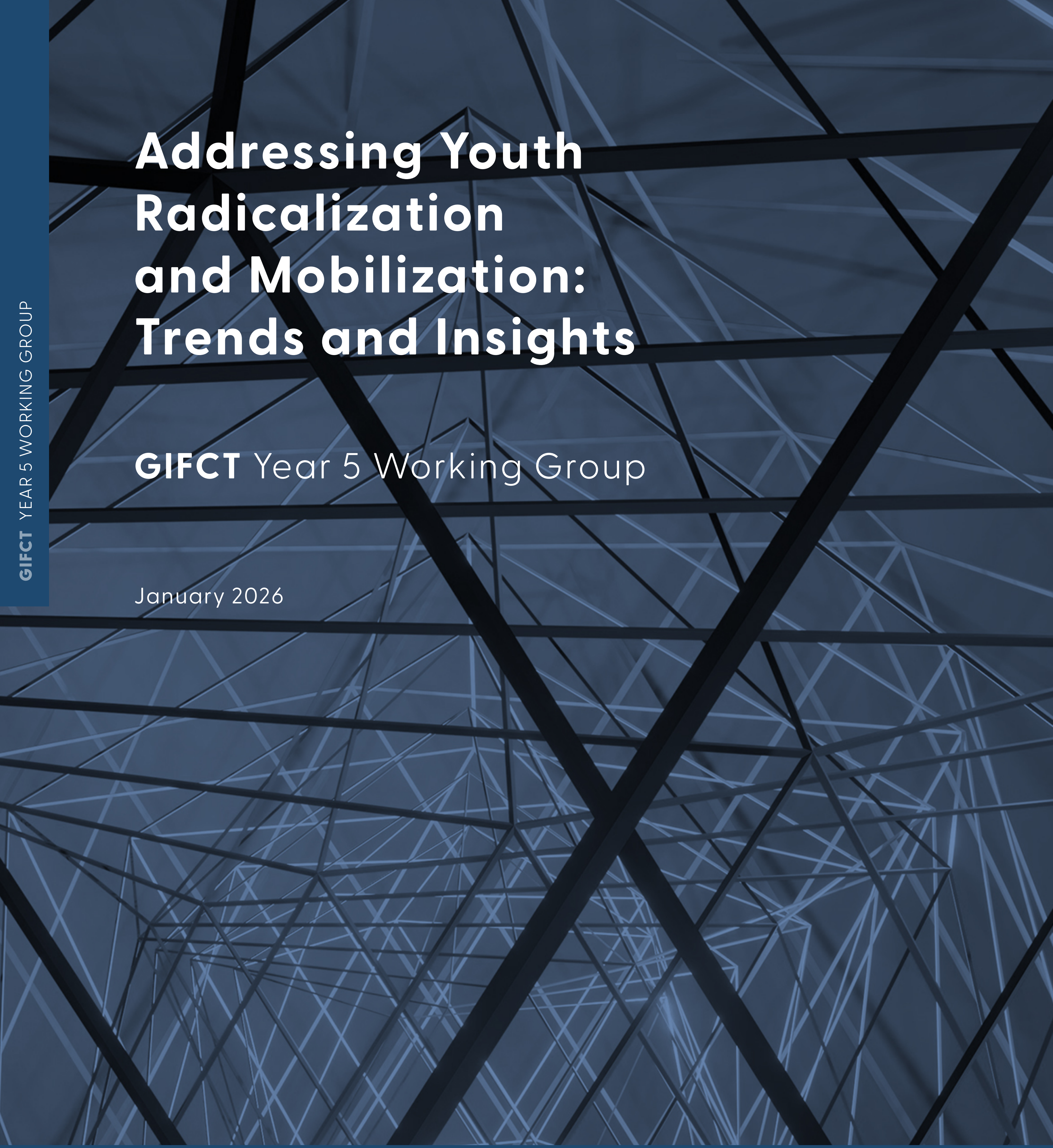


GIFCT YEAR 5 WORKING GROUP

Addressing Youth Radicalization and Mobilization: Trends and Insights

GIFCT Year 5 Working Group

January 2026

Global Network on Extremism & Technology

GIFCT
Global Internet Forum to Counter Terrorism

Table of Contents

Introducing GIFCT Year 5 Working Groups

In February 2025, GIFCT launched its Year 5 Working Groups to facilitate dialogue, foster understanding, and produce outputs to directly support our mission of preventing terrorists and violent extremists from exploiting digital platforms across a range of sectors, geographies, and disciplines. Started in 2020, GIFCT Working Groups contribute to growing our organizational capacity to deliver guidance and solutions to technology companies and practitioners working to counter terrorism and violent extremism, and offer multi-stakeholder perspectives on critical challenges and opportunities.[1]

Overall, the 2025 three thematic Working Groups convened 178 participants from 40 countries across 6 continents with 39% drawn from civil society (5% advocacy, 14% academia, and 20% practitioners), 23% representing governments, and 38% in tech.

Sectoral Breakdown of Working Group Participants

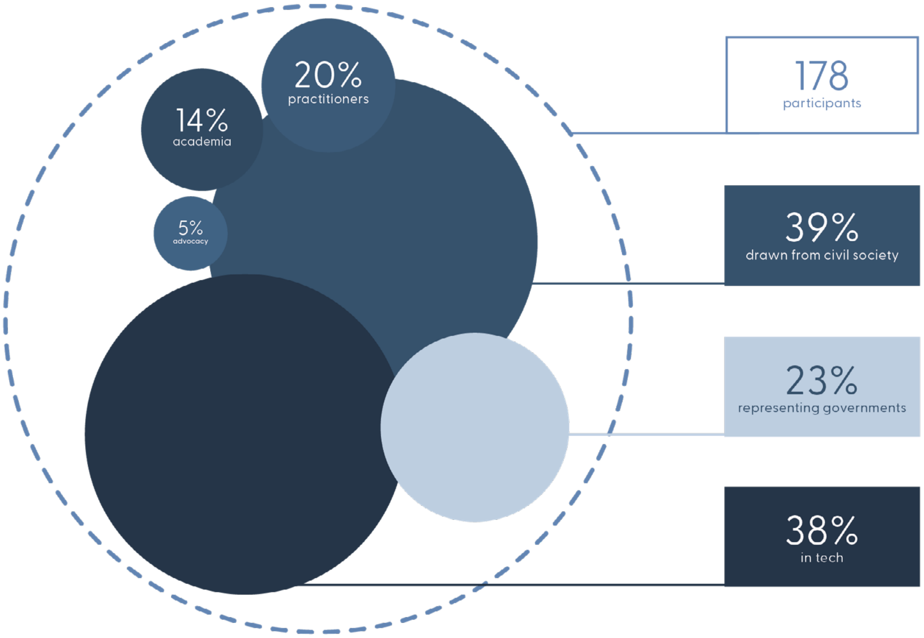


Figure 1: 2025 GIFCT Working Group participants by sector.

[1] Working Group outputs are produced by independent experts and do not necessarily represent the views of GIFCT, its members, or the GIFCT Operating Board.

GIFCT Year 5 Working Group Topics

The 2025 GIFCT Working Groups focused on the following three themes:

Investigators Community of Practice

The Investigators Community of Practice (ICOP) brought together a network of investigation, analytic, incident response, and operational trust and safety (T&S) professionals from GIFCT member companies who met monthly throughout 2025. ICOP and its monthly meetings built off-of and iterate-on the GIFCT's working group structure, and fostered a community of mutual learning between GIFCT and its members. Through ICOP, GIFCT created an ongoing and practical partnership with member T&S practitioner teams. Specifically, ICOP served as a destination for members and GIFCT staff to learn from one another, and brainstorm new GIFCT information sharing solutions. Periodically, ICOP leveraged external experts to provide substantive input for participants in the form of dedicated topic-oriented briefs.

Each ICOP session was focused on a challenge facing T&S operation teams and discussed: (1) threat landscape, (2) best practices, and (3) collective/GIFCT solutions. Sessions included a combination of member-company presentation, structured group discussion, and GIFCT solutions focus group.

Artificial Intelligence: Threats and Opportunities

This Working Group consolidated and established actionable, cross-sector best practices and standards for AI safety products related to exploitation by terrorist and violent extremist (TVE) actors. Drawing from industry experience, the group mapped TVE threats, identified effective mitigation strategies, and analyzed overlaps in different companies' approaches to develop best practices tailored to specific product types. This effort was conducted in collaboration with government and civil society practitioners to incorporate diverse perspectives and ensure comprehensive, sector-wide impact.

Addressing Youth Radicalization and Mobilization

This Working Group focused on identifying the current trends in youth radicalization and mobilization, and identifying lessons learned from prevention and positive intervention strategies to address these dynamics. This group highlighted best practices while connecting industry, practitioners, and experts to enhance cross-sector efforts. Through a series of structured multistakeholder dialogues, this group mapped evolutions in both the threats and responses, considering in particular how terrorists and violent extremists have targeted younger audiences online.

The group examined lessons learned from practice and programs, including positive interventions, counter-speech or "counter-narrative" work, and wider PCVE engagements, building from previous GIFCT Working Groups. Key findings and insights gleaned from the group, as well as the identification of relevant tools and resources, have helped equip practitioners in online safety efforts to build resilience in young online users and further positive intervention efforts.

Addressing Youth Radicalization and Mobilization: A Global Multistakeholder Approach

Erin Saltman and Mika Lopez Woodward

Introduction

Each year, GIFCT brings forward key Working Group themes to produce substantive outputs facilitating efforts to counter terrorism and violent extremism online. The *Addressing Youth Radicalization and Mobilization* (AYRM) Working Group convened international experts working on this topic to identify global trends, develop recommendations across sectors, and update key toolkits and resources to help platforms and practitioners advance these efforts. The AYRM Working Group convened participants from social media and gaming platforms, PCVE practitioners, expert researchers tracking youth radicalization, law enforcement, and government.[2]

The goals of this Working Group were:

1. To better understand the current threat landscape of youth radicalization in a global context.
2. To connect cross-sector practitioners with updated case studies, methodologies, and resources for youth prevention and positive interventions online (including other related child safety efforts).
3. To understand what tools can be shared to scale efforts and where gaps remain.

In meetings devoted to the main themes, the group heard presentations and discussed topics to advance the aforementioned goals. To better understand the threat, the group brought forward case studies, analysis, and recent evidence of terrorist and violent extremist groups proactively targeting younger online audiences.

To facilitate the dissemination of the Working Group's valuable information and insights to a wider practitioner audience, this paper is divided into three sections. The introductory section gives a summary of key themes and discussion points from the thematic meetings, including links to resources and programs addressing youth radicalization. The second section provides a series of insights from participants within the Working Group. These were published by GIFCT's academic research arm, the Global Network on Extremism and Technology (GNET), and are consolidated in this volume to provide key analysis related to the group's goals. Insights related to the AYRM theme will continue to be highlighted through GNET's Youth x Extremism series.

[2] Affiliations of all participants in 2025 GIFCT Working Groups are listed in an appendix at the end of this publication.

The final section of this paper provides an annotated bibliography of additional research and resources presented by the group to help technology companies, governments, experts, and practitioners advance their work to address youth radicalization and mobilization online.

The Working Group's discussions featured case studies across a wide range of established terrorist and violent extremist groups, and highlighted some of the challenges in addressing radicalization involving harmful online communities with less clear ideological frameworks and/or involving convergences of multiple harm types. Outputs from the AYRM Working Group include this insight series, a report on online subcultures of nihilistic violent extremism produced with ISD Global and GNET, and an updated relaunch of the GIFCT Campaign Toolkit, produced in coordination with Mythos Labs.

AYRM Narrative Summary

Each of the Working Group's thematic meetings featured presentations from participants who shared insights, case studies, tools, and resources on the three key themes.

Theme 1: Understanding the Current Threat Landscape in the Radicalization of Young People Online

The AYRM Working Group commenced with discussions on current trends of youth radicalization toward violent extremism. These focused on the growing concern in different parts of the world and across various platforms about the overlap between radicalization and grooming. They also delved into newer terrorist and violent extremist (TVE) trends brought forth by groups and networks like 764, Order of Nine Angles (O9A), and the COM network (explored further in this report through Insights by Pierre Sivignon and by an anonymous Working Group participant and Valdemar Balle, as well as a separate AYRM-GNET publication by Hannah Rose and Milo Comerford). Practitioners also voiced their concern about Islamist extremist resurgences connected with decentralized ISIS support (discussed in this volume by Maria Zupello). The group discussed how gamification and gaming surfaces are being used to attract younger audiences toward violent extremist and terrorist groups (examined in detail in the article in this volume by Linda Schlegal, Constantin Winkler, and Lars Wiegold). Practitioners working on prevention and disengagement shared cases and examples from their own safety programs, which highlighted the following trends:

- Increasing numbers of young people referred to intervention programs who are showing an interest in or engagement with "salad bar" or "mixed-ideology" extremism. In these cases, younger audiences are combining rhetoric and ideology from various types of violent extremist groups.

- Children referred to both law enforcement and civil society-led prevention and intervention programs have been getting progressively younger, particularly in North America and Europe.
- The radicalization process in youth case studies takes place very quickly (sometimes within a matter of weeks), making it difficult for law enforcement or wider intervention programs to identify vulnerable youth in advance of more downstream, violent signals.
- In cases where youth radicalization intersects with groups like the COM network, 764, or wider nihilistic and sadistic violent extremist trends, the overlapping of different harm types has increased, sometimes falling in the gaps between identification and enforcement. Increasingly, there are cases containing mixed signals that combine violent extremism with child exploitation, harassment, and self-harm.
- Several Working Group participants who were practitioners working on disengagement programs reported seeing a prevalence of young male users referred.

Key Considerations

Convergence of Harm Types: Participants across the group noted the trend of violent online networks targeting children with cross-cutting harm types involved in their attempts to engage, including grooming, radicalization, and other cybercrimes. Participants noted cases of nihilistic violent extremist and far-right accelerationist groups targeting children and engaging in and/or encouraging child sexual abuse, self-harm, violence against animals, and the planning of attacks. Violence has become a status symbol among some of these communities.

Online Subcultures: Regarding online gaming communities in particular, some tech company participants raised concerns about the combination of gaming culture, hate-based extremist narratives, and social status-seeking, citing clout-based groups where criminal acts are committed to achieve status within the group, and participants escalate behavior to gain recognition. In a similar vein, participants highlighted the use of “edgy” humor by bad actors in online communities to normalize and desensitize young people to violence and avoid content moderation in the process.

Finally, some participants working with intergovernmental organizations highlighted that cases in which minors are both perpetrators and victims blur the line on how to treat the young offender and raise challenges for approaching intervention work.

Theme 2: Considerations and Frameworks for Youth Prevention and Positive Interventions Online

AYRM participants reviewed how different sectors define legislation and frameworks, categorize youth audiences, and, at times, shift approaches for positive interventions based on age considerations. Youth audiences are vulnerable to radicalization toward hate-based ideologies and violence at times in similar ways to more mature online users, but in other ways need extra considerations and protections. The group discussed what could be learned from other sectors and related online harm areas to inform policies, approaches, and prevention tactics. How positive interventions were deployed across different parts of the world also prompted discussions about sociopolitical and cultural nuances that needed to be considered to develop effective online intervention strategies (as discussed further in this volume by Abraham Ename Minko).

Key Considerations

Age Categorizations: Participants highlighted the need to consider how a child's specific developmental stage may impact their vulnerability profile, and that differentiating among age categories within the "youth" bracket is necessary when assessing individuals' risk factors. For example, one participant noted that young people aged 12 to 18 they had encountered in their prevention programs were typically more preoccupied with identity creation and peer influence (and therefore more susceptible to social media narratives). In contrast, those aged 18+ were more likely to be preoccupied with political discourse and systemic injustice. Recent legislation in Australia, now being considered in other regions, also prohibits online users under 16 from using social media, recognizing the sensitivities around age and online safety.

Many online platforms have developed policies regarding young people's use of the platform, dividing "youth" into at least two categories: complete bans on "child" users and extra safety settings for "teen" accounts. Platforms such as Facebook, Instagram, and Discord noted that their policies prohibit children under 13 from using their platforms, but put additional safety measures in place for users under 18. For example, Facebook automatically applies audience, messaging, and content restrictions to teen accounts, while Instagram enforces content and interaction restrictions. Discord has developed user behavior policies applying to users under the age of 18, which prohibit them from engaging in sexually explicit or suggestive content, or from using or creating dating servers (even if intended only for other teenage users).

Other online platforms recognize that, due to their nature, they have a larger youth user base and have continued to evolve their technology to facilitate proactive enforcement of youth safety policies. For example, Roblox does not prohibit users under 13 from using the platform. However, they do implement policies geared toward child safety that adapt to different age groups under the "youth" umbrella. One such method is facial age recognition and requiring users to undergo age checks, after which Roblox communication functions limit access to younger audiences. All platforms in the AYRM Working Group recognized that younger audiences sometimes aim to deceive platforms about their age to access gaming and social media services, but advanced tooling and greater awareness among teachers and parents about policies and youth safety centers remain key.[3]

Psychosocial Profile: Practitioners and researchers across the Working Group referenced the potential differences in vulnerability profile and considerations for intervention approaches for neurodivergent young people. Some of the experiences that practitioners had observed as impacting how these young people had been radicalized included:

- **Hyperfixations**, where an individual becomes intensely interested in a topic rapidly. One case study shared in the group involved a teenage boy who was diagnosed as autistic and had developed a hyperfixation on Islam, and through misguidance around deciphering the religion, became engaged in IS-affiliated online spaces. The organization's approach to the intervention process accounted for this by involving a former extremist member on the intervention team. This helped the child develop trust and respect for the former member, primarily because the former member could discuss the child's hyperfixation in depth.
- **Social interaction sensitivities:** Some young people with neurodivergent conditions referred to participants' programs had been noted as struggling with social interactions. In some cases, this meant a younger person became reliant on specific online communities for social interaction and acceptance, leaving them vulnerable to exploitation by an attentive radicalization agent. Practitioners noted that in these cases, rather than just reducing time online, it was particularly important to focus on decreasing reliance on specific online spaces for social interaction and helping replace them with positive communities.

Community and Identity: Identity and belonging have always been key factors that terrorists and violent extremists can target when recruiting sympathizers and members. However, among younger audiences, vulnerabilities are increased due to the sensitive pre-teen and teen period when identity and in-groups are being formed and socialization processes are strongest. One key case study discussed the specific trends in radicalization pathways for Indigenous communities in New Zealand. It was noted that youth radicalization there often stems from historical and ongoing experiences of marginalization, mistrust in state institutions, and identity erasure. The participant highlighted that this makes radicalization factors for these communities deeply relational and tied to collective trauma, and that recruitment tactics increasingly exploit this disconnection. It was highlighted that

[3] The GIFCT Member Resource Guide gives overviews and links to all member companies safety platforms, including specific links to parent and teacher resources, linked from Appendix B in the resource. See: https://gifct.org/resource-guide/.

Western Eurocentric counterterrorism systems tend to be designed for individualized and adult-centric frameworks and not for young people in communities facing marginalization and identity erasure, which require relational and collective P/CVE approaches.

