ISD | Institute for Strategic Dialogue

EMERGING EXTREMISM-RELATED THREATS IN THE UK: IMPLICATIONS FOR POLICY RESPONSES

CONTENTS

Executive summary 3

Key findings 3

- The evolving threat landscape 3
- Shifting mobilisation pathways 3
- Implications for prevention and intervention 4
- Considerations around digital legislation 4

Part 1: The evolving threat landscape 5

- Ideologically amorphous threats 6
- The Manosphere and misogynistic violence 7
- Nihilistic violence 7

Part 2: Shifting mobilisation pathways 9

- The evolving role of online platforms 9
- Youth radicalisation 9
- The growing intersection of extremism and state threats 10

Part 3: Implications for prevention, intervention and regulation 11

- Towards a broader violence prevention framework 11
- Prevention and intervention 13
- Hybridised extremism and digital regulation 15

Conclusion 16

INTRODUCTION

EXECUTIVE SUMMARY

The UK extremism threat landscape is undergoing fundamental shifts, marked by a growing number of decentralised online networks and hybridised ideologies rather than formalised groups. Yet current response frameworks struggle to address individuals who do not fit stable ideological categories.

The evolving threat demands fundamental recalibration of approaches to mitigating extremist-related violence, moving beyond solely ideology-focused approaches towards comprehensive violence prevention.[1] This would address emerging radicalisation pathways, while maintaining proportionate responses to established ideology-based threats.

Building on ISD's evidence to the Home Affairs Committee enquiry on 'Combatting new forms of extremism' and recommendations for Lord Anderson's 'Lessons for Prevent' report, this policy paper proposes a broader framework for violence prevention to encompass both ideological and non-ideological violent threats. Rooted in an analysis of these evolving threats, we suggest how prevention, intervention and digital regulatory efforts can respond to this new challenge.

KEY FINDINGS

THE EVOLVING THREAT LANDSCAPE

- In addition to the more established challenge from far-right and Islamist extremism, a growing set of extremism-adjacent violent threats reflect a diminishing role of organised groups with a clear ideological programme, and an increased prominence of harmful online communities, de-centralised networks and self-initiated individuals.
- The Southport attack exemplifies violence driven by nihilism rather than coherent ideology. Such cases lack traditional political motivations but share similar aesthetics and radicalisation pathways with extremism-based threats.
- School shooter fandoms glorifying mass killers like the Columbine shooters have inspired multiple UK plots, with teenagers mimicking shooter aesthetics. The 764 network and other Com networks engage in sextortion and violence glorification, forcing child victims to produce child sexual abuse material and perform acts of violence.
- Misogynistic ideologies permeate diverse extremist movements, serving both as standalone motivations for violence and pathways into broader extremist networks.

SHIFTING MOBILISATION PATHWAYS

- Platform systems serve to catalyse diverse extremist movements, including the algorithmic amplification of harmful content to users who may not otherwise have encountered it. Memes, aesthetics and gaming motifs lower barriers to entry, normalise violence and foster in-group identities, and help extremists evade moderation through coded references.
- Prevent referrals for young people have doubled in the last year, with minors constituting a fifth of terrorism arrests – four times the proportion of a decade ago. However, recent far-right terrorist attacks have been committed by older individuals, indicating threats across age demographics. High frequency of neurodiversity and poor mental health in young terrorism cases shows the importance of protective – rather than solely securitised – responses.
- Hostile states employ a spectrum of strategies to destabilise British democracy. These range from harmful online influence operations to fomenting violent extremist plots, constituting new pathways for mobilising young people towards harmful activity through online influences.

1 ISD defines extremism as "the advocacy of political and social changes in line with a system of belief that claims the superiority and dominance of one identity-based 'in-group' over an 'out-group'. Extremism is rooted in the advancement of a dehumanising 'othering' mind-set incompatible with pluralism and universal human rights and can be pursued through violent and non-violent means." As this is intended to provide an accessible overview of the threat landscape, we approach the emerging phenomena in this briefing in terms of their status as 'extremism-adjacent' threats. An example of this is nihilistic violence (discussed in detail below), which by definition does not constitute a form of ideological supremacy but nonetheless encompasses highly similar aesthetics, online communities and radicalisation pathways.

