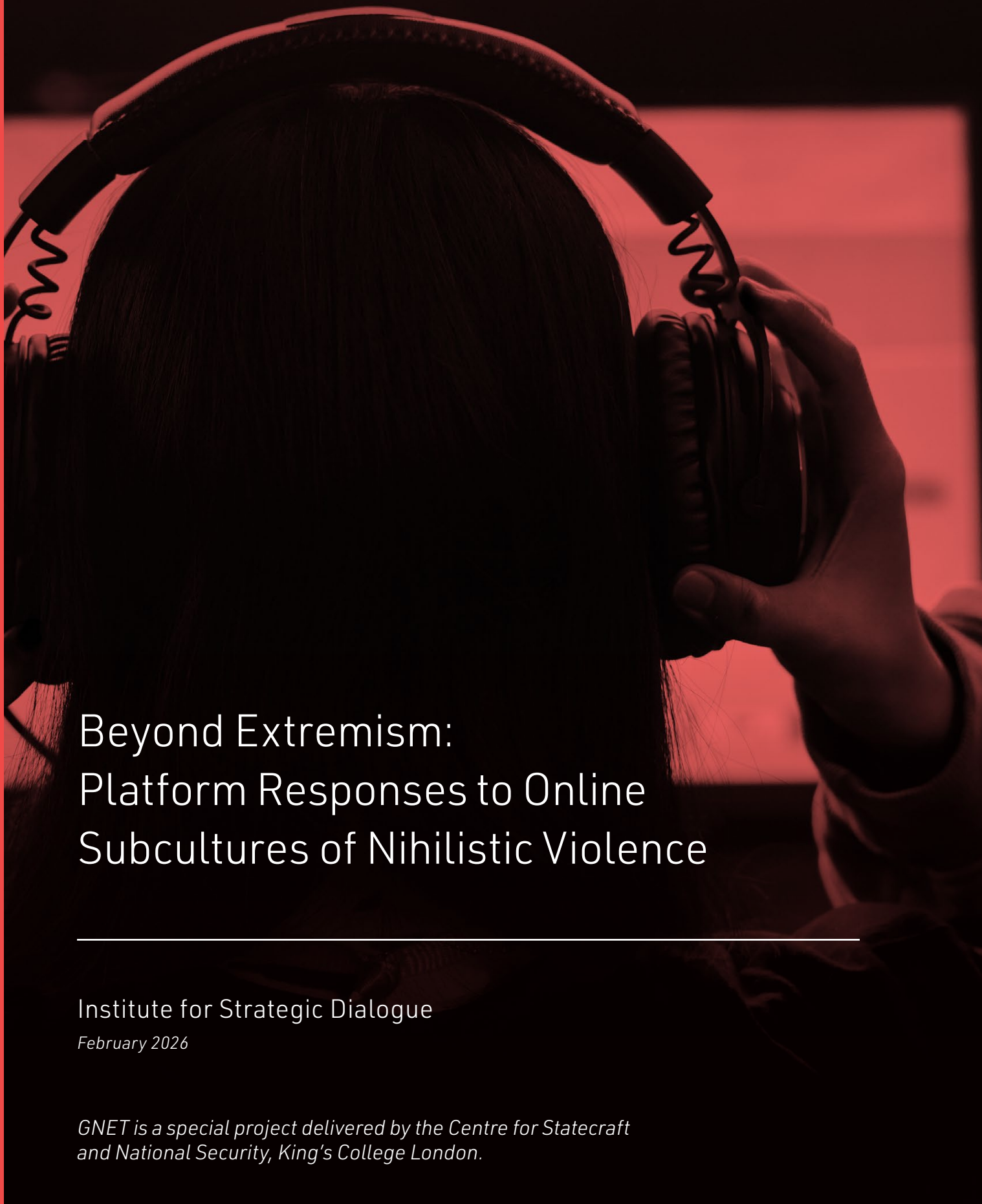
ISD | Institute for Strategic Dialogue

GIFCT | Global Internet Forum to Counter Terrorism

Global Network on Extremism & Technology



Beyond Extremism: Platform Responses to Online Subcultures of Nihilistic Violence

Institute for Strategic Dialogue

February 2026

GNET is a special project delivered by the Centre for Statecraft and National Security, King's College London.

This report was authored by the Institute for Strategic Dialogue.

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the Centre for Statecraft and National Security (CSNS), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET, CSNS or King's College London.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

Global Network on Extremism and Technology (GNET)
Centre for Statecraft and National Security (CSNS)
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**
W. **www.gnet-research.org**

Institute for Strategic Dialogue (ISD)
T: **+44 20 7493 9333**
E: **info@isdglobal.org**
W: **www.isdglobal.org**

Global Internet Forum to Counter Terrorism (GIFCT)
E: **outreach@gifct.org**
W: **www.gifct.org**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Recommended citation:
Institute for Strategic Dialogue, "Beyond Extremism: Platform Responses to Online Subcultures of Nihilistic Violence". London: Global Network on Extremism and Technology (GNET), February 2026. https://doi.org/10.18742/pub01-244.

Key Findings

- While occupying parallel digital spaces and producing similar types of harm, online **subcultures of nihilistic violence are distinct from ideologically motivated extremism**. This unique threat requires bespoke platform interventions rather than expansions and adaptations of existing terrorism- and violent extremism-focused frameworks.

- Nihilistic violence ecosystems are **decentralised, cross-platform and highly agile**, leveraging mainstream and fringe platforms for grooming, propaganda and operational coordination. Platform strategies should not look to respond to the threat as new forms of dangerous organisations, but rather to understand this phenomenon as a more **dynamic threat from nihilistic violent subcultures**, of which 'groups' like 764 and the True Crime Community are just the latest manifestation.

- Nihilistic violent communities produce a much broader range of harms than ideologically motivated extremist networks, spanning sexual exploitation, cybercrime and various forms of real-world targeted violence, including self-harm, animal abuse, interpersonal violence and mass casualty attacks such as school shootings.

- New platform policies are not necessarily required to mitigate the threat, given that many of these harms are already covered in platform community guidelines. However, these should be knitted together as part of a cohesive platform strategy, as enforcement against ecosystems of nihilistic violence is currently fragmented and reactive, enabling ban evasion and rapid regrouping.