Theme 3: Tools, Solutions, and Remaining Gaps

The group finished the year with sessions highlighting tools, methodologies, and resources that exist to help the practitioner community better operationalize youth prevention and positive interventions. This included discussions about gaming for good, innovation in identifying bad actors with strategic network disruptions, and the future of online redirection work. Many of the resources, including platform-specific safety centers and youth safety tools, have now been added to the GIFCT Campaign Toolkit to ensure public access to a broad range of practitioner resources. Participants highlighted a range of approaches for youth engagement and positive intervention work online.

Key Considerations

Fictional Storytelling: The use of fictional storytelling in prevention, resilience, and counter-narrative campaigns was highlighted as an underdeveloped but valuable tool. Practitioners noted that there was previously more funding and innovation in storytelling for youth engagement, but many government and private-sector grants had diminished or disappeared in recent years. The group highlighted that what makes fictional narratives persuasive is not realism but the quality of the storytelling, which allows campaigns to safely develop positive characters to engage with. The distance from reality offered by fictional stories can disarm someone with pre-existing harmful beliefs, allowing individuals to be more open to learning when presented with such narratives. Examples and links to the research shared by the group on the positive impact of storytelling in youth safety work can be found in Appendix 1.

Youth Audience Segmentation: Participants discussed the potential use of tools to profile young audiences online to identify their specific risks of exposure to terrorist or violent extremist content or profiles, as well as tools to assess the potential effectiveness of planned positive intervention work online before launch. Examples discussed by the group included SONAR, the Safeguarder Online Navigation and Resource system, and the BunkWithKindness platform.

AI Facilitated Interventions: Participants discussed the potential role of AI chatbots in positive intervention programs, particularly to scale initiatives and fill gaps in existing programs. Practitioners mentioned that young online users might be vulnerable and might reach out online at different times of day when a caseworker might not be available. Some younger online audiences also feel more comfortable chatting with a non-adult or even a non-human (feeling less judged by a chatbot). While this type of human-tech fusion work for interventions is in early development, some emerging tools discussed include work through Mythos Labs with Aldous AI and Modulate's Moderate AI work.

It was clear from the conversations fostered through the AYRM Working Group that the youth safety sector, alongside the counterterrorism and counter-extremism community, is not starting from zero. There is a range of government and industry policies, CSO-driven frameworks, innovative technical tools and tactics, and research to support further efforts to safeguard young online users from processes of radicalization and mobilization. What the field often lacks is the resourcing and support to expand efforts across regions and platforms, as well as gaps in niche knowledge among practitioners that would help better identify the diversifying threat landscape online. As such, GIFCT will continue to convene global experts and practitioners in its 2026 Working Groups, focusing on key themes raised by the group, including youth safety, online gaming, and the role artificial intelligence will continue to play.

Dr. Erin Saltman *is the Senior Director of Membership & Programs at GIFCT. She has worked in the technology, NGO, and academic sectors, building out international counterterrorism strategies and programs. Her background and expertise span a range of regional and socio-political contexts. Her research and publications have focused on the evolving nature of violent extremism online, youth radicalization, and the evaluation of counterspeech approaches.*

Mika Lopez Woodward *is the Membership and Programs Coordinator at GIFCT. In this role, he supports ongoing member engagement, events, and the development of timely and bespoke resources to assist GIFCT member companies in their efforts to counter terrorism and violent extremism online.*

AYRM-GNET Insight Series

Throughout the AYRM Working Group, several participants authored insights, which were published as individual articles by the Global Network on Extremism and Technology (GNET), the academic research arm of GIFCT.[4] The group's thematic sessions inspired these insights, which have been brought together here to capture the group's efforts to address youth radicalization and mobilization.

Topic	Title & Authors
What makes youth radicalization unique? How should we be categorizing "youth"? What are the main "youth radicalization" trends that you are most concerned about?	*Youth Radicalisation in the Gaming Sphere: An Exploration of Identity-Based Hate and Extremist Content on Roblox* Linda Schlegel, Constantin Winkler, and Lars Wiegold
	From TechHaven to Telegram: How Latin American Youth Are Being Drawn into Jihadist Networks Maria Zuppello
	The Nordic Front of '764': Trends, Drivers, and Countering Youth Exploitation and Radicalisation Valdemar Balle and Anonymous Author
What are the sensitive ways to engage youth prevention or counter extremism? What platforms should be engaged for youth P/CVE work? What are some case studies of successful youth resilience or prevention campaigns?	*Building Digital Trust: Youth-Led Tech Solutions to Prevent Extremism in the Horn of Africa* Abraham Ename Minko
What tools, case studies, and resources are missing for platforms? For practitioners? Where are the gaps?	*Escape The Void: Responding to Youth-Led Nihilistic Violence* Pierre Sivignon
	The Feed That Shapes Us: Extremism and Adolescence in the Age of Algorithms Cecilia Polizzi

[4] These Insights and other authored pieces on the nexus of Youth x Radicalization can be found here: https://gnet-research.org/tag/youth/.

Youth Radicalisation in the Gaming Sphere: An Exploration of Identity-Based Hate and Extremist Content on Roblox

By Linda Schlegel, Constantin Winkler and Lars Wiegold - October 28, 2025

The gaming sector is becoming increasingly relevant in efforts to understand contemporary forms of extremism. Extremist actors of various ideological backgrounds, including right-wing extremists and jihadists, are seeking to exploit gaming in various ways. This includes the production of bespoke propaganda games, the instrumentalisation of commercial video games and in-game communication features, the appropriation of gaming aesthetics and gamified elements, as well as the exploitation of gaming and gaming (-adjacent) platforms. The latter refers to digital platforms that are either directly linked to gaming activities – such as the game distribution platform *Steam* or gaming forums such as *Mod DB* – or can be classified as gaming-adjacent, because they host a substantial amount of gaming-related content or are frequented by gaming communities, such as the chat platform *Discord* or the streaming platform *Twitch*. Many of these platforms have large user communities with millions of members. Although gaming has become a mainstream leisure time activity enjoyed across the whole spectrum of age groups, some gaming (-adjacent) platforms are particularly popular among young people and, hence, extremist propaganda in these spaces poses a particularly urgent challenge. The prime example of a youth-focused gaming platform is Roblox.

Roblox is a game development platform with 380 million monthly active users worldwide. A large portion of the Roblox user base is *minors*: 56% are under the age of 16, and just over 20% are younger than 9 years old, while only 19% of users are older than 25. Users on Roblox can create their own games (referred to as 'experiences'), play other users' creations, personalise their profiles and avatars, join groups, obtain new items for their avatars in a virtual marketplace, and communicate with others via social networking features. While most content on Roblox is harmless and legal, recent research suggests that parts of the platform are being exploited by malign actors and inadvertently host, for instance, playable recreations of mass shootings, content glorifying Nazi Germany, and right-wing extremist groups. Even recruitment into right-wing extremism has taken place on Roblox. Due to the high number of minors on the platform, it is possible that such content is both produced and consumed by underage users, which may have the potential to contribute to youth radicalisation processes in the online sphere. Therefore, Roblox is highly relevant for extremism research and efforts to prevent and/or counter (violent) extremism (P/CVE) in the digital sphere.

We contribute to the emerging research discourse on extremist activities in digital gaming spaces by presenting an exploration of different types of identity-based hate and extremist content on

Roblox. This Insight is based on an analysis of 350 posts and profiles collected between April and June 2025, conducted within the context of the RadiGaMe project. We provide insight into far-right and right-wing extremist, jihadist, and Islamist, as well as antisemitic content that we encountered on the platform, and report the main takeaways that will support not only future research efforts on Roblox, but also content moderation and P/CVE efforts.

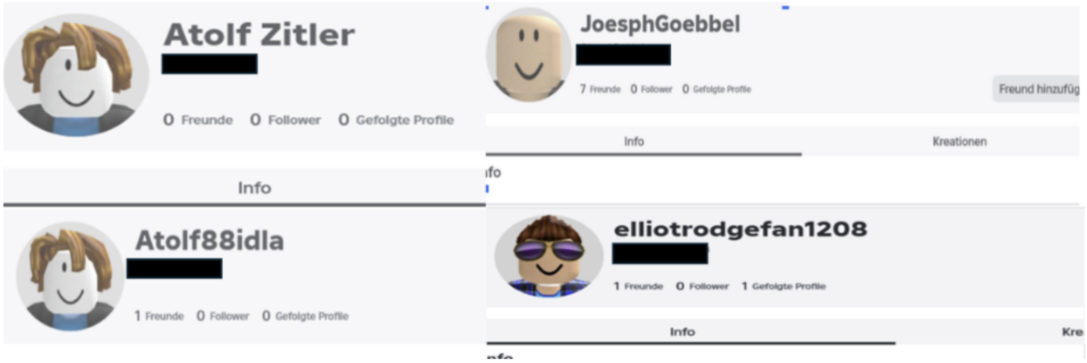
Far-Right and Right-Wing Extremism

Of the 350 posts and profiles collected, 175 pieces of content were coded as far-right and right-wing extremist material, and another 26 as borderline content. The material fell into four broad categories: Usernames, user-generated items (mostly shirts), groups, and experiences. We provide illustrative examples of each category below.

It is important to note that there are two types of user names on Roblox: a unique identifier (@ XYZ) and a self-chosen display name, which is not unique, as several users can employ the same display name. We have censored unique identifiers in the screenshots shown below, but report on non-unique display names where they are relevant to the analysis.

Usernames

Several profiles located during our search had usernames with connections to right-wing extremist figures or attackers. Strikingly, many of the names were purposefully misspelt, seemingly in an effort to circumvent Roblox's AI content moderation, which is trained to recognise and block certain terms. This confirms the findings of prior studies that identified similar misspellings on a Roblox election simulator. Other noticeable characteristics of these profiles were the use of codes such as 88 (a code for HH, Heil Hitler, as H is the 8th letter of the alphabet), a lack of followers and connections to experiences, as well as the use of 'National Socialist' as a popular self-designation.



Atolf Zitler
[redacted]
0 Freunde 0 Follower 0 Gefolgte Profile

Info

JoesphGoebbel
[redacted]
7 Freunde 0 Follower 0 Gefolgte Profile

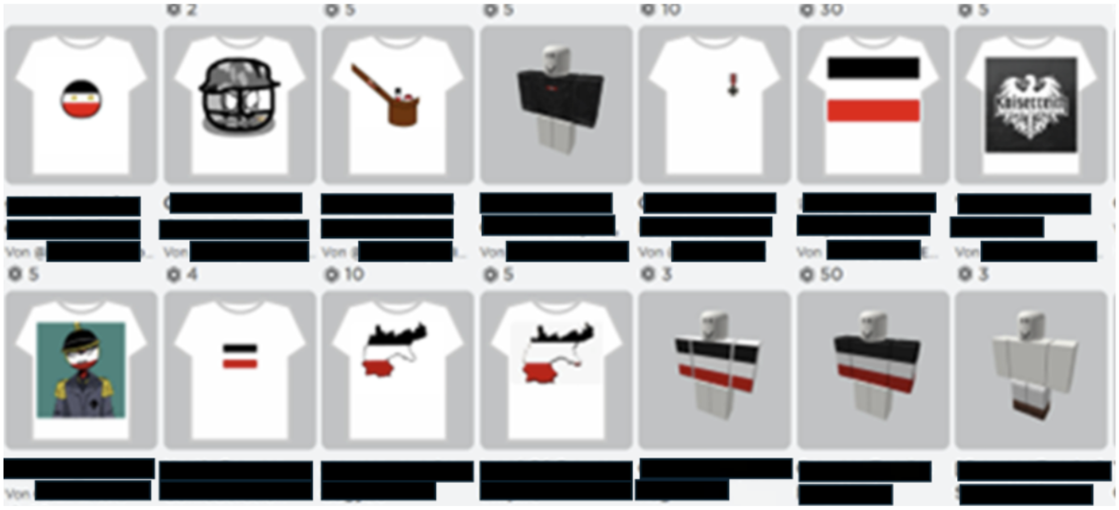
Atolf88idla
[redacted]
1 Freunde 0 Follower 0 Gefolgte Profile

elliotrodgefan1208
[redacted]
1 Freunde 0 Follower 1 Gefolgte Profile

Figure 1: Screenshot of self-chosen user names referencing right-wing extremist codes and individuals on Roblox.

User-generated shirts

T-shirts for Roblox avatars with slogans, flags, and symbols were another prominent content category. The screenshot below shows a collection of user-generated t-shirts with the Reichskriegsflagge, a symbol that is not illegal but used widely by right-wing extremists in Germany. On some shirts, Poland, the Czech Republic and Romania are labelled as "German", and Germany is shown in the borders of 1939. Right-wing extremists and conspiracy theorists often use this to express that they do not consider the Federal Republic of Germany in its current form to be legitimate.



[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

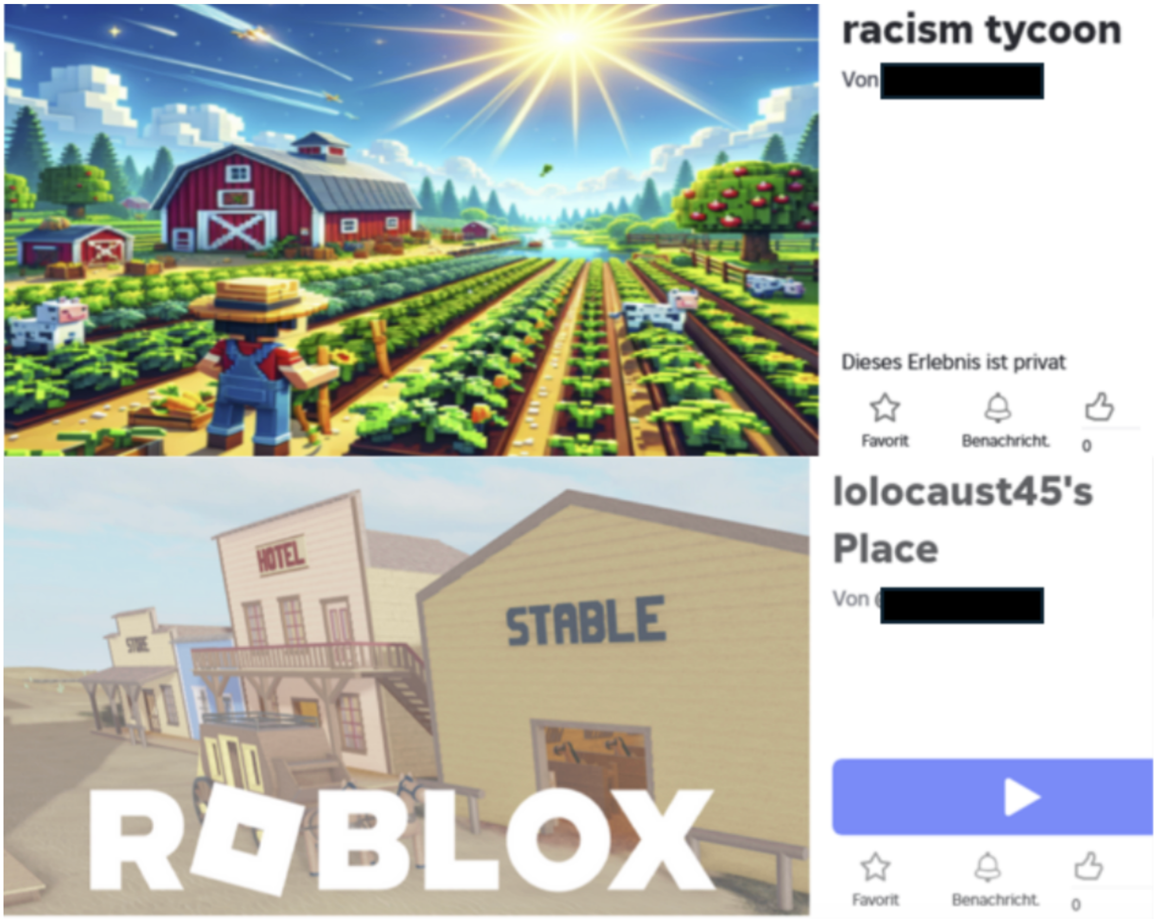
Figure 2: Screenshot of user-generated digital shirts for Roblox avatars showing the Reichskriegsflagge and other far-right iconography.

Groups

We located several groups seemingly affiliated with racist and far-right ideology, including groups with titles such as the since-deleted "white laces" (a reference to the shoe laces of the so-called Springerstiefel, a popular boot among German right-wing extremists) and other variations of "white XYZ". We found groups with a few dozen to over 1,000 members, the latter, for instance, in a group using the right-wing extremist code Honk Honk, which stands for Heil Hitler. Although some groups have a considerable number of members, there is often relatively little user communication within the groups, which may suggest that users join these groups for 'sign-posting' purposes, i.e. to display their political affiliation through the group names – a phenomenon already identified by prior studies. However, these inactive groups regularly include links to other platforms, particularly Discord servers, in their description, which may indicate that the members are actively communicating, just not on Roblox itself.

Experiences

In addition, we found numerous Roblox experiences containing far-right and right-wing extremist content, including titles such as “Racism Tycoon” and “lolocaust” (a misspelling of Holocaust), as well as experiences in which the player can assume the role of the US border patrol and take action against Latin American immigrants. While we did not analyse the gameplay of these experiences, locating experiences with such titles via simple keyword searches suggests that it may be relatively easy to find experiences that make right-wing extremist and racist narratives ‘playable.’



racism tycoon

Von [redacted]

Dieses Erlebnis ist privat

lolocaust45's Place

Von [redacted]

Figure 3: Screenshot of two experiences on Roblox featuring references to racism and the Holocaust. Both have been deleted after the data collection ended.

Islamism and Jihadism

Of the 350 posts and profiles collected, 52 posts were coded as containing Islamist content, 48 espoused Salafism, and 8 data points displayed jihadist content. This material can be grouped into similar categories as the right-wing extremist material: Usernames, user-generated items, groups, and experiences.

Usernames

We identified several profiles with Islamist usernames, including Abu Ubeida, a spokesman of Hamas, and a large number of profiles with self-proclaimed Houthi affiliations. In contrast to right-wing extremist usernames, however, there were usually no spelling mistakes, which may suggest that users do not feel the need to circumvent automated moderation efforts in these cases.