IMPLICATIONS FOR PREVENTION AND INTERVENTION

- Hybridised extremist threats have landed in Prevent's portfolio not by design but due to the absence of other support systems, resulting in overloading and inappropriate triage services. Cases such as the Southport attack have therefore slipped through the gaps of a system designed to identify ideologies, as highlighted by interim Prevent Commissioner Lord Anderson's 'Lessons for Prevent' report.

- Broader violence prevention frameworks could respond more appropriately to this threat landscape and the shared vulnerabilities underpinning it. There are cost-effective opportunities for creating what Lord Anderson describes as a 'big front door' for triaging threats in a more agnostic manner. This includes re-organising local structures such as integrating Multi-Agency Safeguarding Hubs with Channel boards and linking Prevent Oversight Boards and Serious Violence Boards with Community Safety Partnerships.

- Public health models take a non-securitised and ideology-agnostic approach to violence prevention, minimising risk factors while boosting protective factors. Much of this programming already exists but should be knitted together more strategically by a policy oversight board which brings together national and local government.

- Strategic communications and other counter-extremism interventions need to be better rooted in up-to-date understandings of the contemporary online extremist landscape, while learning lessons from best practices over nearly two decades of prevention programming.

- Youth empowerment is central to effectively understanding and responding to rising extremism among young people. Meaningful structures should be established to provide young people increased input to prevention, as in New Zealand and Australia.

- Threats like Com networks cannot be addressed by ideological disengagement but demand bespoke protective and safeguarding programming for young people. Key risk factors should be proactively communicated to caregivers and frontline practitioners.

CONSIDERATIONS AROUND DIGITAL REGULATION

- Social media regulation must account for the full life-cycle of online harms related to extremism including production (e.g. abuse of Generative AI), distribution (algorithmic systems) and consumption (exposure to harmful content). This will require balancing efforts to address the proliferation of illegal content, distortive platform systems amplifying extremist content as well as specific risks to minors.

- Alongside new rules on mitigating illegal content, the effective enforcement of Ofcom's Protection of Children Codes will be crucial to address many emerging youth radicalisation threats. This must span both mainstream and smaller, high-risk services where much of this activity occurs.

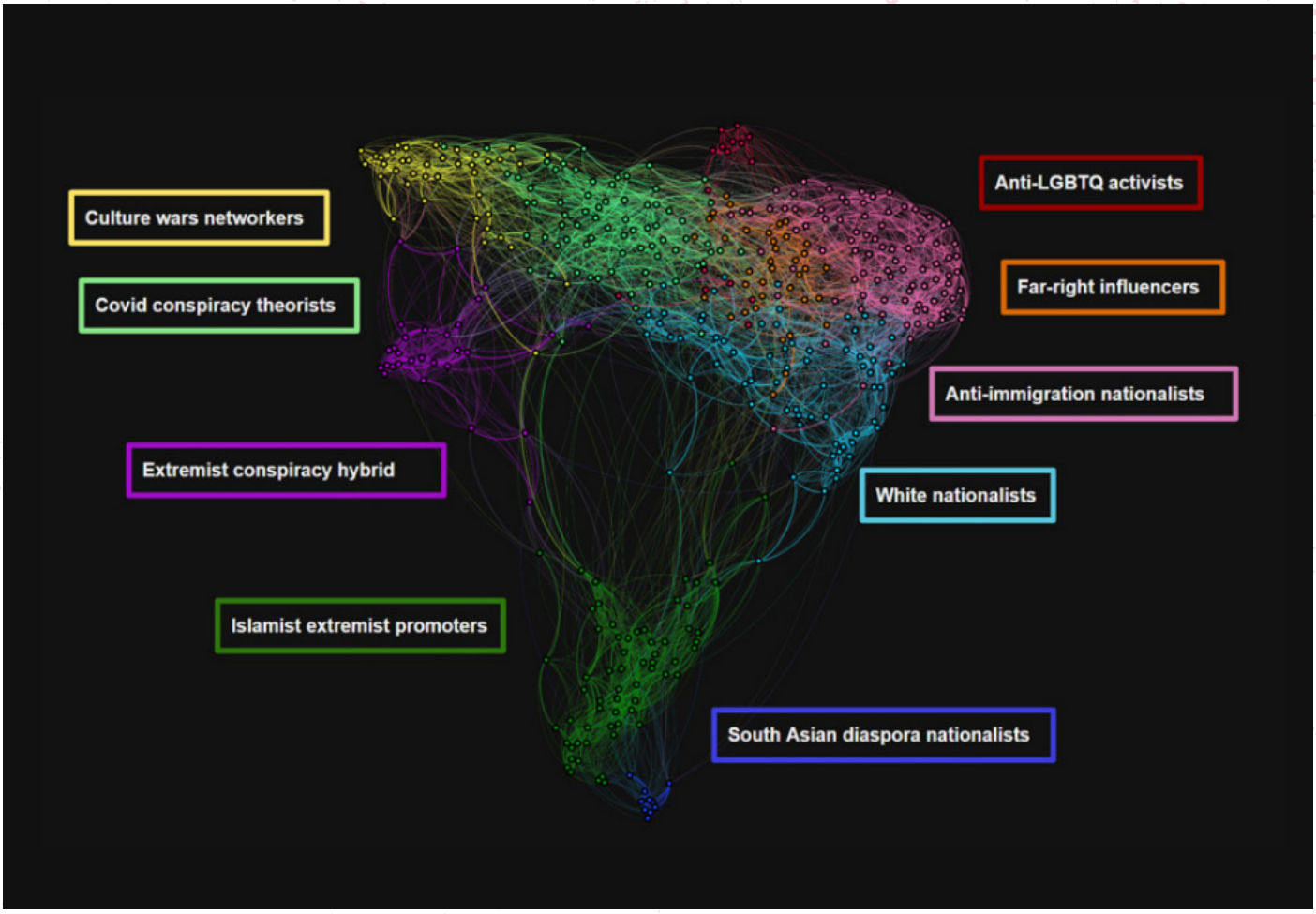
- An effective transparency regime is essential for understanding the evolution of online threats, interrogating how platform systems are amplifying harmful content. The swift implementation of the Data Use (and Access) Bill is essential for providing data access to researchers to scrutinise the efficacy of platform responses to online extremism.

