promoting content with high levels of engagement

Terrorist and extremist groups have learnt to manipulate online infrastructure through deceitful strategies to maximise the reach of their material

Terrorist and extremist groups combine these approaches into broader deceitful tactics designed to support their influence operations

Understanding of the current threat

Today, risks associated with algorithmic amplification are principally linked to amplification of so-called fringe or borderline content on mainstream platforms

The lack of transparency, access to and understanding of proprietary algorithms limits our understanding of the threat posed by the amplification of fringe content and by wider information operations on mainstream platforms

There is limited evidence to link radicalisation pathways to algorithmic amplification and to the consumption of online content generally

Overview of existing measures and initiatives

Legal or regulatory measures

Technical measures

to limit dissemination of extremist and/or harmful content

to counter the potential impact of extremist and/or harmful content

Public-private initiatives

Civil society initiatives

Policy recommendations

Adopt a systemic approach to tackling online dissemination of extremist content

Advance understanding of algorithmic amplification and its impacts through knowledge-oriented initiatives.

Support the implementation of technological solutions through the definition of a framework for content moderation.

Investigate alternative legal measures to those targeting amplification through independent research.

Further invest in digital skills and capabilities for law enforcement to foster collaboration with platforms, including at national level.

Radicalisation Awareness Network

RAN Policy Support

RAND EUROPE