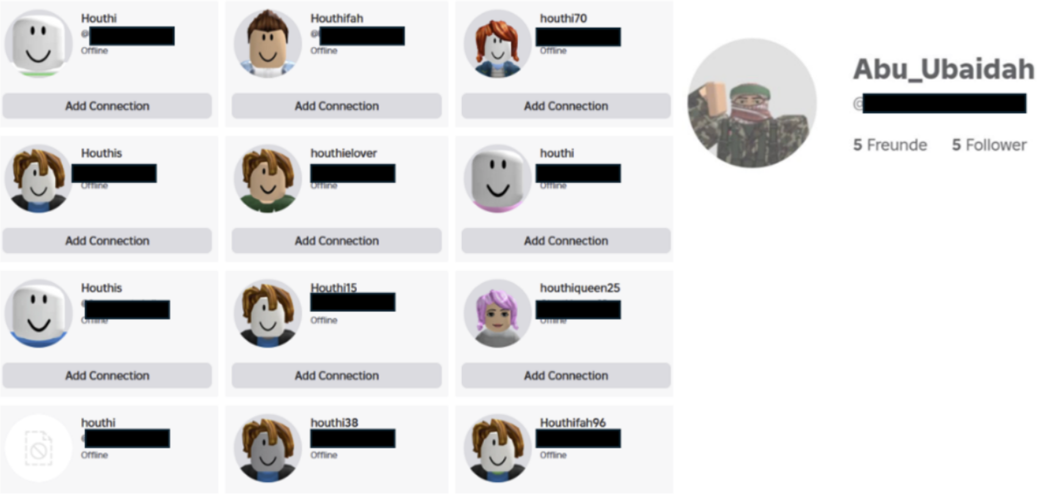
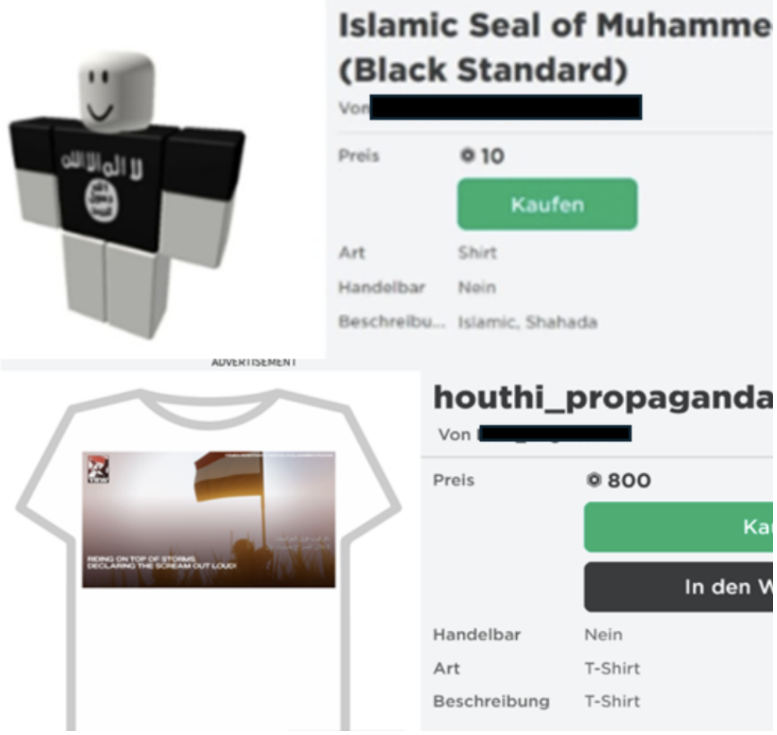


Figure 4: Screenshot of self-chosen names of Roblox user profiles featuring references to the Houthis and Hamas.

User-generated shirts

Just like the right-wing extremist part of the dataset, Islamist and jihadist material on *Roblox* was also expressed via user-generated items, particularly t-shirts. We found (since deleted) t-shirts with the emblem of the so-called Islamic State (ISIS), Houthi propaganda in both English and Arabic, as well as t-shirts supporting Hamas and Hezbollah. In the screenshot below, it is particularly notable that the creator openly named the shirt "houthi_propaganda."



Islamic Seal of Muhamme
(Black Standard)

Von [redacted]

Preis	10
Art	Shirt
Handelbar	Nein
Beschreibu...	Islamic, Shahada

houthi_propaganda

Von [redacted]

Preis	800
Handelbar	Nein
Art	T-Shirt
Beschreibung	T-Shirt

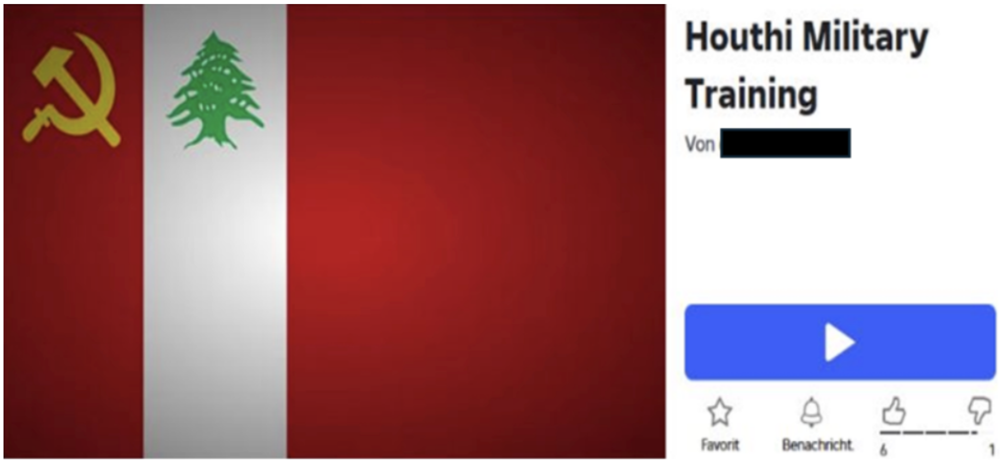
Figure 5: Screenshot of user-generated digital shirts on Roblox referencing the so-called Islamic State and the Houthi militia.

Groups

The corpus of material also includes a handful of groups associated with Salafist and jihadist actors, albeit far fewer than far-right and right-wing extremist groups. However, some self-proclaimed sheikhs who run these groups have over 3000 followers, suggesting considerable reach. Similar to right-wing extremist groups, we found out-links to other digital platforms in Salafi and jihadist groups, including to Facebook groups, YouTube accounts, and Discord channels.

Experiences

Additionally, we located several experiences in both English and Arabic connected to Islamist and jihadist beliefs, showing, for instance, affinity to ISIS. Often, these experiences use inconspicuous thumbnails without an obvious connection to the ideological content of the game, possibly to avoid detection. In several cases, the profiles of the creators had been deleted, but the experiences themselves were still available. Particularly interesting is the presentation of the "Houthi Military Training" experience displayed below, because the creator combined Houthi themes with Hezbollah and communist iconography, potentially suggesting the presence of a mixed ideology or 'salad bar extremism.'



Houthi Military Training

Von [redacted]

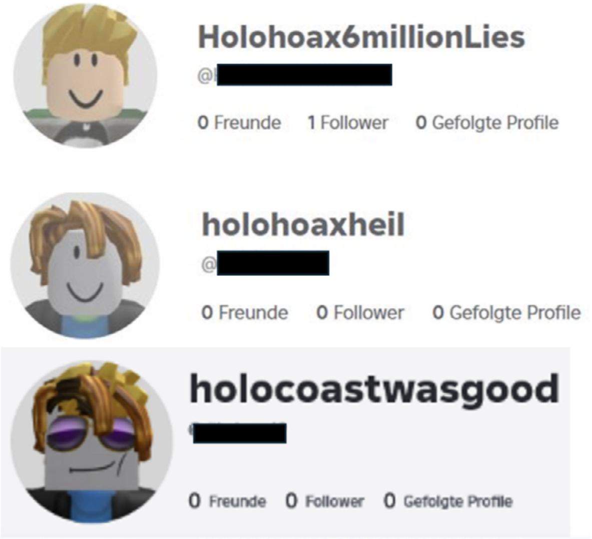
Figure 6: Screenshot of a now-deleted Roblox experience titled “Houthi Military Training”.

Antisemitism

206 posts in the data set were coded as containing antisemitic beliefs and material. Here too, data points included usernames, user-generated content, groups, and experiences.

Usernames

Several profiles with antisemitic user names were located. Particularly striking were a number of profiles with names denying or approving the Holocaust, often in combination with right-wing extremist codes such as Sieg Heil, 14 (a reference to the 14-word white supremacist pledge), and 88.



Holohoax6millionLies

@[redacted]

0 Freunde 1 Follower 0 Gefolgte Profile

holohoaxheil

@[redacted]

0 Freunde 0 Follower 0 Gefolgte Profile

holocoastwasgood

[redacted]

0 Freunde 0 Follower 0 Gefolgte Profile

Figure 7: Screenshot of Roblox user names denying and celebrating the Holocaust.

User-generated items

Here we also see the use of user-generated content, including self-made shirts for avatars. The image below features a shirt with the slogan "This is Kanye West" accompanied by a photograph of Anne Frank. The rapper Kanye "Ye" West has been criticised several times for antisemitic remarks and, earlier this year, released a new album, which includes songs such as WW3 or HH, which espouse antisemitism and glorify Nazi Germany. Among the user-generated items, there are also references to the Shoah as a supposed lie. The shirt below, for example, sarcastically suggests that questioning the Shoah is only punishable by law because it has not been sufficiently proven.

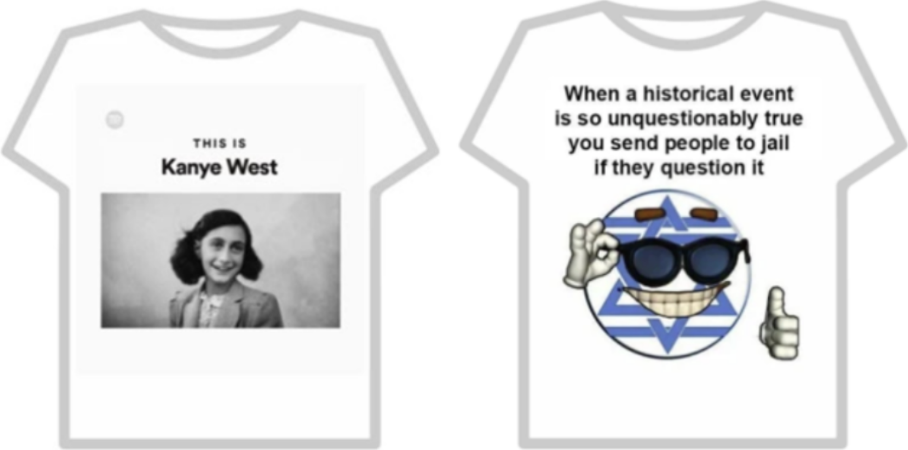
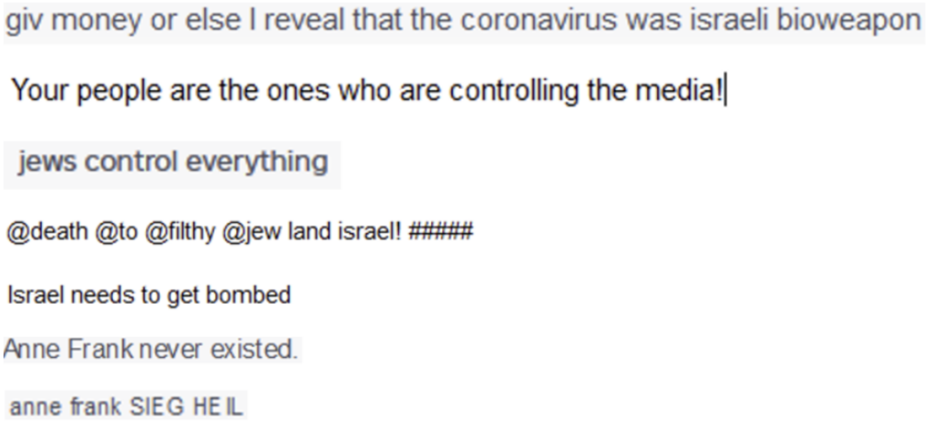


Figure 8: Screenshot of user-generated digital shirts on Roblox referencing the antisemitic music album of Kanye West and denying the Holocaust.

Groups

Many groups reveal antisemitism in their names with the use of graphic phrases. We found the strategic use of misspellings to bypass moderation, for instance, spelling the word "Jewish" as "J3wesh." The discussions on Roblox mainly feature classic antisemitic stereotypes and Israel-related antisemitism. This seemingly 'humorous' post combines the antisemitic myth of Jewish wealth with the conspiracy myth that Israel was behind the spread of COVID-19. Such myths about Jewish power are widespread on the platform. In addition, death threats against Jews and Israel, as well as mocking figures such as Anne Frank, were found in the comments.



giv money or else I reveal that the coronavirus was israeli bioweapon

Your people are the ones who are controlling the media!

jews control everything

@death @to @filthy @jew land israel! #####

Israel needs to get bombed

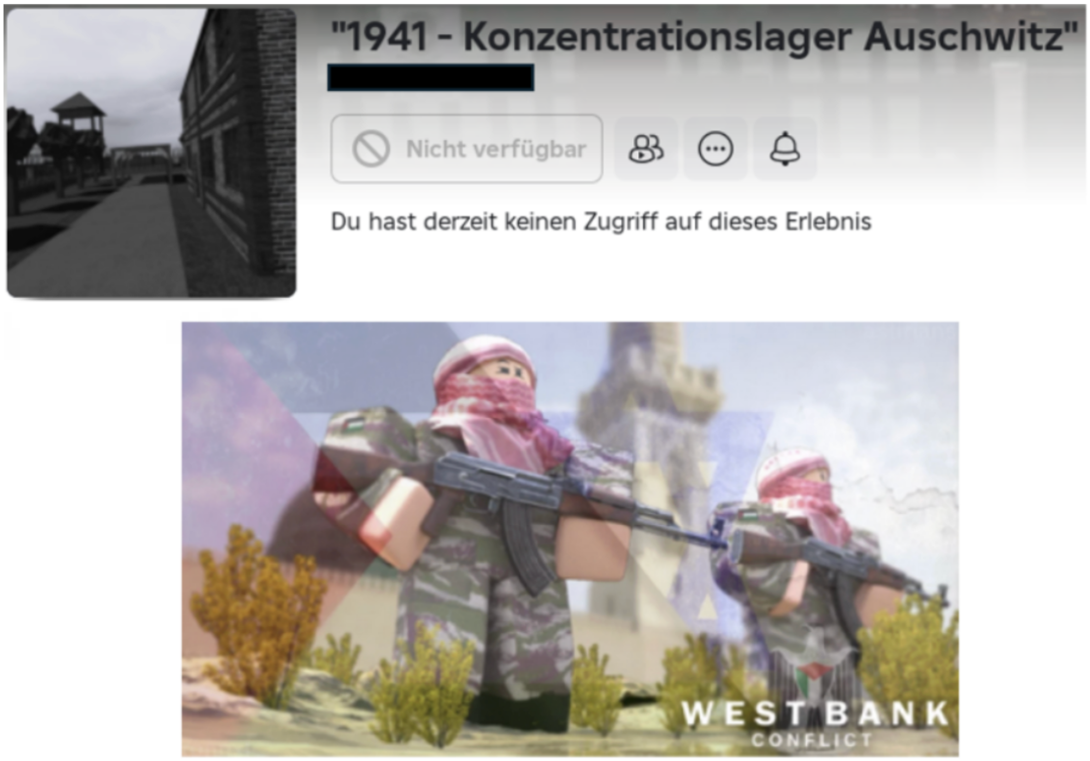
Anne Frank never existed.

anne frank SIEG HE IL

Figure 9: Screenshots of antisemitic statements in groups on Roblox.

Experiences

We found experiences serving as spaces of congregation for antisemitic users, as well as overtly antisemitic games such as replicas of extermination camps or experiences that allowed users to assume the role of Palestinian terrorists.



"1941 - Konzentrationslager Auschwitz"

[redacted]

Du hast derzeit keinen Zugriff auf dieses Erlebnis

Figure 10: Screenshots of Roblox experiences set in a concentration camp and allowing players to assume the role of Palestinian terrorists.

Main Takeaways

Across all types of extremism and identity-based hate we encountered on Roblox, the following observations stand out:

- Usernames on *Roblox* are a key tool to communicate connection to or endorsement of extremist groups and ideas, a trend that can also be observed in popular video games. Misspellings, abbreviations, and codes feature prominently in these usernames, potentially suggesting deliberate attempts to circumvent moderation efforts.
- User profiles must be assessed in their entirety to adequately judge whether the profile espouses extremist worldviews. For instance, using the "Reichskriegsflagge" may, in itself, not be illegal, but it may indicate right-wing extremist tendencies, particularly when combined with a username featuring far-right codes or the creation of experiences espousing identity-based hate.
- T-shirts and other user-generated items to customize avatars are popular and used to display ideological affiliations. Often, they are openly shared in the marketplace, providing further evidence that user-generated content is a key concern in digital gaming spaces.
- Groups with hateful and extremist names were relatively easy to find. They often contain little in-group communication, but may be used as sign-posting and to show the users' ideological affiliation on their profile.
- Experiences containing identity-based hate and extremist content could be located via keyword searches. In several instances, experiences or groups with extremist content remained available on the platform, although the creator's profile had been deleted. It is unclear whether the deletions were carried out by moderators or the creators themselves, but in any case, they indicate the need to examine experiences and groups created by deleted accounts more closely to ensure the complete removal of relevant material.
- Our non-English findings, particularly Islamist content in Arabic, suggest that standards of moderation differ across languages. For instance, we found that experiences described in Arabic letters allowed users to play dictators and war criminals, whereas the names of the same characters were blocked by automated content moderation when typed using the Latin alphabet.

Conclusion

Roblox has already made considerable efforts to curb extremist influences on its platforms. Nevertheless, considering Roblox's very young user base and the fact that all our data was collected in public parts of the platform, our findings suggest that children and teenagers may be exposed to identity-based hate and extremist ideas on the platform. In some cases, this could potentially contribute to radicalisation processes in young people. To be sure, the mere presence of identity-based hate and extremist material does not necessarily mean it has a considerable impact. However, there is the possibility that some young users on Roblox may be negatively impacted by such material and/or form connections to users who create and share such content. It is therefore crucial that moderation is swift, reacts to misspellings and other efforts to circumvent automatic detection tools, and encompasses user profiles, user-generated content, groups, and experiences (including content created by already deleted user profiles) to reduce the possibility of exposing young users to such material. In addition, our findings suggest that Roblox is a crucial space for efforts to prevent and counter increasing attempts by extremist actors to influence minors.

Linda Schlegel *is a Postdoctoral Research Fellow at the Peace Research Institute Frankfurt (PRIF), where she co-leads the RadiGaMe project and researches extremist activities in digital gaming spaces. She is also a Research Fellow at modusIzad, where she explores new avenues for digital P/CVE approaches, and a founding member of the Extremism and Gaming Research Network (EGRN).*

Constantin Winkler *is a Doctoral Researcher at the RadiGaMe Project at the Peace Research Institute Frankfurt (PRIF). He investigates antisemitism and radicalisation in digital gaming communities. He focuses on antisemitism research, cultural sociology, and Critical Theory.*

Lars Wiegold *is a research associate in the RadiGaMe and RADIS projects at the Peace Research Institute Frankfurt (PRIF). His research focuses on radical and extremist online milieus, particularly in digital gaming communities.*

From TechHaven to Telegram: How Latin American Youth Are Being Drawn into Jihadist Networks

By Maria Zuppello - November 14, 2025

In the last decade, Latin America has witnessed a profound paradigm shift in youth radicalisation linked to ISIS ideology. In 2015, Operation Hashtag, conducted shortly before the Rio de Janeiro Olympics, revealed the functioning of the first active jihadist cell in the region. The group was composed of young Brazilian adults who used Facebook, Telegram, and WhatsApp to spread ISIS propaganda and plan attacks in São Paulo and Rio during the international sporting event. However, the investigation had shown that behind the virtual dimension, a real network also existed: some of the members knew each other personally. Ten years later, the rise of the decentralised web (DWeb) has transformed the digital landscape, dispersing control among users and making online moderation almost exceedingly difficult. This shift has widened global connections, enabling violent extremists in Latin America to engage directly with radicalisers abroad. At the same time, youth are increasingly involved in such activities, raising concerns about the social factors driving this change, including poverty, inequality, and educational deprivation that make minors particularly vulnerable to extremist propaganda.