PART 1 THE EVOLVING THREAT LANDSCAPE

The UK extremism landscape is characterised by both a sustained challenge from 'traditional' threat actors – including far-right and Islamist extremists – as well as a growing phenomenon of more amorphous forms of extremism, whose complex relationship with ideology challenge existing intervention programmes and policies. While often constituting harms of equivalent seriousness to terrorism (as outlined in Lord Anderson's 'Lessons for Prevent' report), this broader landscape of threats also generates a broad multitude of harms. These include targeted hate and harassment of vulnerable communities, erosion of rights and freedoms, interpersonal violence, and mass casualty attacks. Contemporary extremist actors often operate in diffuse, decentralised online networks with online activity regularly inspiring violent extremist activities offline.

A notable example of more amorphous forms of extremism includes the 2024 Southport attack, motivated primarily by a teenager with a fascination with extreme violence, nihilism and misanthropy (explained further here). Axel Rudakubana was referred to Prevent three times but was not referred onward to Channel due to the lack of a coherent ideology present. The UK has also experienced multiple cases of such violence with ambiguous ideological underpinnings but links to fringe online communities. This includes school shooter fandoms (most recently a Scottish schoolboy and Nicholas Prosper), neo-Satanist networks (including Cameron Finnigan and Danyal Hussein) and the Manosphere (such as the 2021 Plymouth shooting and the 2020 conviction of Gabrielle Friel). Cases motivated by similarly diffuse and hybridised forms of extremism have occurred across Europe, Australasia and North America.

Figure 1: From ISD research for Ofcom, a map of online accounts in the UK related to extremism and terrorism as well as harmful conspiracy and hate movements. 'Communities' are clustered by distinct language use characterised by expert analysts.