Key Recommendations

- **Adopt an ideology-agnostic, behavioural approach to threat assessment**: Shift from group-focused frameworks to models addressing behavioural indicators, pro-violence content, aesthetics and more diverse harm matrices.
- **Implement a spectrum of platform violence-prevention interventions, informed by a public health approach**: Focus on upstream prevention. Early intervention should seek to build resilience through education and employ inoculation approaches.
    - **Enhance platform-level safeguards**: Consider opportunities for impactful platform-facilitated safety interventions – such as providing expert resources and developing community education campaigns around evolving nihilistic violence threats.
    - **Empower community-level interventions**: Equip moderators in fandom-driven spaces with bystander intervention tools and off-ramping resources.
    - **Build bridges to support services**: Provide a wider range of safeguarding support within relevant communities and ensure relevance to specific subcultures.
    - **Innovate counter-communications**: Use authentic, grassroots content that engages subcultural humour and aesthetics, while avoiding ideological deradicalisation messaging ill-suited to this threat.
    - **Develop dynamic ecosystem disruption strategies**: Coordinate cross-platform takedowns informed by intelligence-led mapping, leveraging GIFCT-style collaborative frameworks for wholesale network disruption.
- **Strengthen moderation and enforcement**: Integrate ban-evasion markers and regrouping codes into moderation practices and consider IP/device fingerprinting to address the proliferation of burner account activity within these communities.
- **Invest in research and cross-sector collaboration**: Establish an information-sharing hub to track evolving codes, platform usage and threat dynamics. As part of this, provide researchers with meaningful access to platform data to enable a joined-up, sectoral approach to this rapidly evolving threat.

Editorial Note

In February 2025, the Global Internet Forum to Counter Terrorism (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, Working Groups contribute to growing GIFCT's 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. Working Group outputs are produced by independent experts and do not necessarily represent the views of GIFCT, its members or the GIFCT Operating Board.

The proposal for this Institute for Strategic Dialogue (ISD) paper came to Global Network on Extremism and Technology (GNET) from GIFCT's 2025 Working Group, Addressing Youth Radicalisation and Mobilisation, which worked to identify current trends in youth radicalisation and mobilisation online, alongside lessons learned from prevention and positive intervention strategies, to address these dynamics.

Through multi-stakeholder discussion, the group highlighted best practices while connecting industry, practitioners and experts to enhance cross-sector efforts. 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 radicalisation involving harmful online communities with less clear ideological frameworks, and/or involving convergences of multiple harm types.

Contents

1 Introduction

Subcultures of nihilistic violence have emerged as a central threat, targeting and manipulating young people online. ISD defines nihilistic violence as violent acts lacking an ideological motivation and driven by a misanthropic worldview.[1] These communities form a decentralised web of chats, forums and channels characterised by support for violence for violence's sake, but with no specific political, ideological or religious goal.

Their tactics and resultant harms often mirror those of ideologically motivated extremist networks (such as an increasing number of community-linked mass casualty attacks), and there is some overlap between the two phenomena's digital ecosystems, activities and cultural references. But the lack of ideology associated with subcultures of nihilistic violence is vital when assessing opportunities for intervention and prevention. Replicating strategies developed over the last two decades to deal with ideologically motivated threats will fail to disrupt a fundamentally nihilistic network.

Rather than inappropriately bolting policies and interventions to counter nihilistic violence on to existing approaches to tackling terrorist and violent extremist content, a more bespoke approach is required, rooted in a greater understanding of specific behaviours and harms. In particular, due to the extreme vulnerability of many participants in online nihilistic subcultures – many of whom are both victims and perpetrators – counter-measures must place particular emphasis on safeguarding and child protection.

This policy paper provides an overview of the specific online threat landscape of nihilistic violence subcultures, and outlines the implications for platform measures to protect users. The first section sets out the networks that comprise the ecosystem, the ways in which they use platform functions to conduct harmful activities, and a taxonomy of resulting harms. The second section of this report considers how existing platform terms of service relate to these different harms. The third section offers an overview of intervention opportunities for platforms and considers additional innovative approaches to ecosystem disruption.

1 "Terror without Ideology? The Rise of Nihilistic Violence – An ISD Investigation," *Institute for Strategic Dialogue*, May 8, 2025, https://www.isdglobal.org/digital_dispatches/terror-without-ideology-the-rise-of-nihilistic-violence-an-isd-investigation/.

2 The Online Landscape of Subcultures of Nihilistic Violence

Online subcultures of nihilistic violence comprise loosely connected webs of different networks, communities and individuals.

The **Com** network is a set of decentralised online ecosystems which encourage and engage in cyber crime, extortion and swatting, and increasingly, acts of violence.[2] The Com often targets vulnerable children and young people, coercing victims to conduct self-harm, serious violence and other forms of extreme criminality.

Some elements of nihilistic violence subcultures are more formally organised. **764** is an organised network of online groups that engage in sextortion and violence glorification. Emerging from the Com network in 2021, it comprises a constantly shifting set of chats, groups and forums across multiple platforms. Some groups remain focused on coercing minors to produce child sexual abuse material (CSAM) and self-harm content. However, ISD analysts assess that following three European stabbing sprees carried out by the 764-affiliated group No Lives Matter, prominent 764 affiliates are increasingly mobilising users towards real-world violence, with four recent mass-violence plots and attacks across the US.[3] 764 is active globally; from 2020–2025, more than 200 individuals were arrested in 28 different countries for sextortion, CSAM possession or violence linked to the network.[4]

True Crime Community (TCC) is a loosely connected online fandom which venerates mass violence and its perpetrators regardless of ideology. Its users memorialise and lionise serial killers, terrorists and mass murderers, encouraging others to conduct similar acts of violence. TCC does overlap with adjacent ecosystems such as gore communities[5] and extreme-right Saints Culture aesthetics,[6] but is motivated by misanthropy and violence fixation rather than supremacist worldviews. ISD has assessed that TCC is a central driver of violence across nihilistic networks, with analysts identifying at least 15 school shooting attacks or disputed plots linked to TCC since January 2024, including high-profile attacks in Minneapolis, Minnesota and Graz, Austria.[7] TCC is active across a range of platforms, including Tumblr, TikTok, Discord and Telegram.

---

2 Federal Bureau of Investigation, "Hacker Com: Cyber Criminal Subset of The Community (Com) Is a Rising Threat to Youth Online," *Public Service Announcement,* July 23, 2025, https://www.ic3.gov/PSA/2025/PSA250723.

3 "From Sextortion to Violence: The Evolving Threat of the 764 Network in the US," *Institute for Strategic Dialogue*, November 12, 2025, https://www.isdglobal.org/digital_dispatches/from-sextortion-to-violence-the-evolving-threat-of-the-764-network-in-the-us/.

4 Marc-André Argentino, "Beyond the Headlines: Arrest Data and Drivers of Nihilistic Violent Extremism in the Com Network," *From the Depths*, September 18, 2025, https://www.maargentino.com/beyond-the-headlines-arrest-data-and-drivers-of-nihilistic-violent-extremism-in-the-com-network/.