This Insight examines the radicalisation transformation that has occurred, focusing particularly on Brazil, and shows how the decentralised web is cultivating an online ecosystem that inspires new lone actors in Latin America.

The Transformation of Online Radicalisation

In 2015, Operation Hashtag first shed light on ISIS's penetration into Latin America. Just days before the Rio Olympics, Brazilian police arrested a network of young nationals across various states who were planning to carry out attacks during the event. According to court documents, they all shared low socio-economic status and poor education. Two of them had met in Egypt, where they had been invited to study Arabic, before later attending radical preaching sessions in São Paulo led by foreign clerics. Social media served to expand the network and amplify the group's radical message, reaching other young Brazilians who ultimately did not participate in the plot. In a closed online group, members circulated posts advocating the introduction of Islamic sharia law in Brazil. They also exchanged information on how to pledge bayat, or allegiance, to the Islamic State. WhatsApp and Telegram groups, on the other hand, had a more operational purpose for the network: sharing information on how to carry out attacks in São Paulo and Rio during the Olympic Games. Brazilian police later said they had foiled the planned attacks after investigators infiltrated the group's WhatsApp chats.

Over the past decade, social media platforms have intensified efforts to tackle terrorist and extremist content by combining artificial intelligence with human review. In 2019, Facebook open-sourced two content-matching technologies – PDQ for photos and TMK+PDQF for videos – designed to detect and block harmful material online. These algorithms create digital hashes, or unique fingerprints, enabling platforms to identify and remove identical or near-identical files, even when altered.

By releasing these tools on GitHub, Facebook empowered tech companies, smaller platforms, and non-profits to detect and remove abusive content more effectively. This open-source approach fosters cross-industry cooperation, allowing multiple services to take down extremist content simultaneously and curb its spread across the internet. On WhatsApp, limits on message forwarding and the monitoring of suspicious activity have also helped restrict the viral circulation of extremist material.

According to a 2024 report by the Organisation for Economic Co-operation and Development (OECD), terrorist and violent extremist groups are increasingly exploiting the decentralised web (DWeb), using its messaging apps, social media, and hosting systems such as Skynet and IPFS to distribute content and evade moderation. Indeed, "sustained efforts by major platforms to combat terrorist and violent extremist content (TVEC) have caused a 'displacement effect,' whereby terrorists and violent extremists turn to alternative platforms," the report said (p.3).

Unlike centralised networks such as Facebook, decentralised platforms allow users to control where data is stored, making them harder to censor or monitor. Services like RocketChat and ZeroNet have become particularly attractive to IS media operatives because their content is hosted on user-run servers, which prevents developers from deleting extremist material. Even when such servers are taken offline, their databases remain intact, reappearing on new servers under new domains – posing fresh challenges for law enforcement agencies attempting to detect and remove jihadist content online.

Propaganda and Cultural Hybridisation

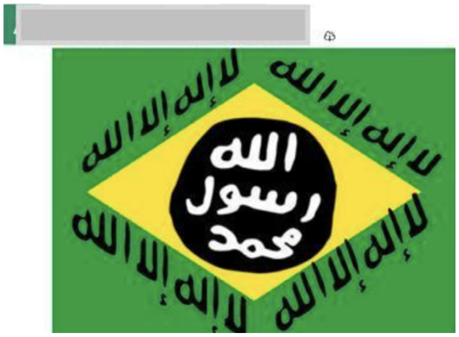


Figure 1: Brazilian group on TechHaven: Brazilian flag overlaid with the ISIS symbol (credit Atlantico Intelligence Group).

Last year, Brazilian police arrested a 45-year-old man accused of being the administrator of the first Latin American jihadist group, aimed at Brazilian and Lusophone users, hosted on a decentralised platform called TechHaven. At his home, officers found chemical materials for bomb-making and a machete – tangible evidence of preparations for violent acts. An analysis of the group's activities over the three months preceding the man's arrest reveals a complex structure with two main objectives: disseminating ISIS propaganda and inciting action by sharing technical and military information to carry out attacks. The group was distinguished by its educational and hierarchical approach, with the administrator acting as a cultural mediator to make complex ideological content accessible to a Brazilian audience. He localised ISIS's global rhetoric to resonate with local sensibilities, blending propaganda from the Amaq Agency—translated into Portuguese—with magazines like Dabiq, Rumiyah, and Voice of Khorasan, and with local cultural references.

For example, the administrator exploited Brazil's strong musical culture by sharing curated collections of nasheeds (jihadist religious chants) and referencing local texts such as the Brazilian Army's Jungle Survival Manual to legitimize his message. Operationally, the group circulated technical manuals for attack preparation. The administrator's final post, showing a Heckler & Koch Mark 23 pistol fitted with a silencer, underscored the shift from theory to intended action.

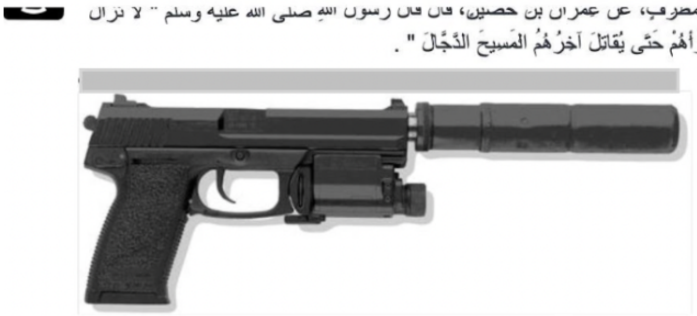
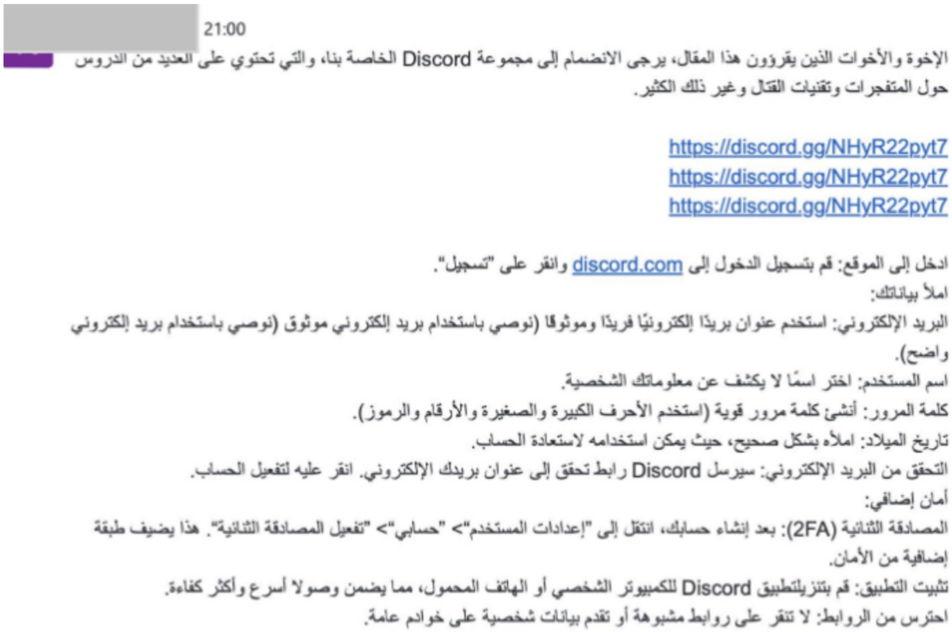

حدثنا موسى بن إسماعيل، حدثنا حماد، عن قتادة، عن مطرف، عن عمران بن حصين، قال قال رسول اللهِ صلى الله عليه وسلم " لا تزال
طَائفة مِنْ أُمَّتي يُقاتِلُونَ عَلَى الحَقِّ ظَاهِرِينَ عَلَى مَنْ نَاوَأَهُمْ حَتَّى يُقَاتِلَ آخِرُهُمُ المَسِيحَ الدَّجَّالَ " .

Figure 2: Brazilian group on TechHaven: final post featuring a handgun (credit Atlantico Intelligence Group).

Although the group primarily targeted a Portuguese-speaking audience and interaction was limited mainly to Brazilian members, foreign users also appeared, requesting materials in English or Urdu (Pakistan's official language) or sharing links to jihadist groups on the messaging platform Discord.



[redacted] 21:00

الإخوة والأخوات الذين يقرؤون هذا المقال، يرجى الانضمام إلى مجموعة Discord الخاصة بنا، والتي تحتوي على العديد من الدروس حول المتفجرات وتقنيات القتال وغير ذلك الكثير.

https://discord.gg/NHyR22pyt7
https://discord.gg/NHyR22pyt7
https://discord.gg/NHyR22pyt7

ادخل إلى الموقع: قم بتسجيل الدخول إلى discord.com وانقر على "تسجيل".
املأ بياناتك:
البريد الإلكتروني: استخدم عنوان بريدًا إلكترونيًا فريدًا وموثوقًا (نوصي باستخدام بريد إلكتروني موثوق (نوصي باستخدام بريد إلكتروني واضح).
اسم المستخدم: اختر اسمًا لا يكشف عن معلوماتك الشخصية.
كلمة المرور: أنشئ كلمة مرور قوية (استخدم الأحرف الكبيرة والصغيرة والأرقام والرموز).
تاريخ الميلاد: املأه بشكل صحيح، حيث يمكن استخدامه لاستعادة الحساب.
التحقق من البريد الإلكتروني: سيرسل Discord رابط تحقق إلى عنوان بريدك الإلكتروني. انقر عليه لتفعيل الحساب.
أمان إضافي:
المصادقة الثنائية (2FA): بعد إنشاء حسابك، انتقل إلى "إعدادات المستخدم"> "حسابي"> "تفعيل المصادقة الثنائية". هذا يضيف طبقة إضافية من الأمان.
تثبيت التطبيق: قم بتنزيلتطبيق Discord للكمبيوتر الشخصي أو الهاتف المحمول، مما يضمن وصولاً أسرع وأكثر كفاءة.
احترس من الروابط: لا تنقر على روابط مشبوهة أو تقدم بيانات شخصية على خوادم عامة.

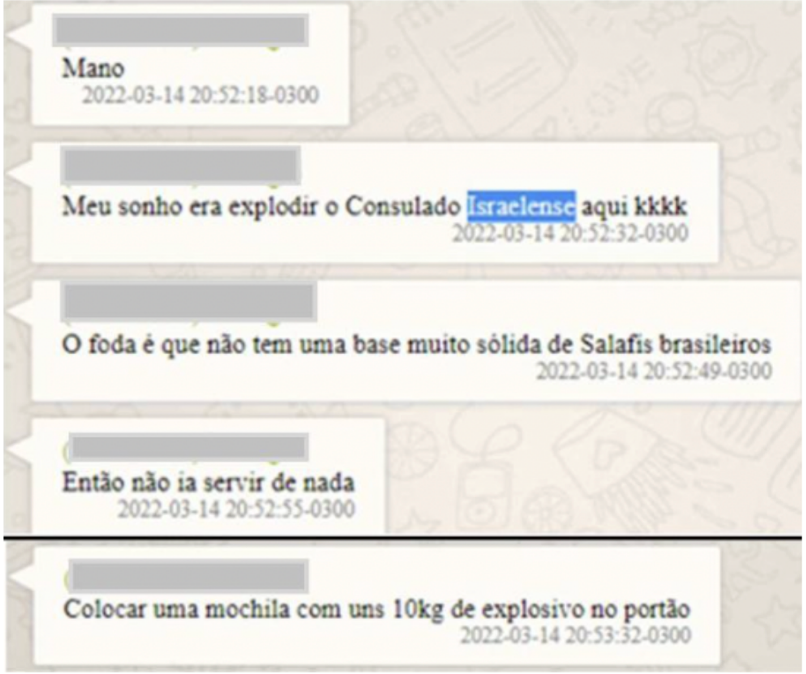
Figure 3: Brazilian group on TechHaven: a post by a member inviting people to a jihadist group on Discord (credit Atlantico Intelligence Group).

According to Brazilian authorities, the group's main strength lay in its ability to redirect members to Telegram channels offering military training for "lone wolves." These channels shared detailed instructions on how to build explosive devices, detonators, suicide vests and belts, as well as manuals for producing and deploying biological and chemical weapons, including phosphine, hydrogen sulphide and cyanide gas. Members of these groups also post requests for cryptocurrency donations to buy materials used for propaganda or to prepare attacks. This shows that extremists sustain their activities through cross-platform migration, swiftly adapting when moderation intervenes. By shifting to smaller or less-regulated platforms, they preserve their networks, rebuild audiences, and continue spreading propaganda.

Decentralised Web Use and Youth Radicalisation

The decentralised web has opened new avenues for accessing jihadist material, making extremist content increasingly difficult to control. In this disjointed ecosystem – lacking central servers or moderation – minors may join encrypted spaces as a game or challenge: navigating the prohibited, disseminating clandestine material, and seeking belonging to an 'exclusive' group. A striking example is that of a 14-year-old Uruguayan boy who, according to investigators, was in direct contact with the administrator of the Brazilian extremist group mentioned above. Police arrested him after posting a video threatening to attack a synagogue in Montevideo, Uruguay.
According to the Global Terrorism Index 2025, published by the Sydney-based Institute for Economics and Peace, in Europe, one in five people arrested for terrorism in 2024 was legally

classified as a minor (p.2). The report also highlights an increase in lone-actor attacks, rising from 32 in 2023 to 52 in 2024. These attacks are typically carried out by young people, often teenagers, who have no formal links to terrorist organisations. Instead, they become radicalised through online content, developing personal ideologies that blend conflicting viewpoints influenced by "fringe forums, gaming environments, encrypted messaging apps and the dark web" (p.2).



[redacted]
Mano
2022-03-14 20:52:18-0300

[redacted]
Meu sonho era explodir o Consulado Israelense aqui kkkk
2022-03-14 20:52:32-0300

[redacted]
O foda é que não tem uma base muito sólida de Salafis brasileiros
2022-03-14 20:52:49-0300

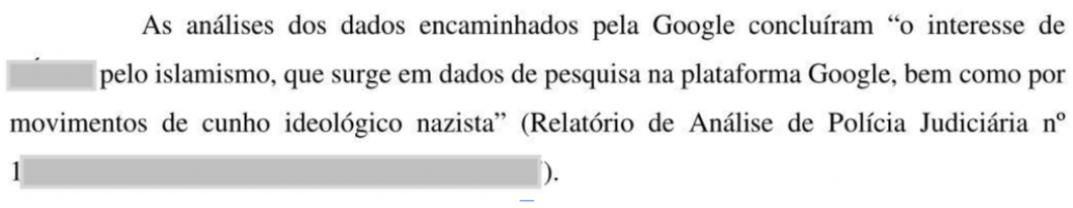
[redacted]
Então não ia servir de nada
2022-03-14 20:52:55-0300

[redacted]
Colocar uma mochila com uns 10kg de explosivo no portão
2022-03-14 20:53:32-0300

Figure 4: Planning on WhatsApp of the attack by a Brazilian and a minor against the Israeli Consulate in São Paulo (credit Brazilian Federal Police).

Uruguay's case is not unique. In Brazil, a different young person was part of an investigation that led to the arrest of a 20-year-old in 2023. This person was apparently prepared to travel to Turkey to fight with ISIS. The Federal Police found that the youngster had been groomed on Telegram and told on WhatsApp to prepare assaults against the Israeli embassy in Brasília and the consulate in São Paulo.

Their discussions indicated a worrying rise: in addition to sharing ISIS propaganda, the two exchanged technical advice for making bombs and improvised explosive devices. The older suspect had also posted a video on pCloud, wearing a mask and responding to a questionnaire for prospective ISIS recruits. Police documents noted: "data provided by Google revealed the young man's interest in Islamism, as shown by his search history, as well as a fascination with Nazi-inspired ideology".



As análises dos dados encaminhados pela Google concluíram “o interesse de [redacted] pelo islamismo, que surge em dados de pesquisa na plataforma Google, bem como por movimentos de cunho ideológico nazista” (Relatório de Análise de Polícia Judiciária nº 1[redacted]).

Figure 5: Excerpt from the investigation (credit Brazilian Federal Police).

In both cases, antisemitism emerged as a central driver of radicalisation, fuelled by online environments that promote hatred and conspiracy theories. Additionally, structural issues such as poor educational attainment, social isolation, and limited opportunities in disadvantaged environments create a climate conducive to extremist ideology.

Recommendations

DWeb, by its very nature, decentralised and resistant to censorship, represents one of the most complex challenges for contemporary counter-terrorism strategies. Within this ecosystem, platforms such as ZeroNet and applications based on protocols like Matrix (for instance, Element) offer jihadist networks new spaces to disseminate propaganda, recruit followers, and communicate through encrypted channels that are difficult to monitor or dismantle. ZeroNet functions similarly to a traditional website but distributes its content across users via peer-to-peer (P2P) technology, eliminating a central server and thereby frustrating censorship or content removal. Matrix, meanwhile, is a decentralised communication protocol that enables interoperability between servers and applications. Element, one of its best-known applications, provides end-to-end encrypted messaging, group chats, and public or private channels, similar to Telegram or Discord but without dependence on a single provider.

Facing this reality requires a strategic reevaluation of prevention and counteraction measures.

The priority must be to strengthen technological surveillance and analytical capabilities by developing advanced monitoring tools that operate on decentralised networks. Combining artificial intelligence (AI) and machine learning would help simplify the identification of traffic patterns and unusual nodes linked to terrorist activity in the decentralised web. At the same time, focused disruption attempts could make it harder for jihadist groups to have a continuous online presence by limiting access to channels used to spread extremist content. As the internet becomes increasingly decentralised, regulated platforms such as Discord and Facebook have an even more crucial anchoring role to play. Among the actions required is better interoperability in safety measures – developing shared standards for content moderation signals, user verification, and abuse detection that can interface with decentralised or federated systems. User education and the introduction of friction tools are also essential. When users click on links that take them to less-moderated or decentralised environments (such as encrypted chats, peer-to-peer sites, or federated servers), platforms should display a safety interstitial – a brief warning or consent screen. This message could alert users that they are leaving a moderated space, explain the risks of exposure to illegal or misleading content, request consent to proceed, and offer further resources on online safety.

But improved technological measures alone are not enough. A coordinated global effort between intelligence agencies, law enforcement, and technology companies is essential. Establishing specialist task forces, primarily those focused on open-source protocols, might facilitate the creation of 'ethical backdoors' or obligatory audit procedures that provide limited oversight without compromising the fundamental principles of decentralisation that characterise the DWeb. Simultaneously, legal and regulatory frameworks must be revised to include clear stipulations mandating the removal or obstruction of terrorist material, even from decentralised nodes. Given that several DWeb sites use blockchain technology, it is essential to implement procedures to monitor and freeze digital wallets linked to terrorist funding. Ultimately, counter-radicalisation initiatives must also include the societal aspect, especially in Latin America. Addressing the fundamental roots of extremism–namely, poverty, inequality, and young marginalisation–requires providing concrete chances in the real world to mitigate the digital isolation that often leads to online radicalisation.