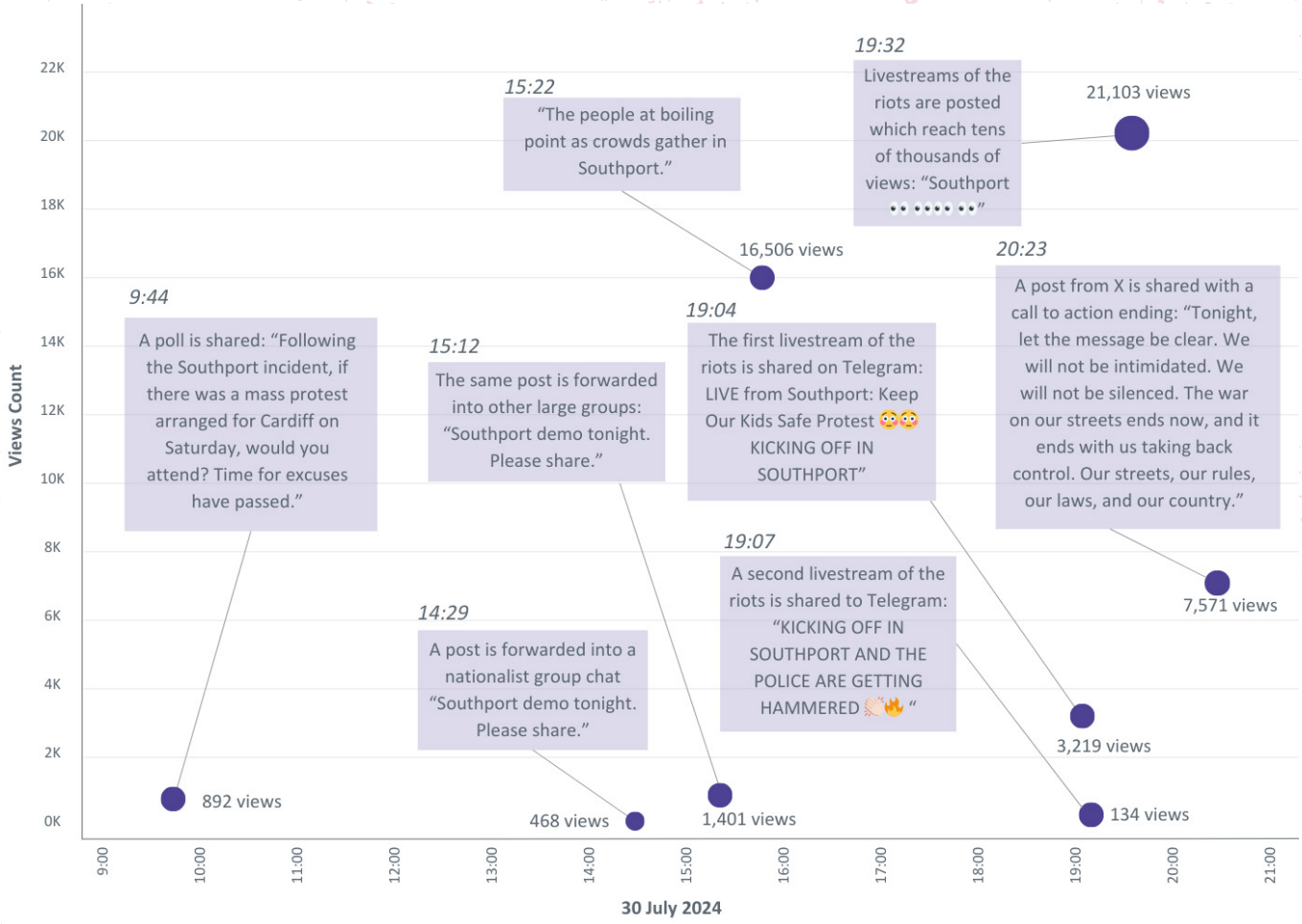
UK counter-terrorism approaches, developed in the aftermath of 9/11 and 7/7, were designed to counter a very different threat, predominantly centred on top-down, ideologically-coherent groups. While efforts have been made to adapt this infrastructure to contemporary threats, existing approaches are poorly equipped to address these more hybridised forms of extremism. This includes both actors inappropriately channelled into the counter-terrorism system, as well as mass violence which the system has been unable to prevent, such as the Southport attack. This report presents our analysis of contemporary trends in extremism – including 'nihilistic violence' – and pathways into extremist (and extremist-adjacent) networks.

IDEOLOGICALLY AMORPHOUS THREATS

A central trend in the UK's extremism landscape is the rise of post-organisational extremism, which represents a structural shift in how individuals engage with and are mobilised by extremism. Rather than traditional group-based movements with coherent ideologies and hierarchal structures, individuals now increasingly radicalise and organise through decentralised online networks. The 2024 Southport riots illustrate this shift: violence was incited and spread across digital platforms without the involvement of a single organisation, leader or ideology but rather through diffuse networks, the algorithmic amplification of outrage-driven influencers, opportunistic calls to action and locally-rooted narratives which targeted marginalised groups and culminated in serious public disorder. These post-organisational dynamics fall between the gaps of existing policies where current infrastructure is often designed to respond to formal group structures. For example, over-reliance on group proscription can limit policy levers for responding to non-group related extremism threats, with the legality of terrorist material rooted in lists of proscribed groups (for example in the social media regulator Ofcom's guidance on terrorist content).