5 Human Digital, Ali Fisher, and Arthur Bradley, *Gore and Violent Extremism: An Explorative Analysis of the Use of Gore Websites for Hosting and Sharing Extremist and Terrorist Content* (VOX-Pol, 2025), https://voxpol.eu/wp-content/uploads/2025/07/DCUPN0751-Gore-Extremism-WEB-250704.pdf.

6 Zoe Manzi, "'Saints Culture'," Institute for Strategic Dialogue, https://www.isdglobal.org/explainers/saints-culture/.

7 "Memetic Violence: How the True Crime Community Generates Its Own Killers," *Institute for Strategic Dialogue*, October 2, 2025, https://www.isdglobal.org/digital_dispatches/memetic-violence-how-the-true-crime-community-generates-its-own-killers/.

Beyond these more coordinated or community-focused elements of online nihilistic violence, there exists a diffuse web of individuals with a nexus to communities that glorify and aestheticise violence. Axel Rudakubana, who killed three young girls at a Southport dance class in July 2024, was obsessed with violence both online and offline.[8] For example, he was fascinated by genocide and consumed gore content, including footage from the stabbing of a bishop in a Sydney church, before committing his own attack.[9] Two young people have subsequently been arrested in separate cases of allegedly planning to emulate Rudakubana, including planning an attack at a similar dance class and mirroring his aesthetic by wearing a similar green hoodie.[10] Their activities demonstrate a spectrum of influence from such subcultures of nihilistic violence, with some violence more community-driven and others individualised. This shows the need for responses to focus on specific harmful behaviours rather than identify violent 'groups'.

Worldviews and Narrative Strategies

Unlike extremist narratives that are rooted in supremacist worldviews, subcultures of nihilistic violence promote the use of violence to fulfil a fundamentally misanthropic end or to gain status within a community.[11] However, while united by this shared 'goal', different online subcultures have distinct narrative patterns. The 764 network and TCC are the most well-defined subcultures of nihilistic violence but display polar-opposite narrative strategies.

The Com network and its constituent nihilistic communities advocate for acts of cruelty, violence and depravity for their own sake, rather than in the service of any coherent ideological or moral objective.[12] In contrast to conventional extremist movements, the aim of these networks is to be provocative rather than to achieve a political goal. They intentionally engage in depraved acts and behaviours to attract attention, notoriety and online clout, rather than to pursue a perceived moral good.

When these networks do promote certain narratives that could be construed as ideological, they are often retrofitted to rationalise their acts of violence and cruelty. However, these narratives may not be genuine drivers of behaviour as ideological discussion in private spaces and group chats is extremely sparse. Narratives espoused by these groups – typically through their manifestoes and publications – centre around themes of misanthropy and hatred for the world, the pursuit of evil as a path towards a 'pure' social order (in what is often a nod to themes contained in Order of Nine Angles literature),[13] and indiscriminate annihilation and destruction as ends in themselves.

8 "Failing to Prevent: Lessons from the Southport Tragedy," *Institute for Strategic Dialogue*, January 25, 2025, https://www.isdglobal.org/digital_dispatches/failing-to-prevent-lessons-from-the-southport-tragedy/.
9 Daniel Sandford, Kathryn Armstrong, and Ian Aikman, "Father Stopped Southport Killer from Going to Former School a Week before Attack," *BBC News*, January 20, 2025, https://www.bbc.co.uk/news/articles/cqx949jzjlyo.
10 Duncan Gardham, "Two Teenagers Who Allegedly Wanted to Emulate Southport Killer Have Been Arrested," *Sky News*, November 10, 2025, https://news.sky.com/story/two-teenagers-who-allegedly-wanted-to-emulate-southport-killer-have-been-arrested-13468022.
11 "Terror without Ideology?"
12 "Terror without Ideology?"
13 Patrik Hermansson, "State of Hate 2025: The Online Exploitation Cult Grooming Teenagers to Violence," *Hope Not Hate*, 2025, https://hopenothate.org.uk/state-of-hate-2025-764/.

The expression 'No Lives Matter' is both the name of a constituent group within the Com network and a mantra meant to communicate the ethos of its adherents.[14] The expression suggests a sense of nihilism and the rejection of conventional morality. However, these narratives should not be taken at face value, as they are just as likely integrated into their propaganda for branding purposes than as a reflection of a genuine worldview.

The 764 network's propaganda features overt calls for violence, and individual groups require prospective members to carry out acts of violence, property destruction or extortion to join. Members who have carried out attacks are glorified in stylised graphics and videos which make up an important part of the network's mythos and culture, and many members include calls to free their imprisoned comrades in their social media biographies. Even the usernames of many 764 members explicitly reflect specific forms of extreme violence.

Conversely, those affiliated with TCC (often referred to as TCCers or TCC fans) rarely, if ever, directly encourage the use of violence. TCC is best understood as a fandom: it lacks the structured hierarchy of the 764 network and has no unified messaging strategy. However, TCCers produce a large volume of content which either explicitly or implicitly glorifies the use of violence and has the potential to mobilise others to violence. This often takes the form of fan fiction, art or writing, featuring extensive research into mass killers – including terrorists – as part of a celebration of any form of mass violence regardless of target.

Despite the diverse worldviews which exist across the network, the common thread of behaviour which glorifies and encourages violence should form the basis of platform-enforcement approaches. The complex web of narrative strategies across the network demands a more agile approach to moderation; one that is able to quickly adapt to rapidly evolving network dynamics, violent reference points and coded language.

Aesthetics

Broader nihilistic violence communities can be identified primarily by behaviours and aesthetics, rather than through the promotion of specific narratives that can be tracked and mitigated. Aesthetics, in-group language and memes are important cultural touchpoints for subcultures of nihilistic violence, with users promoting transgressive or extremist iconography from across the ideological spectrum, such as swastikas, symbols associated with the Order of Nine Angles and Tempel ov Blood, and imagery referencing serial killers and sadistic rapists. This imagery is typically used to form a hyperviolent and unsettling stereotypically 'evil' aesthetic rather than to communicate genuine ideological beliefs. Importantly, this does not mean that individual members of these networks lack ideological beliefs, but that ideology is not an overarching motive for the network as a whole.

TCC narratives are much more focused on the aesthetics and the personal struggles of mass killers. Dylan Roof – who killed nine people in a 2015 attack on a Black church – is a popular figure

14 Ali Winston, "The Violent Rise of 'No Lives Matter'," *Wired*, March 12, 2025, https://www.wired.com/story/no-lives-matter-764-violence/.

within the community, yet conversations and narratives about him more commonly highlight aesthetic features such as his haircut than sympathise with or justify his neo-Nazi worldview.