Maria Zuppello *is an Italian journalist based in São Paulo, Brazil, with a background in investigative reporting. She has covered Latin America for several international media outlets, including The Guardian, Agence France-Presse and Infobae. Her work focuses on the crime–terror nexus, with a particular emphasis on jihadist networks in Latin America. X: https://x.com/mariazuppello*

The Nordic Front of '764': Trends, Drivers, and Countering Youth Exploitation and Radicalisation

By Valdemar Balle and Anonymous Author - January 5, 2026

On 25 November, the FBI issued a warning:

"The FBI is warning the public of a sharp increase in the activity of '764' and other violent online networks which operate within our country and around the globe. These networks methodically target and exploit minors and other vulnerable individuals. (…) Many threat actors systematically target underage females, but anyone – juveniles, adults, males, and females – can be targeted. Victims are typically between the ages of 10 and 17 years old, but the FBI has seen some victims as young as 9 years old."

This is not the first time US authorities have warned about the growing threat from the '764-network', and it won't be the last either. Other countries, like Australia, have recently issued similar warnings. Further, on 8 December, the Canadian Government formally listed 764 as a terrorist entity.

'764' is best described as a Nihilistic Accelerationist online network with little formal hierarchy but global reach. It is part of the online Com network that comprises a number of violent, exploitative, yet distinctive, networks that are terrorising a growing number of victims online and offline.

764 originated in North America in 2021, when 15-year-old Bradley Chance Cadenhead spun a small Discord server out of the earlier CVLT sextortion network and named it after his local ZIP code: 764. What began as a tight-knit US-based group of mostly English-speaking boys and young men very quickly became a transnational hub within the Com. Within a few years, US law enforcement determined that all 55 of the FBI's field offices had open 764-related cases, while parallel investigations were launched in Canada, Europe, and Australia.

From the outset, the network's infrastructure (mainly Discord and Telegram channels with spill-over onto gaming platforms like Roblox and Minecraft) made it easy for North American operators to recruit and direct peers across borders. In practice, "764" functions less as a single organisation and more as a North American–anchored ecosystem of semi-autonomous cells whose members move fluidly between US, Canadian, European and Australian time zones, swapping victims, methods and propaganda.

While originally an online-focused network, Marc-Andre Argentino points to an important new trend with a number of offline attacks taking place: "Though Com is predominantly a digital network and phenomenon, there have been some criminal activities that occurred offline, such as arson, bricking, and murder for hire. Traditionally, these offline activities were carried out by adult members associated with Cyber Com. However, Extortion Com (where 764 is found) has seen a shift in criminal activity over 2024, moving from a focus on sextortion/CSEA to offline kinetic acts of criminality."

This evolution is crucial for understanding the spread of 764. The network's culture, aesthetics and methods are easily copied: a teenager needs little more than a smartphone, access to Discord and Telegram, and an invitation link to be drawn into a world where status is earned by escalating harm. Once a local node forms, pressure from peers and admins to move from online abuse to "real-life ops" – stabbings, arson, sexual assaults – can build quickly. What begins as an American, largely online phenomenon, thus becomes a portable script for violence that can be adopted by teenagers in any country with the same platforms and subcultures.

This Insight showcases the 764 network's worrying activities in the Nordic region. It draws up a timeline of known cases in Sweden and Norway and presents new data on activities in Denmark that have otherwise not been reported in mainstream media. Finally, it presents recommendations on how to better counter these networks on macro-, meso-, and micro-levels.

Inroads into the Nordics

Against this backdrop, it is unsurprising that the 764 network has begun to surface in the Nordics. Since 2024, Sweden has been affected by four known cases, while Norway is facing one court case linked to 764. Common to all five cases – aligning well with broader trends in 764 cases – are extremely young predators exploiting and targeting young girls, and occasionally boys, in a combination of online and offline attacks in their own countries and across borders.

The first known case dates back to April 2024, when a 15-year-old boy known by his online moniker 'Chai' was sentenced to 7 months of youth supervision. Chai was found guilty of targeting a 13-year-old Swedish boy, encouraging him to: self-harm, carry out sexual acts online, and commit suicide using a knife. Despite receiving his sentence, the young Chai has allegedly managed to continue his online activities, with reports of ongoing encouragement to self-harm.

A second case was revealed when a 14-year-old boy known as 'Slain764' in July 2024 attacked a woman in her 50s on her way to work, and two months later, on 13 September, he attacked an 82-year-old man in the Swedish town of Hässelby, a suburb of Stockholm. The victims suffered severe injuries but luckily survived the attacks. Since the attacker was a minor, he initially evaded prison time despite being a leader of the global 764 network and clearly following the 764 propagated modus operandi. In addition to the two known attacks, Slain764 also carried out six other attacks, all filmed and circulated across 764 online groups.

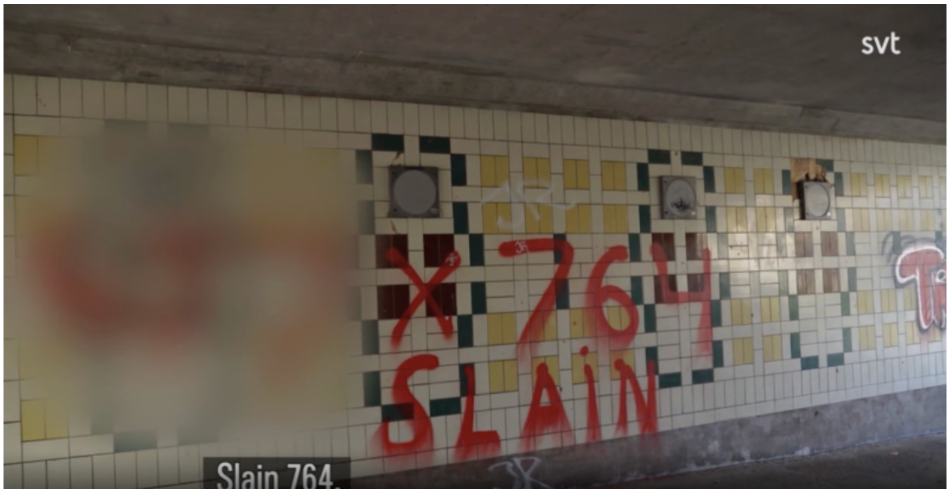


Figure 1: Screenshot from a video originally published by 764-member 'Slain' on Telegram. Credit to SVT.

'Slain764' was allegedly heading up the Swedish chapter of No Lives Matter/764, known locally as 'Mordwaffen'. What this exactly means in a network with little hierarchy is not entirely clear. Yet, Slain764 was acting as an admin in numerous Swedish 764-Telegram channels. Since he was only 14 years old when he committed the crimes, he was not criminally liable in Sweden and has ended up in youth care.

Only a few months later, in January 2025, another 14-year-old attacked a 55-year-old woman with a knife in the city of Borås. The boy himself has acknowledged carrying out the attack, yet claims that he was pressured to do so by people in the 764 network issuing threats against him and his family. Authorities, though, believe the boy acted on his own conviction linked to 764.

The most recent Swedish case was made public in April 2025 and concerns a 17-year-old boy. He was initially accused of sexually exploiting a young girl, encouraging her to commit suicide and sending manuals instructing her how to do so. More recently, new accusations have emerged accusing him of involvement in two attempted murders in June 2024 in Hässelby. While it is not entirely clear from public documents, it appears likely that those two murder attempts refer to some of the attacks linked to Slain764.

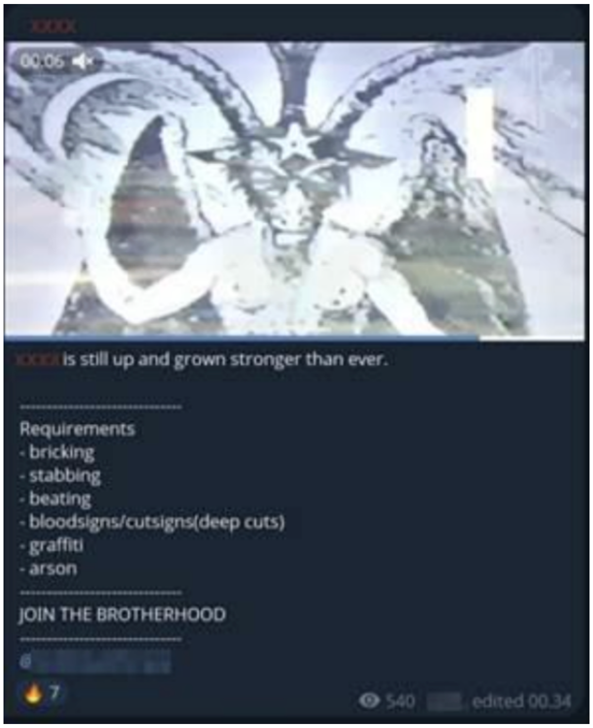
Last Summer, the Norwegian authorities arrested a teenage boy accused of links to 764 and participation in the rape of a young Australian girl. Uncovered material shows communication between the teenager and Slain764 in Sweden. Since then, another boy has come under investigation, but no information has been revealed in his case. A girl, known to have been a victim of sexual exploitation and self-harm, is also under investigation after she was encouraged by actors in the 764-network to kill a family member.

Escalating 764 Activity in Denmark and Beyond

While several incidents linked to 764 networks have already surfaced in Sweden and Norway, the threat in Denmark has, until recently, been far less understood. A new report from Darksight Analytics and the Institute for Countering Digital Extremism (ICDE) now confirms that a Danish individual holds a leading position within one of the most active 764-networks. Additionally, several Danish individuals have been observed participating in the 764-cell's official Telegram and Discord chats, indicating a noticeable increase in Danish involvement within the cell.

This network – driven in part by the Danish actor – has repeatedly coerced and extorted young victims into extreme acts, including self-harm and the production of bloodsign and cutsign material. The same individual is also linked to an alleged suicide livestream on Discord, where a victim was filmed hanging themselves in a bathroom. Although the authenticity of the footage could not be independently verified, the incident aligns with known tactics and previously documented behaviour within 764 communities.

The group's recruitment material openly lists entry requirements such as bricking (refers to throwing bricks through windows and damaging vehicles), graffiti, and arson (other acts of vandalism); stabbings and beatings (violent assaults); and the production of extortion-based self-harm content (bloodsigns and cutsigns).



XXXX

XXXX is still up and grown stronger than ever.

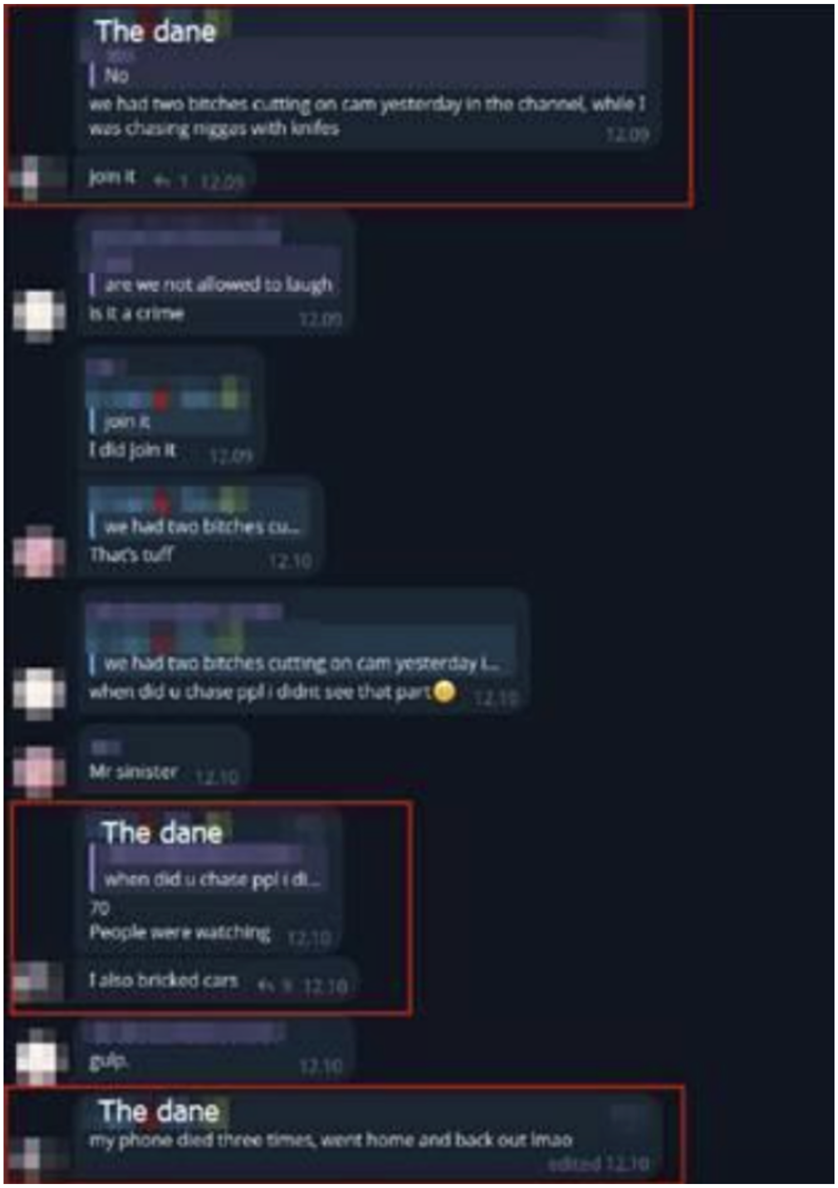
Requirements
- bricking
- stabbing
- beating
- bloodsigns/cutsigns(deep cuts)
- graffiti
- arson

JOIN THE BROTHERHOOD

@[redacted]

Figure 2: Screenshot of a recruitment post published on the 764 cells' official channel.

In early September, the Danish leader reportedly hosted a livestream in which he was seen extorting victims into self-harm, vandalising cars, and chasing random individuals while armed with a knife, as can be seen below:



The dane
No
we had two bitches cutting on cam yesterday in the channel, while I was chasing niggas with knifes 12.09

join it 1 12.09

are we not allowed to laugh
is it a crime 12.09

join it
I did join it 12.09

we had two bitches cu...
That's tuff 12.10

we had two bitches cutting on cam yesterday i...
when did u chase ppl i didnt see that part😊 12.10

Mr sinister 12.10

The dane
when did u chase ppl i di...
70
People were watching 12.10

I also bricked cars 3 12.10

gulp. 12.10

The dane
my phone died three times, went home and back out lmao edited 12.10

Figure 3: Screenshot of conversations between the leading Danish actor and other community members.

The Danish individual appears to have gained substantial traction and status within the community due to his willingness to participate in real-world incidents and conduct online extortions. As illustrated in the hierarchy chart below, he is regarded as one of the leading figures within the 764-cell.

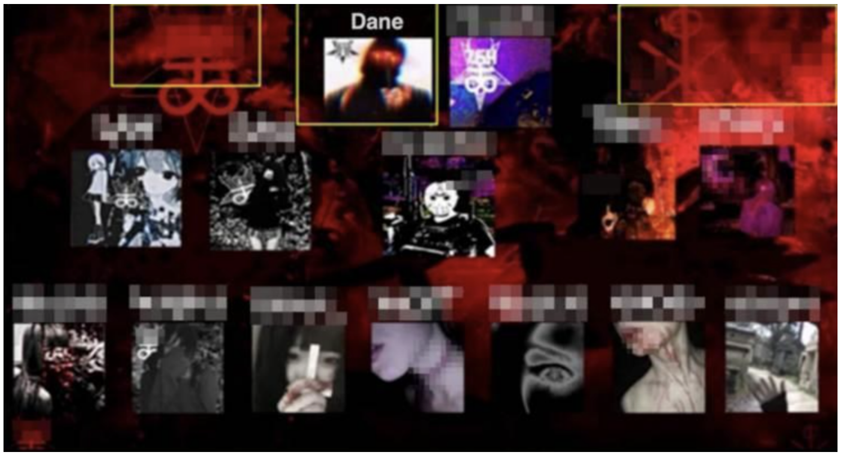
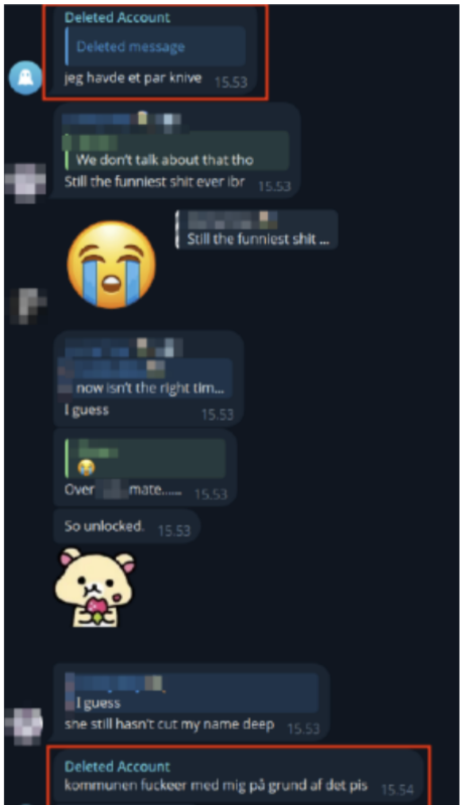


Figure 4: Screenshot of a hierarchy chart shared on Telegram illustrating the management of the 764 cell.

On Telegram, another Danish user stated that he and a friend had brought knives to school, which allegedly resulted in contact with Danish social authorities. In the context of 764 networks – where spontaneous violence against public institutions is routinely encouraged – this type of conversation appearing among Danish users signals a concerning indication of risk.



Deleted Account
Deleted message
jeg havde et par knive 15.53

[redacted]
[redacted]
We don't talk about that tho
Still the funniest shit ever ibr 15.53

[redacted]
Still the funniest shit ...

[redacted]
[redacted]
now isn't the right tim...
I guess 15.53

[redacted]
😭
Over [redacted] mate...... 15.53

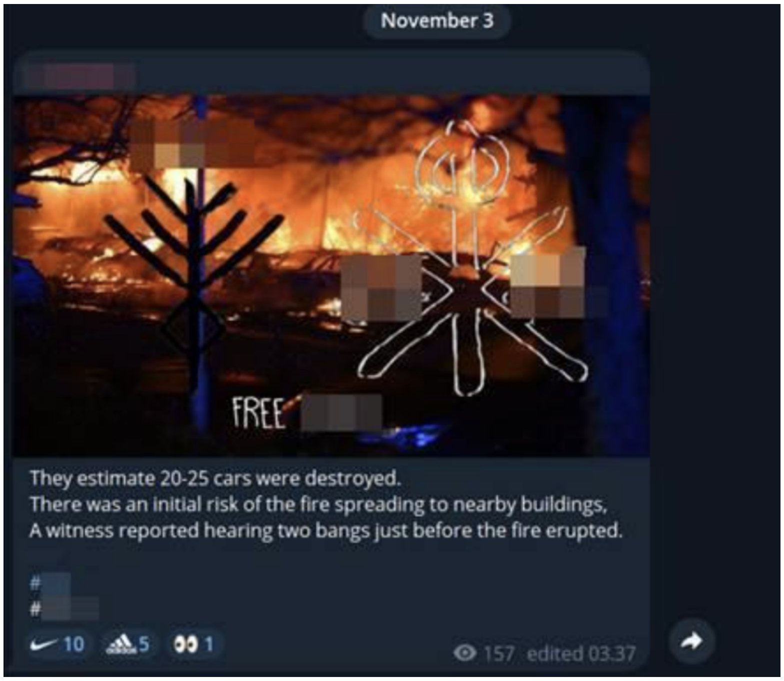
So unlocked. 15.53

[redacted]
I guess
she still hasn't cut my name deep 15.53

Deleted Account
kommunen fuckeer med mig på grund af det pis 15.54

Figure 5: Screenshot of conversations between a Danish threat actor and other community members.