Alongside more coherent extremist ideologies, the UK extremism threat is increasingly characterised by 'hybridised' ideologies where elements of far-right, religious, conspiratorial, misogynistic and/or other extremist worldviews combine into highly personalised

Figure 2: Timeline of a selection of Telegram posts mobilising the 2024 summer riots, demonstrating how the riots were mobilised by diffuse networks of individuals rather than formal groups.

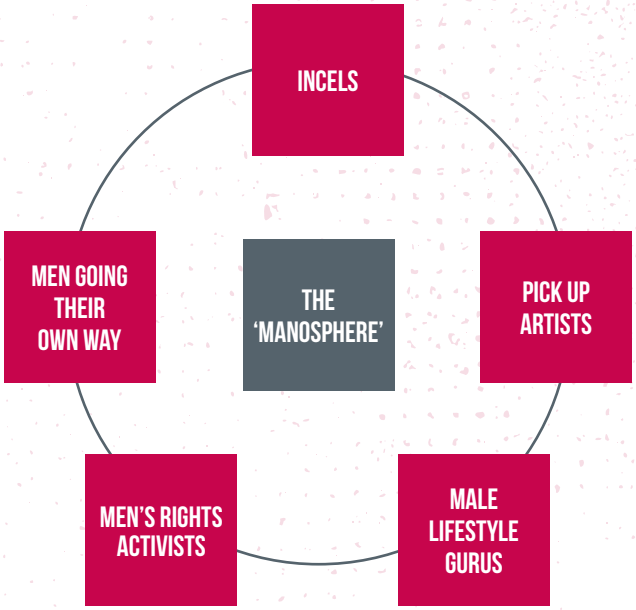


belief systems that are shaped and shared across online spaces. ISD's research shows that such hybrid belief blending is no longer an exception but an emerging norm. Existing response frameworks based around identifying ideologically defined threats may be challenged to handle individuals who present this type of hybrid risk and who do not meet terrorism thresholds or trigger established safeguarding responses. A parallel dedicated mechanism is needed urgently to assess and manage hybridised radicalisation dynamics alongside existing frameworks that address individuals who adhere to more stable ideological categories (outlined in greater detail in the section below).

THE MANOSPHERE AND MISOGYNISTIC VIOLENCE

Across the evolving extremist landscape in the UK, misogyny remains a pervasive and cross-cutting ideology. While there has been no confirmed case of misogynistic terrorism in the UK to date, the role of misogyny in driving violence is increasingly evident. Recent incidents – including the 2021 Plymouth Shooting; the killing of an ex-girlfriend, her sister, and her mother by Kyle Clifford; the stabbing of a lesbian couple on Bournemouth beach; and a Luton case where a perpetrator murdered family members after abandoning plans for a school shooting – demonstrate how misogynistic motivations often underpin acts of mass violence. These cases illustrate how violence rooted in grievance can escalate into violence at the intersection of targeted hate and extremism. Misogyny also plays a key role in radicalisation across a broad ideological spectrum, including far-right and Islamist extremism. Misogynistic ideologies are central to terrorist organisations, enabling misogyny to serve not only as a standalone motivation for violence but as an open door into more extremist ideas.

Figure 3: A visualisation of the Manosphere



The Manosphere is a loosely connected network of groups, actors, influencers, communities and spaces online, including ideological communities such as incels, Men Going Their Own Way (MGTOW), pick up artists, male lifestyle gurus and men's rights activists. While not all inherently extremist in nature, the Manosphere serves as a breeding ground for the most extreme and violent expressions of misogyny, with elements of incel communities frequently glorifying or justifying acts of violence – such as those committed by Alek Minassian and Elliot Rodger. ISD's online analysis reveals that online misogyny often acts as a gateway between extremist communities.

A more recent development within the wider Manosphere ecosystem is the rise of male lifestyle influencers, who blend content on fitness, finance and self-improvement with ideologically charged and often misogynistic messaging. These so-called 'male lifestyle gurus' have become highly influential figures, particularly among young men and boys, using aspirational narratives to position dominance over women as central to achieving status, success and self-worth.