The experience of engaging with TCC narratives is often deeply emotional for online users. In some cases, individuals will form parasocial relationships with deceased or imprisoned mass killers and paint them in a highly sympathetic light. For example, an early debate among Columbiners (a subset of TCC entirely focused on the Columbine attackers) was known as "15 not 13". In the debate, users discussed whether only the 13 people who died in the attack were the victims, or whether the shooters Eric Harris and Dylan Klebold should also be considered victims of the shooting. A significant number of community members identify themselves as non-condoning of violence, using the label "Does Not Condone (DNC)" on their profiles. These users claim that they do not glorify the killers; however, they still play a role in enabling violence, producing content and research that drive TCC discussions.

The strong emphasis on aesthetics across subcultures of nihilistic violence demands a much more nuanced approach to identification and moderation. Keyword-based moderation will struggle to identify and respond to the aesthetics of violence, which include inferred meanings and multi-modal content. Rather than simply identifying specific symbols – such as runes or logos – associated with listed groups, moderation approaches must integrate a more holistic understanding of the overarching aesthetics which provide a common visual frame, binding together nihilistic violent communities online.

Platform Usage and Strategies

ISD's ethnographic monitoring of nihilistic violence communities has shown how different networks leverage distinct platforms for varied purposes.[15] The Com network, and in particular its sextortion elements, operates across a broad swathe of social media platforms and online games, tailoring its usage to the specific functionality, user dynamics and social architecture of each platform. Generally, the network uses large, mainstream social networking platforms such as X and Reddit to identify targets for grooming and exploitation, casting a wide net for potentially vulnerable users with whom they can initiate contact. Members of sextortion networks regularly canvas these large online ecosystems using targeted profile and hashtag searches to identify suitable candidates for victimisation.

After establishing initial contact, extorters often attempt to move their interactions to more niche platforms that are conducive to secure one-on-one messaging, such as Discord and Telegram, where they engage in grooming, exploitation and extortion. Analysts have identified that, among members of sextortion communities, Telegram is the most important platform for coordinating activities and exchanging sexploitation material. However, analysts' ethnographic monitoring shows how Discord stands apart from other platforms given its multipurpose nature, which includes serving as an environment where members of the network can identify potential victims, groom them and ultimately broadcast their abuse.

15 "Networks of Harm: A Victim-Centric Information Resource on the 764 Sextortion Network," *Institute for Strategic Dialogue*, November 6, 2025, https://www.isdglobal.org/isd-publications/networks-of-harm-a-victim-centric-information-resource-on-the-764-sextortion-network/.

Beyond these more functional layers, the 764 network also uses platforms for aesthetic purposes, branding and cultural signaling. Platforms can be mainstream, such as TikTok, or more niche environments like SoundCloud and specific message boards. By establishing a distinguished aesthetic and distributing its propaganda across these spaces, the 764 network entrenches its group identity and attracts new recruits who may be drawn to its extreme aesthetics.

Of note, the 764 network does not treat any particular platform as a rigid, single-purpose environment. Members of these networks constantly adjust their use of various platforms according to their specific needs at the time (such as identifying victims, grooming and exploiting them, broadcasting their abuse or disseminating propaganda). However, this dynamic is often fluid. For example, although Roblox is primarily used to identify potential victims due to its young user base, the platform has also been used for grooming purposes and to engage in sexual roleplay.

Overall, members of sextortion networks take a layered, cross-platform approach to their online operations – large social media platforms are used as hunting grounds, private messaging applications are used for grooming and control, and more niche platforms are used for branding and propaganda. This enables the network to evade platform-specific moderation efforts and to move freely between various online environments to perpetrate a variety of harms.

TCC users can be found on nearly every mainstream social media platform; however, they are most prominent on Tumblr, TikTok, Discord, Telegram and Pinterest.[16] Tumblr is the main platform for TCC narratives and the short-form writing features of the platform lend themselves well to the research and engagement users desire. Similarly, the features of TikTok and Pinterest are leveraged to share and discuss TCC media.

Ban Evasion Methodologies

Some areas of nihilistic communities have developed particular resilience to moderation practices. The 764 network uses a variety of operational security techniques to evade both platform moderation and law enforcement scrutiny. Notably, some members maintain a rigorous identity management regimen comprising the creation of dozens if not hundreds of sockpuppet (fake online identity) email addresses, burner phone numbers and social media profiles. Many community members are disciplined in employing this identity management routine, making attribution of their activities difficult. Responding to platform detection and moderation, such individuals are able to easily re-establish their presence using backup accounts. Members may also rapidly delete accounts and switch their monikers across platforms, which further challenges detection and enforcement.

Beyond the operational security of individual users, the network as a whole also employs numerous techniques to avoid coordinated moderation. For example, sextortion-related group chats may include rules and guidelines which claim to prohibit extreme material such as CSAM, gore or animal abuse material. However, such guidelines appear to be largely superficial, with violative content going unmoderated within the chats themselves.

16 “Memetic Violence”.

Techniques can also be more sophisticated – for example, these networks use a nested structure in which access to sensitive discussions is heavily gated, often requiring members to demonstrate their loyalty by engaging in depraved acts of violence and cruelty before gaining access.[17] Furthermore, these networks often set up backup channels or group chats so that if their core channels are disrupted, they can regroup and plan their next steps. This bolsters the resilience of the network in the event of a platform takedown or arrest.

A Taxonomy of Harms

Given that their harmful activity is much diverse than that of violent extremists, figure 1 visualises a taxonomy of harms most commonly linked to online subcultures of nihilistic violence. These harms broadly fall into three categories and are defined as such by the Com network itself: sexual harms, cyber harms and real-world violence. Cutting across these tangible harm areas are the psychological impacts on victims, broader processes of radicalisation and desensitisation to violence.

In nihilistic violence subcultures such as those within the Com network, there are blurred boundaries between victim and perpetrator. Young people may conduct severely harmful acts as a result of coercion or grooming. Harms are therefore often conducted by dual victim/perpetrators, and the taxonomy below provides an overview of both harms carried out by victims of the network and those carried out by its members.