On 3 November 2025, the network claimed responsibility for a major arson attack in Ängelholm, Sweden, allegedly carried out in collaboration with another 764-cell. The attack, which reportedly targeted between 20 and 25 vehicles, may have been a reaction to the arrest of one of the network's key members.



November 3

[redacted]

They estimate 20-25 cars were destroyed.
There was an initial risk of the fire spreading to nearby buildings,
A witness reported hearing two bangs just before the fire erupted.

#[redacted]
#[redacted]

10 5 1

157 edited 03.37

Figure 6: Screenshot of the 764 cell claiming responsibility for an arson attack in Ängelholm, Sweden.

As can be seen in the above announcement, the 764-network claims responsibility for the arson attack in Ängelholm, Sweden. Images collected from the scene show the scale of destruction left behind.

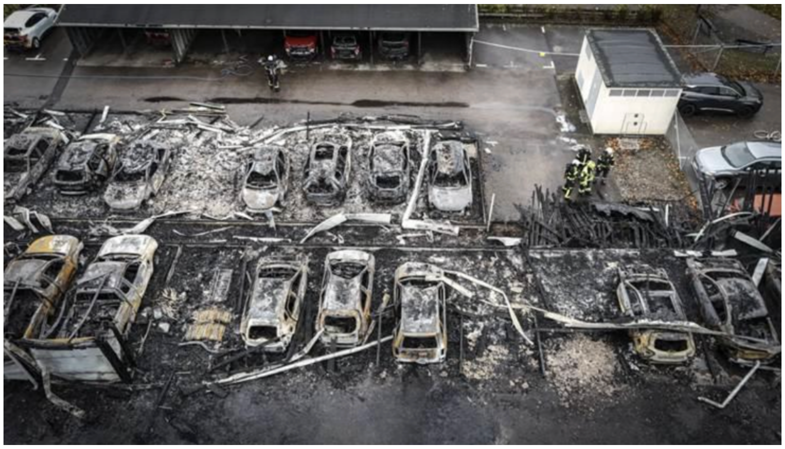


Figure 7: Screenshot showing the aftermath of the arson attack published by Swedish media HDon 03.11.2025.

Conclusion and Recommendations: Countering 764's Online Presence

While countering movements like 764 requires a broad, multisectoral effort, the platforms hosting related content remain central to mitigating this rapidly evolving threat. Social media companies must proactively identify and address conduct-related risks in the online spaces where 764-networks recruit new members and exploit vulnerable youth. The cross-platform nature of this activity further underscores the need for strong coordination and information-sharing between platforms and external stakeholders, including law enforcement agencies, child protection services, and social authorities.

It is therefore recommended that platforms significantly intensify moderation efforts across communities that overlap conceptually or behaviourally with 764. These include spaces centred on gore content, the idolisation of mass attackers, and communities that romanticise or encourage self-harm. Such environments frequently serve as entry points into 764-affiliated networks and require targeted, sustained interventions.

Because many individuals active in 764-linked networks are themselves very young, it is essential that front-line personnel working with the youth are equipped to recognise indicators of 764-affiliation. The group's terminology, symbols, and communication patterns are tacit and subculturally distinct; understanding this coded language is considered crucial for identifying both potential perpetrators and vulnerable individuals engaging with these communities online. For this reason, greater awareness and targeted training for teachers, school staff, youth workers, law enforcement and social workers is strongly recommended to enable earlier detection and timely intervention.

Valdemar Balle *is an Open-Source Intelligence specialist and researcher whose work explores the intersection of computational social science, online extremism, and online threat intelligence.*

Anonymous Author *is a member of GIFCT's Working Group on Addressing Youth Radicalization and Mobilization.*

Building Digital Trust: Youth-Led Tech Solutions to Prevent Extremism in the Horn of Africa

By Abraham Ename Minko - September 3, 2025

The Horn of Africa – a region encompassing Ethiopia, Somalia, Eritrea, and Djibouti – has long been at the epicentre of political instability, protracted conflicts, and violent extremism. Gaining access to digital technologies has been a notable shift in the region's social and political landscape, opening both opportunities and risks. In Somalia, for instance, internet penetration has surged in recent years, with an internet penetration rate of over 55% as of earlier this year. Ethiopia's internet penetration rate, meanwhile, is considerably lower, with about 21.3% internet penetration as of early 2025. Nonetheless, while extremist groups increasingly exploit digital spaces to recruit and radicalise vulnerable youth, these same technologies offer critical opportunities for engagement, empowerment, and peacebuilding. Within this duality lies the need to understand how youth in the Horn of Africa, particularly in Ethiopia and Somalia, can be supported in creating digital trust frameworks to resist radicalisation and build inclusive, resilient societies.

Youth in this region represent a majority demographic, often marginalised economically, politically, and socially. This exclusion has made many susceptible to the lure of extremist ideologies that promise identity, purpose, and belonging. However, the same youth also possess the creativity, technological adaptability, and grassroots insight necessary to drive community transformation. Increasingly, young people in Ethiopia and Somalia are turning to digital tools not only for self-expression but as a means to challenge violent narratives, bridge inter-communal divides, and create localised peace initiatives. This Insight proposes that youth-led, tech-driven interventions – particularly those centred on digital storytelling and community-based cyber hubs – can serve as sensitive and sustainable mechanisms to prevent violent extremism. Unlike conventional counter-terrorism efforts that often rely on top-down or securitised strategies, youth-led initiatives foster trust, dialogue, and agency from within communities. Ethiopia and Somalia offer compelling case studies: in Somalia, youth-run media and peace platforms are reclaiming narrative spaces from terrorist groups like Al-Shabaab; in Ethiopia, digital activism is emerging amidst ethnic and political tensions as a force for reconciliation and civic engagement.

Youth-Driven Digital Storytelling to Counter Extremist Narratives

Youth in Somalia and Ethiopia are increasingly harnessing digital storytelling as a proactive means to challenge violent extremist propaganda. In Somalia, organisations such as the Federation of Somali Journalists (FESOJ), supported by BBC Media Action and EU funding, have trained journalists and young content creators in Mogadishu to produce social media content focused on conflict prevention and peacebuilding.

Figure 1: FESOJ Conducted Training for Youth on Co-Producing Social Media Content for Conflict Prevention and Peace building in Mogadishu, April 2025. Source: FESOJ.

These trainings – which cover ethics, storytelling, vox-pop interviews (brief, informal street-style interviews), and social media strategy – equip youth to craft narratives that counter violent extremist discourse while modelling digitally safe and responsible practices. A powerful example is the work of Nairobi-based Somali youth collective Badbaado Team, which produces short films and talk shows addressing issues like tribalism, human trafficking, and drug abuse. Their visual dramas reach growing audiences across social media, and in one instance, reportedly dissuaded a young man from pursuing smuggling, demonstrating the immediate personal impact of locally relevant storytelling.

Parallel initiatives in Ethiopia emphasise digital literacy as a foundation for resilient digital communities. The #DefyHateNow project works across Oromia, Dire Dawa, and other regions to train youth, educators, and content creators in fact-checking, media literacy, and responding to hate speech online. By elevating youth voices to debunk disinformation and hate rhetoric, #DefyHateNow builds a digital movement of peer educators and storytellers promoting inclusive narratives. In Dire Dawa, a USAID-funded program led by Synergie for Community Development engaged hundreds of high school and university students, and local influencers, to create positive social media campaigns under the banner of #HateFreeEthiopia. These campaigns, rooted in peer-to-peer digital storytelling, foster civic participation and reinforce a collective identity resistant to extremist messaging.

The theoretical rationale behind these interventions lies in narrative psychology: stories anchor identity and shape meaning, especially for young people navigating conflict-prone environments. Violent extremist groups often fill vacuums left by social or economic exclusion, offering simplistic, emotionally compelling stories. Youth-led digital storytelling counters this by empowering communities to craft and circulate counter-narratives rooted in local languages, cultural nuance, and lived reality. Training initiatives that focus on digital safety and ethical media use not only enable impactful storytelling but also foster trust in youth-generated content—increasing its visibility and acceptance. These projects demonstrate how, in both Somalia and Ethiopia, youth can reclaim the digital sphere through artful, grounded storytelling that promotes resilience, dialogue, and peace. Their work offers a scalable model: by investing in digital media skills, cultural authenticity, and locally driven narratives, peacebuilders can chip away at extremist appeal and nurture a generation able to redefine the dominant narrative from within.

Community-Based Digital Hubs for Trust-Building and Early Warning

In Somalia, grassroots digital platforms are forming vital bridges between young citizens and community institutions, fostering trust and enabling early detection of conflict dynamics. The Daldhis initiative, for instance, combines SMS-based citizen scorecards, radio call-ins, and local government feedback loops to create an interactive civic-feedback mechanism in towns like Baidoa and Kismayo. These digital hubs don't just relay grievances—they amplify youth voices and translate real-time concerns into governmental responses, gradually building institutional credibility and social cohesion. This two-way communication structure also encourages young people to share emerging community tensions or rumours, effectively functioning as grassroots early warning systems against radicalisation or violence. Across Somalia, platforms such as Daldhis and early warning systems implemented by NGOs like Manaal Relief Foundation (MRF) gather information about land disputes, competition over natural resources, election and clan tension, and livelihood insecurity. These grievances – linked to service delivery, political marginalisation, and communal tension – are collected via SMS, radio call-ins, and digital scorecards, allowing communities to report concerns as they emerge. In particular, the technology-enabled early warning systems in Somalia enable local youth and community volunteers—sometimes called EWER "champions"—to capture reports of potential violence or rumour-based tensions. These reports are collected through mobile phones (SMS) or voice-based systems and are processed through cloud-based reporting platforms such as WikiRumours. Community platforms verify, analyse, and share the alerts with local authorities and peace committees, triggering timely mediation or response.

Complementing such local efforts, broader regional platforms like IGAD's trainings for Somali youth showcase the connective potential of regional digital hubs. Workshops held in Jigjiga engaged Somali participants with Ethiopian facilitators in creating youth-driven counter-extremism strategies—embedding technology, dialogue, and community-based early warning into program design and policy development. At the regional level, the IGAD Center of Excellence for Preventing and Countering Violent Extremism (ICEPCVE) plays a coordinating role in knowledge-sharing and disseminating best practices for community-based digital approaches across the Horn of Africa. What makes these hubs most effective is their grounding in local social infrastructure and trust. In both contexts, community leaders, educators, and youth co-create digital spaces where sharing critical information doesn't threaten personal safety or social reputation. Parallel to hubs, national-level digital youth portals such as the Somali Youth Hub – run by the Ministry of Youth and Sports – offer virtual forums, idea submission sections, blogs, and storytelling features built with accessible, mobile-friendly web design using platforms like WordPress. These platforms enable youth to share experiences, pose questions, contribute ideas, and engage with peers and policymakers in a moderated digital setting. Technology-driven co-working spaces and innovation labs, such as the iRise Tech Hub and SiHUB in Somalia, offer digital infrastructure, mentoring, and incubation services. These hubs support mobile-first initiatives and leverage social media, workshops, and networking to produce tech-enabled peace and civic campaigns. This trust is built through transparency, inclusive participation, and partnership with local institutions. These initiatives gain legitimacy and attract youth participation by embedding digital hubs in existing communal frameworks – schools, religious networks, and local radio stations. The early warning function emerges naturally as youth report localised tensions or misinformation through trusted channels, triggering peer-led responses or stakeholder dialogues.

Together, the Somali and Ethiopian case studies illustrate how community-based digital hubs can serve dual functions: strengthening trust between youth and institutions while enabling the timely detection of conflict drivers. These hubs model a transition from securitised, outsider-imposed counter-extremism to participatory, tech-enabled resilience built from the ground up.

Policy Implications

Governments in Somalia and Ethiopia should adopt holistic digital governance strategies that align with continental best practices, such as the African Declaration on Internet Rights and Freedoms. National policies must guarantee equitable internet access while safeguarding freedom of expression, privacy, and anonymity—principles essential to fostering trust in youth-led digital civic spaces. By embedding these rights into legislative frameworks, authorities can legitimize community-based digital hubs and support youth-generated content that counters violent extremism without risking censorship or repression.

Tech firms operating in the Horn of Africa can play a transformative role in counter-extremism efforts by partnering deeply with the community-based digital infrastructure already being built. In Somalia, telecommunications firms like Hormuud Telecom have taken the lead in expanding 4G and even 5G connectivity across urban and rural areas, facilitating reliable access for underserved youth populations. As digital hubs and youth-driven initiatives emerge, tech companies should strategically integrate into these trusted local spaces. For instance, APIs or platform access agreements could empower digital hubs to stream their locally produced content, host interactive webinars, or use mobile money micropayments to incentivise positive engagement. Tech providers reinforce trust, visibility, and sustainability of community-led narratives by aligning with youth-run centres rather than only offering top-down programs. Advanced solutions such as AI-powered early warning analytics constitute another promising frontier. Youth-run hubs and civic technology centres already collect real-time input on tensions, rumours, or sensitive local developments. Tech companies could provide shared analytics tools—using natural language processing, sentiment analysis, or dashboard alerts—to detect rising narratives or sudden spikes in extremist-relevant terms, thereby supporting grassroots resilience efforts. These tools can be embedded in the civic-feedback mechanisms like Daldhis in Somalia or community hubs in Ethiopia to trigger peer-led interventions or escalate warnings to NGOs and local authorities. Crucially, this model centres youth and civil society as users of—but not substitutes for—digital intelligence, keeping ownership local while enhancing capacity.

In parallel, integrating counter-extremism objectives into local governance plans strengthens the impact of digital interventions. As research from East Africa confirms, placing P/CVE (Preventing/Countering Violent Extremism) responsibilities at the local government level allows tailored, context-responsive initiatives informed by youth most at risk. Ethiopia's regional administrations and Somalia's district councils can allocate resources to youth-run cyber hubs, ensuring these spaces are rooted in local institutions, staffed by trained facilitators, and supported with modest operational funding.

Investing in digital infrastructure and literacy is also vital. Reflecting lessons from Kenya and other African countries, policy must support the expansion of affordable broadband connectivity in underserved areas, while promoting digital literacy through schools and youth centres. In practice, the Ethiopian government could partner with telecom operators and community networks to improve access in rural Oromia or Somali regions, while simultaneously funding training in critical thinking, fact-checking, and media ethics.

Effective policies must also foster cooperative platforms between youth, civil society, religious and clan leaders, and institutions. Counter-extremism in Somalia requires not only a rapid national response but also a localised pushback: engaging clan elders, religious figures, women leaders, and youth influencers in crafting and disseminating counternarratives enhances credibility and reach.

Policymakers should formally support multi-stakeholder councils that guide digital hub content and amplify local voices. Lastly, regional coordination through entities like the Horn of Africa Digital Governance and Cybersecurity Initiative, supported by the EU and ITU, offers an important foundation for P/CVE policy coherence across Ethiopia, Somalia, Djibouti, and beyond. National governments should participate actively in such platforms to harmonise cybersecurity policies, share best practices for youth engagement, and ensure digital interventions respect human rights. A regional approach enables scalable models, peer learning, and pooled resources for sustainable support of youth-led digital resilience initiatives. Collectively, these policy directions—

rooted in digital rights, local governance integration, infrastructure expansion, inclusive stakeholder engagement, and regional cooperation—can build an enabling environment where community-based digital hubs thrive. By translating policy into actionable support, governments empower youth to become digital peacebuilders, drive early warning mechanisms, and counter extremist narratives from within their communities.

***Abraham Ename Minko** is a senior researcher and policy analyst in Peace, Security, and Conflict Resolution. He holds a Ph.D. in Political Science and International Relations. His research interests are UN Peace Operations, Terrorism and Counter Violent Extremism, Peace and Conflict Resolution, Mediation and Negotiation, International Humanitarian Law and Armed Conflicts, Peacekeeping, and Peacebuilding.*

Escape The Void: Responding to Youth-Led Nihilistic Violence

By Pierre Sivignon - February 2, 2026

In December 2025, Canada designated 764 and Maniac Murder Cult as terrorist entities, amid a growing international concern over what the FBI and the U.S. Department of Justice have termed Nihilistic Violent Extremism (NVE). Also in December 2025, New Zealand took similar action as Canada, against the Order of Nine Angles and Terrorgram, two networks associated with far-right accelerationism and frequently cited as influential within NVE ecosystems. These designations reflect mounting governmental concern over the rise of 'violence-focused online communities', particularly those linked to The Com and its affiliated groups. Since the late 2010s, such communities have proliferated online and spread globally, with arrests reported in at least 29 countries, according to Marc-André Argentino, as of September 2025. These communities glorify violence and its perpetrators while engaging in manipulative and coercive practices that draw young people into committing extreme acts of violence against others, animals, or themselves. The behaviours promoted range from self-harm and animal cruelty to the production and distribution of Child Sexual Abuse Material (CSAM), assault, murder, and incitement to hate crimes and terrorism. While the full scope of this phenomenon – hereafter referred to as nihilistic violence – remains difficult to determine, the growing number of documented cases and victims underscores the urgent need for targeted and coordinated responses. In line with this observation, this Insight first examines the characteristics and drivers of nihilistic violence, before exploring how existing prevention and intervention strategies might be adapted for greater effectiveness.

Post-Ideological Violence: Defining Nihilistic Violence

Nihilistic violence is a complex phenomenon that has been given many names, reflecting ongoing debates about its ambiguous nature and its relationship to violent extremism. Examples include Nihilistic and Apocalyptic Violent Extremism, Sadistic Online Exploitation, Participatory Memetic Violent Extremism, and online cult communities. While this Insight does not seek to arbitrate these debates, it is important to note that viewing nihilistic violence simply as a subcategory of violent extremism likely obscures its specificities, not least the fact that ideology plays little role. By contrast, the concept of violence-focused online communities, proposed by Leena Malkki and colleagues, situates the phenomenon within a broader ecosystem or continuum of toxic and marginal online subcultures and is therefore adopted in this Insight.