While not always overtly violent, the rhetoric deployed by figures such as Andrew Tate and others promotes a worldview in which women are seen as lesser and duplicitous, and in which control and coercion in relationships are framed as marks of masculine success. Their reach blurs the line between self-help and ideological grooming, embedding misogynistic attitudes into mainstream digital culture. As such, these figures act as a bridge between mainstream and fringe ideologies, normalising harmful narratives and lowering the threshold for engagement with more extreme content and communities.

NIHILISTIC VIOLENCE

The concept of 'nihilistic violence' has recently gained traction among researchers, policymakers and the media but remains a poorly understood phenomenon. While many ideologically motivated extremists cite nihilism and/or misanthropy as part of their motivation, there is a distinct trend of mass violence that eschews traditional ideological drivers. Nihilistic violence is distinguished from ideologically motivated extremism by its lack of an overarching ideological motive and is generally driven by misanthropy or a desire to gain acceptance or notoriety in online communities. While these acts of violence outwardly resemble extremist

violence, they lack the political or ideological dimension that drives typical extremist attacks. This was evident in the case of Axel Rudakubana whose digital activity reflected a volatile mix of violent nihilism, antisocial resentment and sporadic engagement with far-right and mass shooting subcultures.

764/COM NETWORKS

764 is a network of online groups that engage in sextortion and the glorification of violence. The network, which comprises a constantly shifting landscape of splinter groups and offshoots, forces child victims to produce Child Sexual Abuse Material (CSAM). They then use that CSAM as leverage to force victims to perform acts of violence, animal abuse or self-harm. They also engage in extensive swatting, harassment and intimidation campaigns to silence their victims. Since 2021, at least 20 members or affiliates of 764 have been arrested in at least 5 countries. While the bulk of these arrests were for sextortion and/or possession or distribution of CSAM, the group has also been linked to incidents of mass violence. At least two Swedish teenagers affiliated with a 764 offshoot (No Lives Matter) were arrested for separate stabbing sprees in 2024 and 2025. Additionally, an American teenager who allegedly participated in 764 social media chatrooms was arrested in June 2025 for planning a mass casualty attack in Oregon. 764 members are located around the globe. While researchers do not have sufficient information to assess the number of British 764 members, the case of Cameron Finnigan demonstrates the presence of the network in the UK. In June 2025, police recorded a car vandalised with 764-related messages in York.

764 emerged in 2021 from the "Com Network," an online cybercrime, extortion and swatting community. Com and 764 members continue to interact and analysts have observed a number of 764 members "swatting" researchers, schools, banks and government organisations. These swatting calls are carried out for online notoriety, to intimidate victims of 764 sextortion and for profit (swatting-for-hire).

SCHOOL SHOOTER FANDOMS

School shooter fandoms, particularly those that revere school shooters, have been a driver of targeted school violence in the United States for decades. A spinoff from the larger True Crime Community (TCC) – a fandom devoted to obsessing over high-profile killers – 'Columbiners' consider Eric Harris and Dylan Klebold with intense interest that ranges from infatuation to sometimes outright worship. The shooters' expressed nihilism, desire for revenge and notoriety, and belief that they could ascend to a kind of godhood through violence resonates strongly with their fans, many of whom have a similar interest in nihilistic violence and misanthropy. Like most fan communities, this interest manifests as online discussion forums, art and fanfiction, cosplay, roleplaying, and imitation. While not everyone in these communities presents a risk to themselves or others, dozens of school attacks worldwide can be linked back to these online communities, whose participants' zealotry occasionally inspires them to try attacks of their own. These communities overlap significantly with white supremacist spaces, due in part to their interest in white supremacist killers and a habit of collecting attack footage, regardless of their ideological basis.

Several such plots have been interrupted in the UK in recent years. In 2018, two boys were convicted of planning a school shooting, including mimicking the aesthetics of the Columbine shooters. In 2019, 19-year-old Shane Fletcher was arrested for plotting a Columbine-inspired attack in Workington. In one of the most disturbing recent incidents, 18-year-old Nicholas Prosper killed his mother, sister, and brother as the first part of his plan to carry out a school attack that would rival the Sandy Hook and Virginia Tech shootings in the United States. While the limited availability of case information, especially in cases involving minors, can make it difficult to gauge to what extent perpetrators were involved in these online spaces, obsessions with – and plans to emulate – mass killers (with little to no ideological relation to the perpetrator), and the collection of photos, journals or fan materials of their favourite killers all imply a likelihood of some involvement with communities such as TCC or Columbiners.