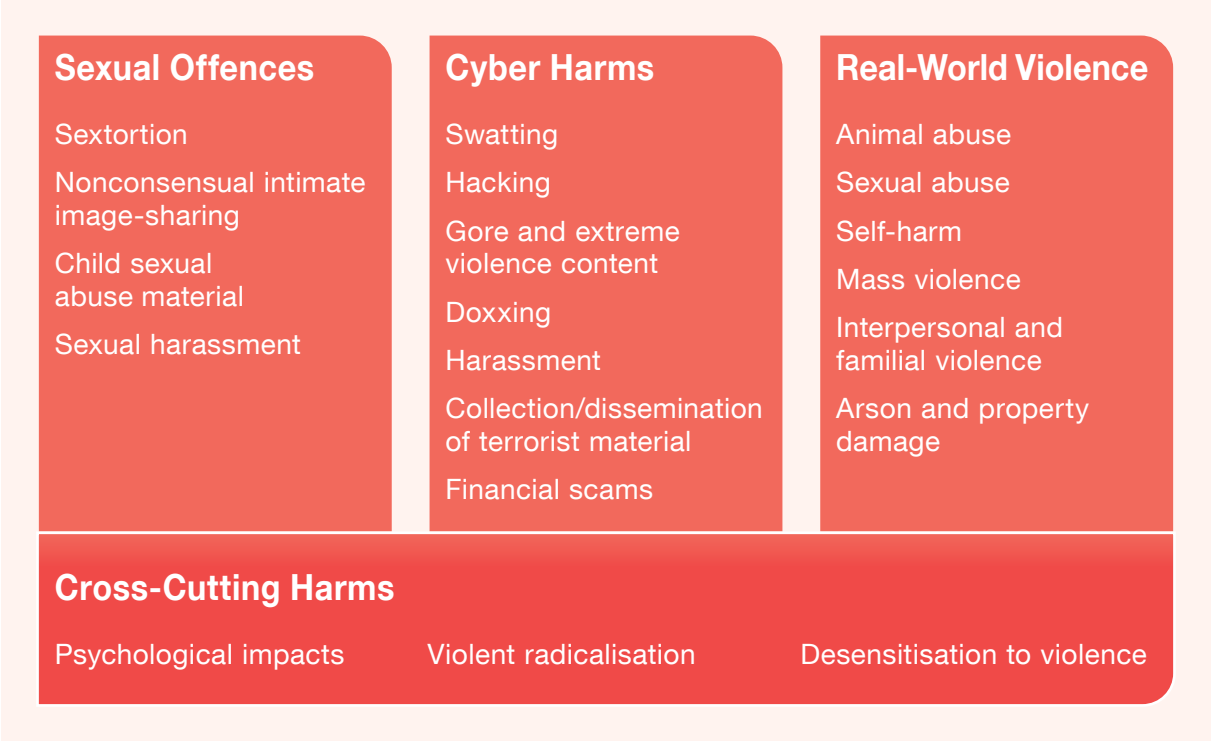


Figure 1: A taxonomy of harms associated with subcultures of nihilistic violence

17 Marc-André Argentino, "Blood, Betrayal, and Branding: Inside 764's Hierarchy of Horrors," *From the Depths*, March 7, 2025, https://www.maargentino.com/blood-betrayal-and-branding-inside-764s-hierarchy-of-horrors/.

3 Existing Policy Frameworks

Platforms typically have provisions within their community guidelines to address violent extremism and terrorism. However, these policies often focus either on terrorist groups as a means of identifying and banning content, or on violence or hate speech directed towards groups or individuals with protected characteristics.

Subcultures of nihilistic violence fall under neither category, given their loose structures and broad misanthropic views with no specified ideology or target group. As identified in the harms taxonomy above, these subcultures incite and produce much wider forms of harm than the mere promotion of targeted hate and violence. To investigate how current policy approaches map on to nihilistic violence, this section maps the harms taxonomy to policy frameworks of platforms identified by analysts as particularly relevant to subcultures of nihilistic violence.

Sexual Offences

Across the majority of studied platforms, sexual offences are largely covered in community guidelines. Relevant policies tend to be explicit in their identification of sexual harms, with dedicated policy areas for both minors and adults. CSAM is universally banned under platform community guidelines. There is strong awareness of the harms of nonconsensual, intimate image-sharing, which is prohibited among the majority of platforms. Sextortion is not always explicitly named but typically falls under broader sexual exploitation or harassment policies.

Cyber Harms

There is a more mixed picture of platform coverage of cyber-related harms most commonly associated with communities of nihilistic violence. More traditional and common forms of harm such as financial scams and harassment of individuals tend to be more comprehensively addressed in platforms' community guidelines. Collection and dissemination of terrorist materials is aptly covered under either violence or terrorist organisation provisions, even when the disseminator is not associated with a group.

Several emergent harm areas are less consistently captured. There was coverage of doxxing harms among larger platforms. Doxxing might also be captured through other policies against the nonconsensual sharing of personal information. However, most platforms showed prohibited gore and extreme violence. Most platforms' community guidelines made no mention of swatting, although this may be less relevant to the functionality of some platforms.

	X	Instagram	TikTok	Reddit	Tumblr	Roblox	Discord	Snapchat	SoundCloud	Telegram
Sextortion	Yes – under child and adult exploitation policies	Yes – under child and adult exploitation policies	Yes – under child and adult exploitation policies	No	No	Yes – under child sexual extortion policy	Partially – only when related to harassment	Yes – under sexual content policy	Yes – under child safety and sexual exploitation policies	No
Nonconsensual intimate image sharing	Yes – under non-consensual nudity policy	Yes – under child and adult exploitation policies	Yes – under child and adult exploitation policies	Yes	Yes	No – not explicitly mentioned	Yes	Yes – under sexual content policy	Yes – under sexual exploitation	Partially – under illegal pornographic content
CSAM	Yes – under child safety	Yes	Yes	Yes	Yes – under harm to minors	Yes – under child exploitation policy	Yes	Yes – under sexual content policy	Yes – under child safety and sexual exploitation policies	Yes
Sexual harassment	Yes – under abuse and harassment	Yes	Yes – under harassment and bullying	Yes	Yes – under harassment	Yes	Yes	Yes – under sexual content policy	Yes – under sexual exploitation	Not explicitly mentioned and unlikely to fall under illegal activities

Table 1: Sexual offences mapped across the community guidelines of platforms relevant to nihilistic violence (as of November 2025)