In practice, a significant number of these communities – including some of the most influential, such as 764, No Lives Matter (NLM), and Maniac Murder Cult (MKY) – are affiliated with the decentralised cybercriminal ecosystem known as The Com (short for The Community). It comprises subgroups and networks that vary in structure and scope, ranging from informal group chats to structured organisations. These promote and engage in three main types of illegal activities: cybercrime, sextortion, and offline acts of physical violence. Rather than constituting a fully-fledged organisation, these groups form a fluid network – an 'ecosystem of semi-autonomous cells' and splinter groups that both compete and collaborate with one another. For instance, recent criminal cases related to 764 have involved subgroups such as Greggy's Cult, 764 Inferno, and 8884. Violence-focused communities exhibit several recurring characteristics and dynamics:

- Non-ideological motivations: motivations, goals and justifications are predominantly non-ideological, detached from coherent political or religious narratives, yet anchored in nihilistic and misanthropic discourses.
- Autotelic violence: violence occupies a central and autonomous role as both 'the medium and the message'; it is neither strategic nor instrumental, but an end in itself, glorified for its own sake.
- Performative markers of belonging: aesthetics, symbols, and performative or memetic practices supplant ideology as markers of membership, with participation driven by grooming, coercion, and peer-led socialisation rather than ideological indoctrination.
- Youth-led participation: communities are youth-led, with young perpetrators and victims often comprising vulnerable minors facing mental health challenges, eating disorders, bullying, and social isolation, and who may shift between the roles of perpetrator and victim.
- Cross-platform dynamics and modus operandi: communities operate across multiple platforms – mainly Discord and Telegram – to identify and target vulnerable users, draw them into private and increasingly transgressive spaces (servers, group chats, channels etc.), and coerce them through grooming, sextortion, or threats. For instance, a victim may be first contacted on a mainstream platform such as TikTok or X and subsequently moved to private spaces on Telegram or Discord.
- Hierarchies and status-seeking: group dynamics are coercive and hierarchical, and status is earned through escalating violent acts, which are systematically documented and archived both as a means of gaining peer recognition and of exerting control over victims.
- Distinctive culture and language: communities cultivate their own folklore and coded language, including terms and practices such as 'lorebooks', 'fansigning', 'cut signs' or 'blood signs', alongside other community-specific symbols.

A Hybrid Space: Continuities and Ruptures with Adjacent Phenomena

In the late 2010s, violence-focused communities emerged against the backdrop of increasing hybridisation and ideological cross-pollination within extremist ecosystems. These broader dynamics have produced groups, networks, and ideological profiles shaped by multiple, and sometimes contradictory, influences. As a result, many radicalised individuals, particularly in Europe and North America, no longer exhibit coherent extremist belief systems. Scholars and practitioners have described this phenomenon using concepts such as 'Mixed, Unclear, and Unstable' (MUU) ideologies, 'salad bar' belief systems, 'fringe fluidity', Composite Violent Extremism (CoVE), or Hybridized Prefatory Extremism (HYPE). Irrespective of the terminology used, this phenomenon reflects an escalating trend in extremist violence, increasingly characterised by an 'amalgamation of disparate beliefs, interests, and grievances'. Nihilistic violence represents one manifestation of this broader paradigm, exhibiting a dual form of hybridisation: within violent extremist ecosystems, and between violent extremism and other forms of online harm, criminality, and violence.

Violence-focused communities are therefore shaped by multiple influences, drawing selectively from adjacent subcultures and extremist ecosystems, including ideologically motivated ones. The primary influences include far-right or 'militant' accelerationism (e.g. Siege Culture, the Order of Nine Angles, Terrorgram, 'Saints culture', etc.), the most extreme subsets of the True Crime Community (TCC), and gore and snuff communities (notably 'hurtcore'). These influences are evident in the aesthetics, symbols, modes of action, and practices of violence-focused communities, as well as in their interactions with extremist ecosystems and related phenomena. Crucially, they function primarily as cultural reservoirs and visual repertoires, rather than as direct ideological drivers.

That said, fragments of ideology, or secondary ideological motivations, can also be observed in some groups, particularly MKY, as well as in individual trajectories. For example, the France-based founder of CVLT, which inspired 764, ran a fascist Discord community called 'Harsh Reality', which has since been taken down. Similarly, a MKY leader from Georgia apprehended in 2024 openly adhered to neo-Nazi accelerationist ideology, disseminating a manifesto entitled 'The Hater's Handbook'. The production of manuals, guides, and manifestos is a common practice among violent extremists and has also been adopted by NLM ('Manhunt Guide' and 'NLM Kill Guide') and 764. In November 2025, an individual connected to 764 was arrested in the United States; the FBI discovered writings outlining plans for terrorist attacks, including joining the Islamic State and returning to the US to carry them out. The interplay of continuities and ruptures with ideologically motivated extremism and adjacent phenomena positions nihilistic violence within a hybrid space, situated between violent extremism, marginal online subcultures, and (cyber)criminal networks.

Crisis & Affordances: Explaining the Emergence of Nihilistic Violence

It is important to analyse: why did violence-focused online communities emerge in the late 2010s? The following discussion advances a set of hypotheses across three interlocking levels: societal, structural, and individual. This analytical framework is inspired by the work of Lewis Brace and colleagues on MUU ideologies. In summary, the argument is that nihilistic violence emerges from the interplay of three factors: a conducive socio-cultural context (societal level), the exploitation of enabling technological affordances (structural level), and widespread, youth-related personal vulnerabilities (individual level). This framework is not just analytical; it also has practical implications for prevention and intervention strategies, which should address all three levels simultaneously.

- At the societal level, nihilistic violence emerged in a specific context, characterised by a 'crisis of meaning', a deepening youth 'mental health crisis', and a 'global polycrisis'. The impact of major crises and disruptive events on young people, including the COVID-19 pandemic and associated lockdowns, has created a fertile environment for the development of nihilistic worldviews. In this context, nihilistic violence can be understood as one of the most extreme manifestations of generational anxieties, pessimism, and social disconnection.
- At the structural level, violence-focused online communities have probably benefited from the 'technological affordances' of platforms such as Discord and Telegram. Certain features on these platforms may create an environment conducive to grooming, coercion, and violent behaviour. These include closed or invitation-only groups, persistent and archive-like communication, support for sharing multimedia content sharing, and role-based hierarchies on Discord. Together, these features can do more than simply provide a space; they can actively shape communities. Discord, in particular, is perceived by violence-focused communities as 'multi-purpose', supporting all stages of the victimisation process within a single environment. Consequently, since becoming aware of 764's existence in 2021, Discord has been actively trying to disrupt its activities on its services by investing in moderation tools, teams and techniques. In 2023 alone, 34,000 user accounts associated with 764 were taken down. Furthermore, Discord's relevant safety policies, including the Teen and Child Safety Policy, Suicide and Self-Harm Policy and Violence and Graphic Content Policy, which were last revised in August 2025, explicitly prohibit CSAM, grooming, sextortion, self-harm, depictions of gore and animal cruelty, and the glorification of mass murderers or serial killers. That said, it is not the platforms themselves that matter, but the affordances they offer. These groups could theoretically jump to platforms with similar features as Discord and Telegram.

- At an individual level, personal vulnerabilities, including mental health challenges, experiences of bullying and social isolation, are directly exploited by violence-focused communities, especially 764, and during all stages of the victimisation processes. Peer dynamics, personal quests for 'status' or 'significance', and hierarchical structures reinforce escalation dynamics. Lastly, repeated exposure to graphic and violent content may desensitise some young people to such material and even give them a 'taste' for it, laying the 'groundwork for an identity and social relationships built around the glorification of violence'.

Recommendations: Rethinking Prevention and Intervention

Nihilistic violence is 'post-ideological' and does not stem from indoctrination or coherent belief systems. Consequently, P/CVE approaches focused on ideological disengagement are ill-suited, and mobilisation to violence can occur rapidly, narrowing the window for intervention. This underscores the relevance of a 'public health approach' to nihilistic violence, focused on reducing 'risk factors' and strengthening 'protective factors' at individual and societal levels, rather than on ideology or at-risk groups. It prioritises 'indicative behaviours' and social conditions such as isolation, lack of purpose, and weakened belonging, to foster long-term resilience.

Early detection and exit support are critical. Families, teachers, educators, and frontline professionals should be equipped to recognise warning signs – such as 'obsessive interest in gore, fascination with mass killers, or performative displays of cruelty' – through targeted training and awareness-raising. The ISD risk assessment framework, covering 'indicators', 'accelerants', and 'triggers', offers a valuable tool for guiding early identification. Given the prevalence of blackmail and coercion, exit pathways must be trauma-informed and supported by specialised services.

Platform-level measures are equally essential. Major platforms have invested in Trust & Safety, including dedicated moderation teams and techniques, automated detection systems, reporting mechanisms, and safety policies, and some, such as Discord, also participate in cross-industry initiatives through their GIFCT membership. However, nihilistic violence reveals gaps in current systems, which are primarily designed to detect content rather than behaviours. Beyond youth safety-by-design measures, tech platforms can reinforce their responses through:

- **Cross-platform strategies.** Because violence-focused communities exploit multiple platforms and their distinctive features, both affected platforms and at-risk platforms should adopt coordinated cross-platform responses. Platform-specific measures are insufficient to address recruitment, group migration, reconstitution, and hybridisation. Only collaborative approaches can disrupt the full cross-platform victimisation cycle. Concrete measures include data-, information-, and hash-sharing, as well as other joint enforcement mechanisms.

- **Adjacent community monitoring.** Platforms should extend oversight to adjacent communities that frequently function as gateways or recruitment pools (e.g. extreme true crime, gore, gaming, and mental health–related spaces). Particular attention should be paid to recruitment tactics and outlinking practices across affected and at-risk online environments.
- **Behavioral risk detection.** Content moderation should be complemented by behavioural analysis to identify patterns of recruitment, grooming, coercion, and escalation. In this respect, Discord's use of machine-learning models based on metadata and network dynamics is particularly relevant, as addressing nihilistic violence requires systems that move beyond explicit content violations to detect subtler behavioural signals.
- **Targeted capacity-building.** To support the identification of grooming dynamics, coded language and coercive group structures, platforms should invest in bespoke training for moderators, supported by long-term partnerships with researchers, NGOs and frontline practitioners.

Finally, societal-level interventions must address the 'crisis of meaning' characteristic of our digital age, as well as the existential void exploited by violence-focused online communities. Initiatives that foster digital literacy, social (re)connection, and meaningful offline engagement can likely reduce the appeal of these communities.

***Pierre Sivignon** is a Project Manager and Analyst working in European security and defence cooperation. He specialises in analysing, preventing, and countering transnational and hybrid threats, including radicalisation and violent extremism (P/CVE), Foreign Information Manipulation and Interference (FIMI), and Transnational Organised Crime (TOC). He manages and coordinates EU projects tackling illegal, violent, and harmful online activities, while also contributing to open source intelligence (OSINT) studies and investigations. He also contributes to the EU Knowledge Hub on Prevention of Radicalisation (Thematic Panel "New Technologies and the Online Dimension").*

The Feed That Shapes Us: Extremism and Adolescence in the Age of Algorithms

By Cecilia Polizzi - December 12, 2025

In today's digital ecosystem, radicalisation no longer takes root in ideological echo chambers but permeates into the speech, humour, and emotional syntax of youth culture. Online spaces once reserved for socialisation and self-expression now double as arenas where identity, belonging and ideology collide.

In the attention economy, algorithms reward engagement over nuance, and outrage may travel faster than empathy. In this online ecosystem, effective prevention requires helping young people understand the very architectures that shape what they see, how they feel, and who they connect with. Reframing prevention as the cultivation of participatory design, the Insight proposes an alternative paradigm for thinking about youth not only as passive consumers, but also as co-creators of ethical norms in their digital coming-of-age.

Facing a fragmented, algorithm-driven digital environment, we may need to shift from a traditional reliance on content moderation and takedowns toward an infrastructure that promotes transparency in recommender systems. Algorithmic literacy may be the key missing element in devising more effective responses to the online logics of extremism and radicalisation.

The New Topography of Youth Radicalisation

An analogy by Oren Segal of the Anti-Defamation League (ADL) captures the accessibility of ideologically-oriented content and its normalisation within everyday digital routines: "Accessing a world of hate online today is as easy as it was tuning into Saturday morning cartoons on television". The irony, of course, is that for many children and young people, the algorithmic equivalent of "Saturday morning cartoons" now comes scripted by extremists.

Terrorist and violent extremist (TVE) digital engagement has evolved from a one-way conversation, primarily marked by its educational and propaganda value, into an extensive overreliance on social media as a novel, interactive, and user-friendly tool. These interactions no longer demand specific pre-existing orientations, interests or access know-how, and enable the broadcasting of extreme ideologies to friends, families, and wider audiences.

Within the current threat landscape, social media not only plays a central role at some stage of an individual's radicalisation process but also sustains the infiltration and projection of influence over virtually every aspect of their life. Through various iterations of social media ideological inoculation, concerns over privacy and anonymity have become increasingly important and pushed both violent discourse and extremist or extremist-adjacent online cultures onto encrypted platforms, such as Telegram and Gab.

The necessity to withdraw from the public mainstream of ideology, partly due to moderation and other containment efforts, led to what some scholars defined as a 'visual turn'. Seemingly innocent memes, humour, and fandoms now add a layer of versatility and inherent lightheartedness to violent narratives, increasing the appeal of adopting specific ideological orientations. For example, the far-right accelerationist 'Terrorgram' network has operated as a neo-nazi subculture on Telegram, promoting violence through a unique visual style and aesthetics that both defines the Terrorgram brand and reinforces in-group identification.

Irony and satire assume a central role in entrenching youth in extremist communities while desensitising them to the racism, sexism, and radical rhetoric that permeates this online discourse. Extremists develop their own language, and frequently unite by antagonising authority and 'political correctness'. Behaviours specific to the modern digital subculture, including provocative posting practices and meme-making, represent important pull factors for engagement while simultaneously challenging identification by counter-terrorism and extremism practitioners. Shitposting and trolling, or the use of otherwise deliberately offensive and provocative content, simultaneously mask extremists and solidify intra-group bonds.

Blame the Algorithm?

Multiple incidents across the United States and Europe ignited a debate over the surfacing of hate speech, misinformation, hoaxes and the role of algorithmic recommendations in amplifying extremist material.

Hoaxes and misinformation can serve as entry points into extremist ecosystems. In 2016, Hoaxmap documented how, during the refugee influx in Germany, a wave of false claims about crimes allegedly committed by refugees circulated widely, fueling xenophobia and far-right mobilisation. Similarly, following the Buffalo shooting, researchers found that the perpetrator had transitioned from mainstream video clips of firearms to white supremacist manifestos via recommendation engines and related content links.

The concern is that automated content suggestions on social media and video platforms facilitate the fall of both intentional and unwitting youth into radical digital rabbit holes where exposure to extreme or antagonistic content is perpetually escalating and self-reinforcing.

Algorithms designed to maximise engagement shape what is sent to users based on their digital footprints and frame personal online activities by controlling what is seen and when. Algorithms promote controversial or sensational material by prioritising metrics such as likes and shares, creating a feedback loop that may amplify fear, anger, outrage, and polarising narratives. This can make users vulnerable to radical content or susceptible to extremism, while strengthening a sense of community and belonging within digital subcultures.

Theories of direct media effects on radicalisation were subsequently developed, alongside a preliminary definition of algorithmic radicalisation as "changes in human attitudes, beliefs, or behaviour as individuals are directed to extremist content, networks, groups, or other individuals as a result of guided searches, filtered news feeds, recommended videos, and connections from extremist adjacent sites". However, while it is undeniable that automated content suggestions remain powerful tools for malign actors, blaming the algorithm alone may fail to address a more complex reality.

Exposing someone to far-out ideas is unlikely to suddenly change their perspectives or raise their critical thinking skills. Algorithmic exposure to extremist content on one platform may surface via referrals from other sites, and young users are not simply passive consumers but often interpreters, curators, and even co-producers of their own 'algorithmic reality' within digital systems. Youth interpret and negotiate meaning through their social, emotional, and cultural lenses, decide what to engage with, remix or reject, shape feeds through interactions, and even when doing so 'ironically,' train the system on their preferences. Ultimately, they may perform in ways that resist or subvert violent content.

Beyond Top-Down Approaches: Participatory Design and Algorithmic Awareness

Moderation, deplatforming, intelligence-gathering and censorship have been widely adopted by governments and tech companies alike to counter the spread of online radicalisation. However, the extent to which these top-down approaches offer robust solutions remains unclear. While they often attract criticism, they tend to achieve only temporary disruption, push users to less-regulated platforms, and raise concerns about potential infringements on fundamental freedoms.

A more constructive direction is emerging through participatory design as an iterative and flexible process that closely involves youth-aged users in shaping healthier digital environments. Research on children and youth's participation in different roles in the design of technologies, including those driven by Artificial Intelligence (AI), demonstrates that while harms have been increasingly recognised, young demographics have been underexplored as potential contributors to the future of responsible AI. The involvement of young people in participatory design can play along a continuum ranging from "users to testers to informants to design partners." As Iversen et al evaluated each of these roles in terms of their objectives, processes, and outcomes, they went on to propose the role of protagonists, in which children are the primary agents of the design process. It is also recognised that young end users, when given the opportunity, can make meaningful contributions in the design of algorithmic systems.

A study by Noh et al, exploring algorithm auditing as a potential entry point for youth to assess generative AI, demonstrates that adolescents can detect harmful behaviours in technologies they are familiar with that would otherwise go unnoticed. The capacity of minors to confront AI harms is equally visible in real-life settings. For example, a youth-led protest in the United Kingdom led the government to terminate the use of an AI grading algorithm due to the inequities it caused to working-class students. It is therefore clear that young users are not only capable of understanding, assessing and even manipulating the logics of algorithmic systems, but also can articulate what fairness, accountability and effectiveness should look like in practice.

Overcoming barriers to youth agency while simultaneously safeguarding teenagers from radicalisation and algorithmic influences requires increased transparency into social media mechanisms as part of sustained pedagogical practice. Disruptions caused by digitalisation "span from news to culture, from formal knowledge systems to everyday sense-making", and concern not only young people's access to accurate information but their ability to exercise control over the acquisition of knowledge, or otherwise how beliefs are formed and revised. Algorithms, based on predictive modelling, big data, and the optimisation of attention, intervene in the production, circulation, and legitimation of meaning by structuring knowledge hierarchies, ranking content, and determining visibility. The term 'attention ecology' provides a conceptual framework for understanding the role of algorithms in shaping the flow, peaks and decay of visibility across online ecosystems. Users' micro-level activity is aggregated to increase visibility and may exceed virality thresholds. However, attention itself, more than the content of any trend, appears to be the driving force behind hyper-circulation and network saturation. Recommender systems' societal impacts, defined by some scholars as the foundation of an 'epistemic crisis', call for algorithmic awareness, or otherwise the ability to understand how automated systems work, identify their operative logics, acknowledge the biases they embed, and analyse the symbolic, social, and cultural effects they generate in individuals and collectives.

"Trending" Isn't Harmless: What Follows

AI is now omnipresent in a range of commercial tech and a keystone of content distribution and engagement on social media platforms. Recommendation tools are designed to optimize users' experiences and facilitate information access by presenting them with the most "relevant" content according to a series of pre-set criteria. The tagline "this is trending" quantifies attention and repackages it as a statement of value. It is so common and misleadingly innocent that it frequently passes from speaker to listener without a chance to question its validity. For several forms of communication and broadcasting, the fact that something is "trending" itself constitutes the ultimate goal of producing it, or, otherwise, millions of visits, views, likes, and shares.