PART 2 SHIFTING MOBILISATION PATHWAYS

THE EVOLVING ROLE OF ONLINE PLATFORMS

Specific digital subcultures such as incel forums, anti-feminist spaces, conspiracist and extremist online communities have come to play an increasingly central role in radicalisation trajectories in the UK. These spaces cultivate grievances, offer an identity and belonging - particularly to young men - and serve as gateways to the normalisation of hostility and dehumanisation towards whichever group is perceived as the source of harm or injustice. In recent UK cases, including Southport, perpetrators display long-term immersion in such subcultures without being affiliated to any formal movement. There is a need to recognise such online subcultures as potential incubators of violence, requiring tailored intervention strategies, earlier safeguarding responses and enhanced practitioner training to respond to the potential psychological, social and violent risks emerging from these communities.

Aesthetics have become a core component in the spread of extremist ideas particularly among younger online audiences who are increasingly exposed to extremist narratives not only through online subcultures but also through visual culture. ISD analysis has documented the deliberate use of irony, memes, gaming motifs and more to repackage extremist narratives to appeal to new recruits in ways that resonate culturally whilst also circumventing platform moderation. These tactics diminish resistance to hateful or violent messaging by presenting it as humour, entertainment and even personal empowerment.

Distinctive aesthetic signatures have also emerged which cross-cut diverse extremist networks, with ISD research documenting how segments of Gen-Z Salafi communities have adopted visual tropes pioneered by alt-right ecosystems whose worldview they otherwise reject. This so-called Islamogram network includes the use of fashwave (far-right synthwave), edited videos and gaming inspired content repurposed to create new hybrid genres such as mujahidwave. These elements play a decisive role in extremist socialisation, incubating in-group dynamics and lowering thresholds to engagement with violence, and have been linked to a wave of pro-Islamic State (IS) group violent plots across Europe from teenagers heavily engaged in extremist content creation.

Social media platforms' systems have been found to exacerbate these dynamics, including through closed, anonymous servers which incubate highly harmful in-group dynamics. Based on analysis of gaming platforms such as Steam, Discord, DLive and Twitch, ISD research shows how gaming can act as a means of bringing extremists together to socialise, cement harmful ideas and recruit new individuals, particularly young people. The gamification of violent extremism across diverse platforms encourages users to continuously innovate and expand violent extremist activity.

Figure 4: Examples of Islamogram memes blending alt-right aesthetics with Salafi-jihadi ideas.

ISD's evidence to the Science, Innovation and Technology Committee inquiry on social media, disinformation and harmful algorithms shows how platform recommender algorithms can serve users extremist content, which curates online environments, cements societal bias and exposes users to harmful content which they otherwise may not have seen. During the summer 2024 riots, ISD evidenced platform algorithms serving a false name of the attacker to users searching for 'Southport' even hours after the name was confirmed by the police as inaccurate, potentially serving to exacerbate anti-migrant narratives which resulted in widespread targeted violence. In a separate study, ISD and Reset found that 10 Australian YouTube accounts were recommended increasingly misogynistic and Manosphere content on YouTube Shorts. Platforms systems must be considered when assessing both radicalisation pathways and potential offramps.

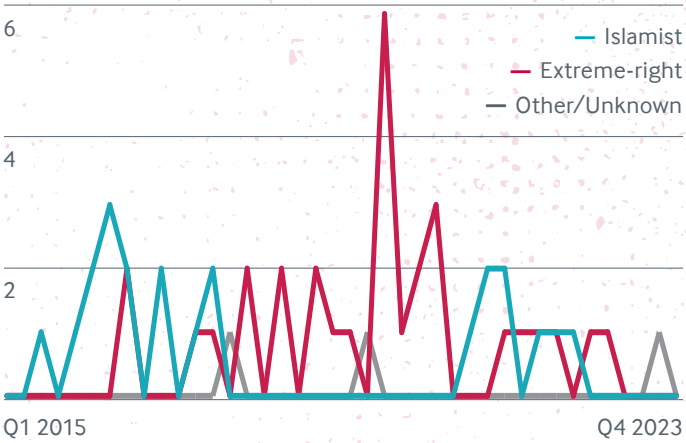
YOUTH RADICALISATION

The average age of individuals involved in extremist networks is decreasing. The Home Secretary recently identified that referrals for young people to the Prevent programme have doubled in the last year. Minors constitute a fifth of terrorism arrests, four times the proportion a decade ago. At least 55 minors have been convicted of terrorism offences in England and Wales since 2016, including 34 cases of collecting terrorist information, 27