	X	Instagram	TikTok	Reddit	Tumblr	Roblox	Discord	Snapchat	SoundCloud	Telegram
Swatting	Not explicitly	Yes – under coordinating harm and promoting crime	Not explicitly	No	May apply under unlawful uses or content	Not explicitly but could fall under illegal and regulated goods and activities	Not explicitly mentioned	Not explicitly mentioned but may fall under illegal or regulated activities	Not explicitly mentioned but could fall under illegal content	Not explicitly, but included where illegal
Hacking	Partially – under authenticity	Yes – under cybersecurity	Yes – under platform security	Not explicitly but may apply under rule to not break the site	May fall under disruptions, exploits or resource abuse	Yes – under cheating and scams	Partially – In reference to IP	No	Somewhat – Terms of Use prohibit unauthorised account use	Not explicitly, but included where illegal
Gore/ extreme violence	Yes – under violent content	Yes – under violent and graphic content	Yes – under shocking and graphic content	No	Yes – under violent content and threats, gore and mutilation	Yes	Yes	No	Yes	No
Doxxing	Yes – under private content	Yes – under coordinating harm and promoting crime	Yes – under harassment and bullying	Yes	Yes	Partially – under sharing personal information	Yes	Yes	Yes	Not explicitly, but included where illegal
Harassment	Yes	Yes	Yes – under harassment and bullying	Yes – harassment policies	Yes – harassment policy	Yes – including off-platform behaviour	Yes – harassment policy	Yes – harassment policy	Yes – harassment policy	Not explicitly, but included where illegal
Collection or dissemination of terrorist materials	Somewhat – across a. violent and hatefully entities policy and b. perpetrators of violent attacks	Somewhat – when linked to a dangerous organisation	Yes – under violent and hateful organisations and individuals	No	Yes – terrorism	Yes – under terrorism and violent extremism	Yes – under violent extremism	Yes – under hateful content, terrorism and violent extremism	Yes – with specific reference to dissemination	Not explicitly, but included where illegal
Financial scams	Yes – under authenticity	Yes – under fraud, scams and deceptive practices	Yes – under fraud and scams	Yes	Not specifically but may be covered by deceptive or fraudulent links	Partially – could fall under cheating and scams	Yes	Yes	Yes – under fraud and scams and criminal property	Yes

Table 2: Cyber harms mapped across the community guidelines of platforms relevant to nihilistic violence (as of November 2025)

	X	Instagram	TikTok	Reddit	Tumblr	Roblox	Discord	Snapchat	SoundCloud	Telegram
Animal abuse	Somewhat – bestiality is banned but serious mutilation is restricted to adults	Yes – under coordinating harm and promoting crime	Yes – under violent and criminal behaviour	No	Yes – under violent content and threats, gore and mutilation	Yes – under violent content and gore	Yes	Partially – only sale of endangered animals mentioned	Yes – under violence and threatening behaviour	Not explicitly mentioned
Sexual abuse	Yes	Yes	Yes	No	No/Partially – only under harassment	No/Partially – under general abuse restriction	Not explicitly mentioned, but may fall within illegal harms provisions	Yes – under sexual content policy	Yes	Not explicitly mentioned but could fall under promotion of violence
Self-harm	Yes – under suicide	Yes – under suicide, self-injury and eating disorders	Yes – under suicide and self-harm	No	Yes – under promotion or glorification of self-harm	Yes – under suicide, self-injury, and harmful behaviour	Yes	Yes – under threats, violence & harm	Yes – under suicide, self-harm, eating disorder promotion, and other harmful behaviour	Not explicitly mentioned but could fall under promotion of violence
Mass violence	Yes – under violent content	Partially – tier 1 of dangerous organisations policy prohibits content that "glorifies, supports or represents [attempted] multiple-victim violence"	Partially – under violent and criminal behaviour	No	Partially – when targeted at a protected group	Yes – under real-world sensitive events	Not explicitly mentioned but likely falls under broader violence provisions	Not specifically mentioned	Yes – under violence and threatening behaviour	Not explicitly mentioned but could fall under promotion of violence
Interpersonal violence	Yes – under violent content	Yes – under violence and incitement	Yes – under violent and criminal behaviour	Partially – reference to threats of violence and hate based on identity or vulnerability	Yes – under violent content and threats, gore and mutilation	Partially – under threats, bullying and harassment	Yes	Not specifically but hate speech references include violence on the basis of certain characteristics	Yes – under violence and threatening behaviour	Not explicitly mentioned but could fall under promotion of violence
Arson/ property damage	Yes – under violent content	Yes – under coordinating harm and promoting crime	Yes – under violent and criminal behaviour	No	Yes	Yes – under threats, bullying and harassment	Yes	Not explicitly mentioned but may fall under illegal activities category	Not explicitly but could fall within violence and threatening behaviour	Not explicitly mentioned but could fall under promotion of violence

Table 3: Violent incitement mapped across the community guidelines of platforms relevant to nihilistic violence (as of November 2025)

Incitement to Real-World Violence

The promotion and incitement of violence is well addressed in platforms' community guidelines. Typically, larger platforms with more comprehensive guidelines are able to explicitly identify different forms of real-world violence, and include sub-provisions for animal abuse, property damage and various targets of violence. Incitement to violence is commonly addressed regardless of the target or perpetrator. However, especially among smaller platforms, catch-all language for violent behaviour tends to be employed, rather than wording that accounts for the specific targets and manifestations of subcultures of nihilistic violence.

A Relatively Comprehensive Platform Policy Picture

Overall, the vast majority of online behaviours and harm areas resulting from these subcultures is already within the scope of many platforms' community guidelines. While nihilistic violence subcultures, mobilisation pathways and strategies are relatively new phenomena – only gaining significant traction in the last five years – their resultant harms are not. Much of the content relevant to nihilistic violence is overtly violative, reducing the threshold decision-making burden for moderators and offering clear routes to recourse within existing policies. The question then is primarily one of effective enforcement.

As identified in the above matrices, platform policies on violent extremism, terrorism and dangerous organisations will have limited application to nihilistic violence communities. Instead, the toolkit of responses should be widened to include the focused enforcement of existing child safety, cyber crime, coordinated inauthentic activity, incitement of violence and sexual abuse policy areas. This will require much greater coordination between internal policy teams to align and coordinate on the intersections of these disparate harm areas.

4 A Behavioural Approach to Preventing Nihilistic Violence Online

Nihilistic violence cannot be addressed simply by pivoting or expanding existing work to counter terrorism and violent extremism, particularly where such strategies focus on ideological disengagement or group involvement. Instead, a public health model of violence prevention – focused on boosting protective factors and minimising risk factors – can be instructive, capturing not just ideological but also behavioural indicators and drivers of many forms of violence.[18] Such an approach seeks to prevent not just violent outcomes but the vulnerabilities that lead individuals towards violence and the range of resulting harms to society. Approaches traditionally distinguish between primary, secondary and tertiary prevention, which broadly encompass:

- Primary – Building immunity and resilience to violence at both a societal and individual level.
- Secondary – Addressing specific vulnerabilities and risk factors through targeted interventions.
- Tertiary – Mitigating the impact of violence and preventing acute and imminent harm.