Teens are especially susceptible to algorithmic influence because they regularly interact with a new socio-technical environment that has fundamentally displaced the centrality of traditional cultural transmission from schools, families, and mass media to platforms governed by algorithmic architectures that automate identity exploration and community formation. Youth cultures on the Internet are intrinsically ambiguous, layered, and aestheticised. Their fusion with extremist ideology stylises terrorism through art, music, and manifestos, trivialises and gamifies violence through scoreboards, and makes radicalisation more appealing and harder to detect. In the end, "It is just a joke," until it isn't.

The impact of data-driven technology on young people, both at an individual and social level, is shaped by a complex interplay between the interactions of browsing users and the intelligent components of the platforms. The opacity surrounding recommendation systems complicates the ability to clearly size and scope extremism threats. It creates uncertainty about the rules governing content amplification, the pathways through which users are funnelled into digital rabbit holes and get fed increasingly radical material, and whether violent or extremist language was coded or simply went undetected. Algorithmic transparency, or otherwise making the built-in systems that decide what you see, which videos appear next and which accounts or hashtags are suggested, understandable, auditable and accountable, is, however, hampered by trade secrets and 'black box' complexities.

Thus, youth participation and understanding of the dynamics that seek their attention play a determinant role. Platforms, as well as the technology behind them, are moving targets, and preventing youth radicalisation should prioritise strategies that inform young people navigating the digital environments they already inhabit and equip them to be authorities in their own online safety.

Cecilia Polizzi *is an international security strategist and leading expert on child recruitment and radicalization. She has shaped policy and strategy for national governments and multilateral organizations, including NATO, OSCE, the Council of Europe, the European Commission, and UN agencies. Polizzi has spoken before the United States Institute of Peace, the Italian Ministry of Defense, and other high-level institutions, and has published extensively in academic journals and other outlets. She is the Founding CEO of the Next Wave Center, a leading organization in the counter-terrorism and extremism community, focused on addressing the recruitment and radicalization of minors. Recognized for her international impact, she was awarded the 2025 McCain Global Leaders fellowship. X: https://x.com/_CeciliaPolizzi*

Appendix 1: Annotated Bibliography of Relevant Resources

Appendix 1: Annotated Bibliography of Relevant Resources
Over the course of the AYRM Working Group meetings, GIFCT and participants shared relevant resources to support efforts to prevent youth radicalization and counter violent extremism. This annotated bibliography shares links to resources that can be housed under four categories:

1. GIFCT Working Group resources related to AYRM themes
2. Global Network on Extremism and Technology (GNET) Insights
3. Academic research shared by AYRM Working Group participants
4. Policy documents brought forward by government representatives

GIFCT Resources

GIFCT Year 1 Working Group for Content-Sharing Algorithms and Processes and Strategic Interventions (CAPPI): Briefing on Positive Interventions
This document maps and consolidates examples of positive interventions used by industry, governments, and civil society practitioners within a theoretical framework to build greater awareness across the GIFCT multi-stakeholder community. It considers the full range of objectives, strategies, and tactics that are worthy of consideration by GIFCT members and highlights case studies of positive interventions that bring these components to life. Finally, in mapping these positive interventions, the document makes a series of multi-stakeholder recommendations for potential areas of future work.

GIFCT Year 2 Working Group for Positive Interventions and Strategic Communications: Active Strategic Communications: Measuring Impact and Audience Engagement
This report focuses its attention on the processes, practices, and challenges of designing, delivering, and measuring online positive interventions within Countering Violent Extremism (CVE) and counter-terrorism operational contexts. It examines how to move beyond traditional "vanity metrics" toward more meaningful impact metrics, exploring best practices for audience targeting and the effective use of credible messengers. Finally, by drawing lessons from the disinformation space and highlighting practitioner case studies, the report offers guidance on transforming passive counter-narratives into active strategic communications that can achieve lasting behavioral change.

GIFCT Year 3 Working Group for Blue Teaming: Alternative Platforms for Positive Intervention: Blue Teaming Playbook
This output provides a tailored set of approaches and best practices to further PVE/CVE efforts across a broader range of platforms, addressing a gap that has historically led practitioners to focus on only three to four major social media sites. It aims to help activists in their efforts to

challenge hate and extremism online and to foster broader CSO-Tech Company partnerships, examining the potential for interventions on (1) new social media platforms, (2) gaming platforms, and (3) marketplace platforms. A final chapter addresses regional and cultural considerations, examining the importance of localized partnerships in designing effective global interventions.

GIFCT Year 4 Gaming Community of Practice: Supporting Gaming Tech Safety: Prevent, Detect, and React: A Framework for Countering Violent Extremism on Gaming Surfaces

This output is a series of explanations detailing various intervention strategies for countering violent extremism on gaming surfaces, structured across three stages: Prevent, Detect, and React. Each stage outlines specific interventions that gaming platforms can implement, organized by clearly described objectives ("How") and supported by real-world examples with links to resources ("Case Studies"). It provides a comprehensive framework encompassing policy development, safety-by-design principles, detection mechanisms using both human and machine learning, and reactive measures, including user reporting systems and behavioral change initiatives.

GIFCT Member Resource Guide

This guide to GIFCT and Member Resources discusses the different ways tech companies approach and fulfill GIFCT's membership criteria and presents links to all relevant member company resources related to these criteria. This guide is designed to support tech companies, civil society groups, governments, and academic researchers interested in learning about GIFCT member company efforts to prevent terrorists and violent extremists from exploiting digital platforms.

Global Network on Extremism and Technology (GNET) Insights

The Global Network on Extremism and Technology (GNET) is GIFCT's academic research arm, based at King's College, London. GNET publishes 1500-2000-word articles (Insights) focusing on the nexus of extremism/violent extremism and technology.

All GNET Insights focusing on youth can be found here. The following Insights were discussed and/or shared during Working Group meetings:

Grooming for Violence: Similarities between Radicalisation and Grooming Processes in Gaming Spaces

Elizabeth D. Kilmer and Rachel Kowert, 2024

This Insight outlines the similarities identified by scholars between a subset of radicalization to violent extremism (RVE) processes and grooming for Child Sexual Exploitation (CSE), focusing on gaming spaces where limited moderation creates opportunities for perpetrators. The authors argue that recognizing youth groomed for violence as victims deserving support can inform more effective prevention strategies.

Youth and Adolescent Online Radicalisation: Critical Cases From Singapore

Kenneth Yeo and Ahmad Saiful Rijal, 2024

This Insight discusses the processes of online radicalization in Singapore, providing an in-depth analysis of how individuals become susceptible to Islamist and far-right extremist ideologies. The author explains that Singapore has a unique online threat landscape given its heavily multicultural society and lack of active terrorist groups, contending that countering online extremism requires offline investments in social and psychological resilience.

764: The Intersection of Terrorism, Violent Extremism, and Child Sexual Exploitation

Marc-André Argentino, Barrett G, and M.B. Tyler, 2024

This Insight draws on ongoing research into O9A and 764 to shed light on the hybridization of harms from the CSAM and TVEC fields and on how these threat actors leverage platforms and technologies to commit acts of sextortion and plan mass-casualty incidents. The authors reviewed court records, public chat logs, and social media accounts linked to members of these networks.

Extreme Right Radicalisation of Children via Online Gaming Platforms

Dr. Daniel Koehler, Irina Jugl, and Verena Fiebig, 2022

This Insight presents a summary of the authors' study, From Gaming to Hating: Extreme-Right Ideological Indoctrination and Mobilization for Violence of Children on Online Gaming Platforms. The study focuses on highlighting the radicalization pathways (and the role of gaming within them) in the anonymised police investigation files for two cases of radicalization of two twelve-year-olds.

Youth-on-Youth Extreme-Right Recruitment on Mainstream Social Media Platforms

Hannah Rose and A C, 2022

This Insight presents key findings from the longer report, "We are Generation Terror!": Youth-on-youth Radicalisation in Extreme-right Youth Groups, which explores the ways young racial nationalist groups across Western Europe recruit, radicalize, and attract other young people into their movements. The authors highlight how these groups exploit mainstream social media platforms and circumvent moderation by using backup accounts and funneling content to Telegram.

Ari's Mission: Educating Young Audiences on Conspiracy Theories Through Fictional Narratives

Linda Schlegel, 2023

This Insight discusses the theoretical foundation of modus|zad's project, "Ari's Auftrag" [Ari's Mission], a counter-narrative campaign against extremism that employs fictional narratives to raise awareness among young audiences about conspiracy theories. Drawing on narrative persuasion research, the authors argue that fictional storytelling—rarely used in P/CVE campaigns—can reduce audience reactance and
counter-arguing while retaining persuasive impact.

Misogyny and Violent Extremism: Can Big Tech Fix the Glitch?

Gazbiah Sans, 2025

This Insight examines the dynamics of Sexual and Gender-Based Violence (SGBV), Technology-Facilitated Gender Based Violence (TFGBV), and violent extremism, arguing that these intertwined phenomena share root causes in misogyny and are amplified by platform algorithms that reward engagement with polarizing content. The author offers recommendations for digital platforms to prevent harm through algorithmic fairness, content de-amplification, and proactive counter-narratives.

Persuading with Fantasy: Why Digital P/CVE Narrative Campaigns May Benefit from Fictional Elements

Linda Schlegel, 2022

This Insight explores the potential role of fictional storytelling in counter- and alternative narratives (CANs) to prevent and counter (violent) extremism (P/CVE). The author argues that fictional narratives offer P/CVE actors benefits, including greater entertainment value, creative freedom, and the ability to discuss controversial issues through psychological distance.

Creating Digital Narrative Worlds: The Promises of Transmedia Storytelling for P/CVE Narrative Campaigns

Linda Schlegel, 2022

This Insight explores the potential benefits of transmedia storytelling in counter- and alternative narrative (CAN) campaigns, noting how extremist groups coordinate complementary propaganda across multiple platforms and media formats while P/CVE efforts typically remain limited to one or two channels. The author argues that transmedia approaches could create more immersive narrative experiences, enable collaboration between projects, and support longer-term engagement.

Academic Research

Protecting Children from Online Grooming: Cross-cultural, Qualitative and Child-centred Data to Guide Grooming Prevention and Response

Ümit Kennedy, Girish Lala, Pavithra Rajan, Shima Sardarabady, Lilly Tatam, and Amanda Third, 2024

This report from Save the Children and Western Sydney University presents findings from qualitative research with 604 children aged 8-18 years across seven countries on how they experience and respond to interactions with unknown people online. The study found that children employ sophisticated strategies to assess risks but face barriers to formal reporting, and offers recommendations for updating safety education, leveraging technology, and improving cross-sector collaboration.

Community, More than Conviction: Understanding Radicalisation Factors for Young People in Australia

Kristy Campion and Emma Colvin, 2025

This study examines the radicalisation of young Australians in the New South Wales context. This study was conducted in association with the Engagement and Support Unit (ESU) within the Department of Communities and Justice in the New South Wales government. The authors suggest that it is community, more so than conviction, which influences the engagement of young Australians with extremism.

Telling tales against the dark arts: How fictional storytelling could support narrative campaigns against extremism

Linda Schlegel, 2021

This Peace Research Institute Frankfurt (PRIF) blog post assesses the potential uses of fictional storytelling in P/CVE counter-narrative campaigns, noting that despite ample evidence of fiction's persuasive power, current efforts rely almost exclusively on realistic stories. The author argues that fictional narratives offer benefits, including reduced demands for realism, the ability to exaggerate issues without backlash, and flexibility around credible messengers.

Missing an epic story: Why we are struggling to counter extremists' utopian narratives

Linda Schlegel, 2021

This blog post by the Peace Research Institute Frankfurt (PRIF) assesses and identifies gaps in existing counter-narrative campaigns, arguing that while extremist propaganda relies heavily on utopian visions of a perfect society, pro-democracy narratives lack equivalent prognostic elements. The author contends that without grand visions of social progress to offer, alternative narrative campaigns can only partially counter what makes extremist ideologies appealing.

Effective Narratives: Updating the GAMMMA+ model

Alexander Ritzmann, Lieke Wouterse, and Merle Verdegaal, 2019

This paper updates the GAMMMA+ model, a practical guideline promoted by the RAN Communication and Narratives working group since 2017 for conducting effective alternative and counter-narrative (AN/CN) campaigns against extremism. Based on two years of practitioner feedback, the authors add a Theory of Change component and emphasize in-depth audience understanding, credible messengers, and robust monitoring and evaluation frameworks.

The Science of Storytelling: Why Stories Make Us Human, and How To Tell Them Better

Will Storr, 2020

This book draws on psychology and neuroscience to explore how the brain responds to storytelling, what makes narratives compelling, and how storytellers influence, manipulate, and persuade readers. Storr argues that flawed characters are central to effective storytelling and offers practical guidance for writers seeking to craft more engaging stories.

Storytelling Against Extremism: Advancing Theory and Practice of Digital Narrative Campaigns against Extremism

Linda Schlegel, 2025

Counter- and alternative narrative (CAN) campaigns have become a widely used tool in contemporary efforts to prevent and/or counter (violent) extremism (P/CVE). However, neither CAN theory nor practice is grounded in existing research on narrative persuasion processes. Not situating CANs within the broader discourse on narrative persuasion and drawing from the insights narrative persuasion studies offer significantly weakens the theoretical foundation, practical development, storytelling quality, and analysis of CAN campaigns. This book addresses this research gap and transfers concepts, theories, and insights from narrative persuasion and storytelling research to the context of P/CVE narrative campaigns.

Storytelling against extremism. How fiction could increase the persuasive impact of counter- and alternative narratives in P/CVE

Linda Schlegel, 2021

The past decade has seen an increase in research on narratives in extremist communication and their role in radicalization processes, as well as on both counter-and alternative narratives as tools to prevent or counter radicalization processes. Conspicuously absent from the P/CVE literature so far, however, is a discussion on fictional narratives and the potential of stories not based on “realistic” presentations of life. This article is an exploratory contribution to the discourse, suggesting that fictional narratives, low in external realism but eliciting high levels of transportation and identification in audiences, may be helpful tools for P/CVE campaigns built on narratives and storytelling.

Policy Documents

UK Office for Communications' (OfCom) new Protection of Children Codes
Under the UK Online Safety Act, services likely to be accessed by children have a duty to protect children online. From 25 July 2025, providers will need to take the safety measures set out in the Codes of Practice, or use other effective measures, to protect child users from harmful content. This page gives a quick introduction to the safety measures recommended in the Protection of Children Codes.

EU Commission: RAN C&N Digital Grooming Tactics on Video Gaming & Video Gaming Adjacent Platforms: Threats and Opportunities, 15-16 March 2021
This paper first discusses threats posed by grooming tactics in video gaming and on adjacent platforms, providing background on the grooming models discussed during the meeting. The second part of the paper highlights recommendations for using positive, empowering ways to prevent and counter grooming through video gaming.

Appendix 2: GIFCT Year 5 Working Group Participant Affiliations[5]

Academia	Advocacy	Practitioner & Researcher	Government & Intergovernmental	Tech
Center for Cyber Strategy and Policy, University of Cincinnati	All Tech Is Human	ATCO	African Union Commission	Airbnb
Centre for Human Rights, University of Pretoria	Dignity in Difference	Centinel	African Union Counter Terrorism Centre	Anthropic
Centre for Land Warfare Studies, New Delhi	Global Center on Cooperative Security	Centre for Action and Prevention against Radicalization of Individuals	AI Security Institute, United Kingdom	Bitly
Georgia State University	Life After Hate	Centre for Trustworthy Technology	Birmingham City Council, United Kingdom	Clubhouse
Indonesia International Islamic University	Local Youth Corner Cameroon	Christchurch Call	Civipol, France	Dailymotion
International Policing and Public Protection Research Institute, Anglia Ruskin University	Middle East Institute	Control Risks	Classification Office, New Zealand	Discord
Istanbul University	Next Wave, The International Center for Children and Global Security	Diálogo Americas	Counter Terrorism Department, Pakistan	Dropbox
Leiden University	Parents for Peace	Digital Catapult	Counter-Terrorism Committee, United Nations	Giphy
Northwestern University	Republican Public Association	Extremism and Gaming Research Network	Department of Communities and Justice, Australia	Google
Oxford Internet Institute		FBI National Citizens Academy Alumni Association	Department of Health, Australia	Linkedin
Royal Holloway, University of London		InfraGard	Department of Home Affairs, Australia	Meta
Said Business School		Global Community Engagement and Resilience Fund	Department of Internal Affairs, New Zealand	Microsoft
Sapienza University of Rome		Hedayah	Department of State, United States of America	Nexi Group

[5] This table highlights participants across all Year 5 Working Groups.

Strathmore University		Infobae	eSafety Commissioner, Australia	Pan Africa Gaming Group
Swansea University		Institute for Security Studies Africa	European Commission	Patreon
Universidad Anahuac		Institute for Security Studies	European External Action Service	Pinterest
University at Albany, State University of New York		Institute for Strategic Dialogue	Federal Ministry of the Interior, Germany	Somtel
University of Auckland		Irregular Warfare Initiative	Global Initiative on Electronic Evidence, United Nations	Streamable
University of Bristol		Jihadoscope	Hellenic Police, Greece	TikTok
University of Cambridge		Moonshot	Home Office, United Kingdom	Twitch
University of Muenster		Mythos Labs	Interministerial Committee for the Prevention of Crime and Radicalisation, France	Vimeo
University of Oxford		Online Safety Exchange	Ministry of Foreign Affairs	X
		Peace Research Institute Frankfurt	National Counter Terrorism Agency, Indonesia	Yahoo
		PVE Works	National Counter Terrorism Fusion Centre, Ministry of National Security, Ghana	Yubo
		Refslund Analytics	National Counterterrorism Center, Office of the Director of National Intelligence, United States of America	
		Tiaki Akoako	National Defence University, Pakistan	
		Uppsala Conflict Data Programme	Ofcom, United Kingdom	
		VoxPol Institute	Organization for Security and Co-operation in Europe	
		International Development Research Center	Public Safety Canada	
			Strong Cities Network	
			United Nations Counter-Terrorism Committee Executive Directorate	
			United Nations Interregional Crime and Justice Research Institute	
			United Nations Office of Counter-Terrorism	
			United Nations Office on Drugs and Crime	

Recommended citation: GIFCT Artificial Intelligence Working Group Report: AI Threats and Opportunities. Washington, D.C.: Global Internet Forum to Counter Terrorism, 2025.

GIFCT is a 501(c)(3) non-profit organization and tech-led initiative with over 35 member tech companies offering unique settings for diverse stakeholders to identify and solve the most complex global challenges at the intersection of terrorism and technology. GIFCT's mission is to prevent terrorists and violent extremists (TVE) from exploiting digital platforms. In every aspect of our work, we aim to be transparent, inclusive, and respectful of the fundamental and universal human rights that TVE seek to undermine.

www.gifct.org ✉ outreach@gifct.org