Building Immunity and Preparedness

Primary prevention will be vital to building sufficient awareness in society of the risks and harms associated with nihilistic violence and inoculating young people from online manipulation.

Public Education and Awareness Raising

Widespread public education and awareness-raising are essential elements in building resilience and intervening at an early stage. National bodies have recognised that building knowledge among parents and frontline practitioners is a crucial element in protecting minors. For example, UK Counter Terrorism Policing, MI5 and the National Crime Agency delivered a warning to parents about Com network threats ahead of summer holidays when risk might be elevated.[19] All of society has a role to play in this education effort – including teachers, doctors, sports clubs and online platforms.

18 Jordan Reimer, "The 'Public Health Approach' to Prevention," Institute for Strategic Dialogue, accessed November 13, 2025, https://www.isdglobal.org/explainers/the-public-health-approach-to-prevention/.

19 "Counter Terrorism Policing, MI5, and the National Crime Agency Deliver Summer Holiday Warning to Parents," *Counter Terrorism Policing*, July 23, 2025, https://www.counterterrorism.police.uk/counter-terrorism-policing-mi5-and-the-national-crime-agency-deliver-summer-holiday-warning-to-parents/.

Given the compressed timelines of mobilisation to violence in service of solely an aesthetic – compared to extremist groups with deeper ideological programmes – educational efforts must begin at the earliest possible opportunity. For example, in relevant contexts platforms could consider opportunities to encourage (or mandate) engagement with anti-extortion resources. Such approaches could serve to build both resilience among users and friction among communities likely to promote harm. Building on pilot approaches to flagging support services – such as suicide hotlines – around specific keyword searches, opportunities for awareness-raising and off-ramping should be considered throughout the lifecycle of platform usage.

Inoculation and Resilience-Building

Beyond public education and awareness-raising, primary prevention techniques should equip users with the tools to identify the strategies used to manipulate them. Rather than responding to specific ideologies, such initiatives support recipients in identifying online grooming or information manipulation techniques, developing resilience to a range of ideological and non-ideological threats.

Inoculation-based strategies microdose potentially harmful content to participants, to explain flawed reasoning or manipulation.[20] Studies have evidenced how this approach has increased participants' ability to identify and reject extremist propaganda.[21] For example, the Bad News Game takes a gamified approach, with players challenged to build their own fake news empire. In so doing, the game improves the ability to identify and resist misinformation across ages, education levels and political leanings.[22] Such strategies are yet to be trialled against nihilistic threats. This offers an innovative opportunity with high potential for success, which would include impactful pilots on smaller platforms. More research on pathways into ecosystems of nihilistic violence is needed in order to identify the best opportunities and locations for interventions (both online and offline), spanning smaller and larger platforms.

20 *Positive Online Interventions Playbook: Innovating Responses to a Shifting Online Extremist Landscape in New Zealand* (Institute for Strategic Dialogue, 2024), 22.
21 Kurt Braddock, "Vaccinating Against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda," *Terrorism and Political Violence* 34, no. 2 (2022): 240–62, https://doi.org/10.1080/09546553.2019.1693370.
22 "Bad News – Play the Fake News Game," Bad News, accessed November 18, 2025, https://www.getbadnews.com/books/english/.

Engaging with Vulnerable Communities

At the secondary prevention level, efforts to disrupt the development of ecosystems of nihilistic violence must learn from the successes and failings of approaches used to counter violent extremism, while developing strategies tailored to the unique nature of this threat.

Tailored and Dynamic Counter-Communications

Preventing nihilistic violence demands a more tailored, dynamic and joined-up approach to ecosystem disruption. Traditional counter-communication techniques – which have sometimes struggled to achieve salience among ideologically motivated extremist communities – are even more likely to lack impact among nihilistic violence subcultures. Counter-narrative strategies focused on ideological deradicalisation will fall flat in communities not motivated by ideologies or whose abject misanthropy is highly resilient to counter-messaging.[23] In-group cultural dynamics and codes rooted in cynicism and subversive humour may lead nihilistic communities to mock counter-narrative attempts, further feeding harmful online dynamics and propaganda. Poorly considered and inappropriate disruption strategies are therefore not just at risk of futile outcomes but may even backfire.

Counter-communications will likely need to engage with, rather than ignore, subcultural elements such as humour. Such approaches might involve out-competing, out-mocking or out-meming nihilistic communities. Highly targeted, community-based and rapidly-produced content has the greatest likelihood of achieving success, delivered by those with clout in the relevant networks in order to project authenticity. Counter-communications efforts must be rooted in up-to-date research in order to understand the specific codes, drivers and dynamics of a platform network. They should be informed by an understanding of the full ecosystem of platforms employed by these communities to prevent short-term approaches which solely prompt platform migration and replication of communities elsewhere. This will demand a coordinated, cross-platform effort, which should include proactive engagement of smaller platforms used by these communities.

Active Bystander Interventions

Some efforts should be tailored even more closely to the diverse subcultures within nihilistic violence communities. Analysis shows that TCC networks are typically self-governed, constructing an expectation and culture of community intervention. Within closed, high-harm spaces, users police their own communities and non-TCC users are removed by community moderators. This system of self-policing could be leveraged as an intervention opportunity for hard-to-reach online communities. Community moderators can act with more agility, knowledge and trust than platform moderators. Introducing active bystander moderation practices into these communities would offer the closest possible off-ramp for users at risk. Platforms should consider how best to empower community moderators with both prevention resources and off-ramping support to dislodge potential pathways to harm at the earliest possible stage.

23 Milo Comerford, Moustafa Ayad, and Jakob Guhl, *Gen-Z & The Digital Salafi Ecosystem: Executive Summary* (Institute for Strategic Dialogue, 2021), 11, https://www.isdglobal.org/wp-content/uploads/2021/11/Executive-summary.pdf.

Bridging to Support

Tertiary prevention measures will be equally crucial to ensure that highly vulnerable users are effectively directed to the necessary support services.

Platforms have long developed interventions to deliver information notices around potentially harmful keyword searches, such as eating disorders, self-harm and financial scams. Such practices should be expanded to harms associated with nihilistic violence, using relevant linguistic or behavioural identifiers to flag relevant support services. Table 4 provides a non-exhaustive overview of potentially relevant support services to which platforms could signpost.

	US	UK
Child exploitation	National Centre for Missing and Exploited Children (NCMEC)	Child Exploitation and Online Protection Command (CEOP); National Society for the Prevention of Cruelty to Children (NSPCC); Childline
Nonconsensual intimate image sharing and CSAM	Take It Down	Internet Watch Foundation (IWF); Revenge Porn Helpline
Cybercrimes	CyberTipline; FBI Internet Crime Complaint Center	The Cyber Helpline
Self-harm	988 Lifeline; Crisis Text Line; Shout	Mind; Papyrus UK; Samaritans
Eating disorders	National Eating Disorders Association (NEDA)	Beat
Psychological support	Crisis Text Line	Papyrus UK; Samaritans

Table 4: Support services mapped against the nihilistic violence harms taxonomy

There is a high risk of illegal harms – both online and offline – being mobilised in nihilistic online subcultures. There are legal measures in the US that can be leveraged; for example, the Take It Down Act now legally requires the removal of nonconsensual intimate images within 48 hours of a victim request.[24] Building on these new frameworks, such platform systems could easily be mirrored for other relevant harm areas, such as doxxing, CSAM or extreme gore content. This would serve both to protect victims and to disrupt mobilisation pathways.

24 TAKE IT DOWN Act, S146, 119th Congress (2025–2026), accessed November 18, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/146.

Gaps and Opportunities for Further Support

Beyond prevention strategies, social media platforms have ample opportunities to address subcultures of nihilistic violence through improved internal processes and coordination.

Evading Ban Evasion

Some communities associated with nihilistic violence, such as TCC, have become adept at ban evasion. TCC members use markers, tags and references to regroup after their accounts are removed, pre-empting moderation attempts. While individual accounts are removed, these regrouping strategies are not integrated into moderation practices, allowing new accounts to simply re-emerge and re-engage with their peers.

Current ad hoc moderation and account removal processes have failed to hinder an agile and resilient ecosystem. In order to reduce the ability of harmful ecosystems to function, and to ensure sufficient friction is introduced, platforms must implement far more strategic measures. These could include enforcing IP bans or device fingerprinting to reduce the ability of repeat users to create new burner profiles. These systems may already be in place from efforts to counter spam and inauthentic activity and could be pivoted to TCC communities. Platforms should also incorporate regrouping codes into moderation enforcement in order to mitigate repeat offending. As the TCC playbook evolves, such strategies will need to be continually updated and re-enforced.

Cross-Platform Collaboration

The tech stack leveraged by nihilistic violence ecosystems demands a cross-platform solution to encourage wholesale network disruption. Rather than isolated platform enforcement measures from which communities are able to easily regroup using other platforms, a much more collaborative and coordinated approach is needed, engaging networks such as GIFCT. Their tools such as the Hash Sharing Database and Incident Response Framework could provide models for joined-up response, which would include support for smaller platforms. This must start with intelligence-led scoping across platforms to understand not just the users but the key networks driving nihilistic violence. Mapping is a vital step to fully inform opportunities for wholesale network disruption.

Law enforcement networks such as Europol, or private companies, have previously delivered strategic action days against IS and Terrorgram cross-platform networks.[25] This approach could easily be repurposed for nihilistic violence networks, with social media platforms delivering coordinated takedowns based on ecosystem mapping. This would incur far more disruption and introduce more friction into nihilistic violence subcultures than any individual platform takedown attempt.

25 Terrorgram is an online network of neo-fascist accelerationists who produce and share propaganda encouraging adherents to conduct terrorist attacks, which primarily operates on Telegram. For more information, see: Steven Rai, "Beyond the Collective: Understanding Terrorgram's Efforts to Infiltrate the Mainstream on Telegram", *Institute for Strategic Dialogue*, August 24, 2024, https://www.isdglobal.org/digital_dispatches/beyond-the-collective-understanding-terrorgrams-efforts-to-infiltrate-the-mainstream-on-telegram/.

Cross-Sector Partnership

The rapid pace of change of groups, codes and spaces associated with subcultures of nihilistic violence demands dedicated research capacity. The evolution of the threat presents too great a challenge for any single platform's trust and safety team, and instead requires a wide network of individual experts, organisations and law enforcement professionals. In order to gather the necessary deep expertise in a way that captures the constant evolutions of the threat landscape, an information-sharing hub could be established, with experts contributing insights on platform migrations, trends and specific violations. Such a partnership could be particularly impactful for smaller platforms without in-house specialist resources and expertise.

To provide more comprehensive threat landscaping – for example around the scale and reach of these communities – and to support platforms in mitigating content that flagrantly violates terms of service and community guidelines, experts need meaningful access to platform data, for example to understand salient signals from deplatformed accounts.

5 Conclusions

This policy brief has emphasised how online subcultures of nihilistic violence represent a rapidly evolving threat that cannot be addressed through traditional counter-extremism frameworks. These communities are defined not by ideology but by misanthropy and a fixation on violence, creating unique challenges for prevention and disruption.

Networks such as the Com and 764, alongside fandom-driven spaces like TCC, operate across multiple platforms and employ sophisticated ban-evasion tactics. Their activities span sexual exploitation, cyber harms and real-world violence, often blurring the line between victim and perpetrator. While most harms fall within existing community guidelines, the resilience of these networks shows that enforcement remains fragmented and reactive.

Platforms must move beyond siloed 'whack-a-mole' moderation towards coordinated, cross-platform strategies that integrate child safety, cyber crime and violence prevention policies. Prevention-based approaches should centre on a public-health model that prioritises resilience-building, early intervention and safeguarding support for victims. Beyond the typical toolbox used to counter ideologically motivated extremism, more disruptive counter-communications, the promotion of active bystander interventions, and friction-based measures can help disrupt mobilisation pathways. Crucially, cross-sector collaboration, rooted in a shared evidence picture of this ecosystem, will be essential to keep pace with the agility of these networks.

Ultimately, addressing nihilistic violence demands a shift from ideology and group-centric response frameworks to more holistic, behaviour-focused strategies that recognise that violent radicalisation can be understood as much in terms of an aesthetic as a means to an ideological end. Platforms, policymakers and civil society must work together to develop interventions that protect vulnerable users, disrupt harmful ecosystems and build resilience across society. Without such coordinated action, subcultures of nihilistic violence will continue to exploit platform vulnerabilities and escalate severe harms both online and offline.

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

Global Network on Extremism and Technology (GNET)
Centre for Statecraft and National Security (CSNS)
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**
W. **www.gnet-research.org**

Institute for Strategic Dialogue (ISD)
T: **+44 20 7493 9333**
E: **info@isdglobal.org**
W: **www.isdglobal.org**

Global Internet Forum to Counter Terrorism (GIFCT)
E: **outreach@gifct.org**
W: **www.gifct.org**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.