cases of dissemination of a terrorist publication, 12 cases of encouraging terrorism and 14 minors convicted of preparing acts of terrorism. Analysis of these cases shows children are uniquely vulnerable to extremism due to social isolation, thrill-seeking tendencies, adverse childhood experiences, identity formation and community searching [Vale & Rose, Terrorism & Political Violence, upcoming 2025]. Children involved in terrorism therefore simultaneously exist as both perpetrators and victims [Vale & Rose]. Children are at risk of causing serious harm and violence, increasingly able to recruit peers, and foster extremist digital ecosystems independently of adults. However, the response cannot simply transplant highly punitive and adult-centric counter-terrorism strategies onto children. These growing engagement drivers point towards the need for comprehensive preventative and safeguarding responses. While the impact remains to be seen, the recent introduction of Youth Diversion Orders promises to increase non-criminal offramps for children.

As of October 2024, 31% of minors convicted of terrorism in England in Wales since 2016 had a formal neurodiversity or mental health diagnosis. Among extreme-right minors, this rose to almost half (45%), vastly exceeding national averages. At trial, neurodiversity was understood to impact obsessional interests, vulnerability to manipulation and social isolation (Vale & Rose). However, conditions such as ASD are only found to play an exacerbating role in radicalisation processes when combined with other social factors. More research – particularly from psychologists – is vital to greater understand the link between neurodiversity and vulnerability to extremism. A lack of sufficient support for neurodiverse people and those with poor mental health has left vulnerabilities to radicalisation: strengthening of these public services will likely have a knock-on effect on the extremism landscape. Approaches to addressing neurodiversity in radicalisation should focus on protecting, rather than securitising, individuals.

Figure 5: Number of children convicted under the Terrorism Act in England and Wales since 2016.



While youth extremism preoccupies Prevent and terrorism arrests, it is simultaneously true that recent far-right terrorist attacks in particular in the UK have been committed by older individuals, including the murder of Jo Cox (53), the Finsbury Park mosque attack (47), the Exeter synagogue arson (52), and the Dover migrant centre firebombing (66). This is mirrored by a predominantly middle-aged demographic in conspiratorial mass movements which have engaged in violence, such as QAnon. To date, there has not been a terrorist attack committed by a minor in the UK, but minors have perpetrated extreme violence. Youth engagement in extremism demands increasing attention but should not come at the expense of focussing on prevailing traditional threats from adults.

THE GROWING INTERSECTION OF EXTREMISM AND STATE THREATS

The increasing intersection between hostile state actors and violent extremism presents a growing threat to the UK's national security and represents an emergent pathway for violent mobilisation, especially among younger people. ISD's research outlines the spectrum of hybrid tactics leveraged by hostile states, with the recent arrest of eight Iranian nationals linked to a terrorist plot against the Israeli embassy in London emblematic of the potential violent security threat by Iranian-linked and inspired networks. Targeted and agile influence operations frequently instrumentalise online platforms to exploit geopolitical events with the aim of undermining liberal democracy and provoking unrest to advance state interests.

State actors such as Iran, Russia and China amplify divisions already present within British society, weaponising existing extremist narratives, political and community tensions as well as online hate ecosystems to further their strategic objectives. In the aftermath of 7 October 2023, Iranian-linked networks seized on the crisis to intensify antisemitic narratives and agitate against Western democracies, including by making common cause with accelerationist actors. This activity sits alongside a broader Iranian threat spectrum encompassing cyber-enabled attacks, the targeting of critical infrastructure, and plots against UK-based dissidents and journalists.

While legal reforms such as the National Security Act and Foreign Interference Registration Scheme mark important steps, policy responses remain fragmented across extremism, foreign policy and national security domains. A more integrated approach is now required to address the overlap of extremism and state threats in violence mobilisation, including co-ordinated use of counter-terrorism powers, digital regulation, sanctions and wider joined-up prevention efforts.

PART 3
IMPLICATIONS FOR PREVENTION, INTERVENTION AND REGULATION

The current Prevent system – established to accommodate a relatively small cohort susceptible to radicalisation – is not equipped to deal with the volume of cases it now sees. Any system of referral and intervention will inevitably suffer from over-referral because concerning behaviours might represent any number of social harms, from neglect to bullying to abuse to radicalisation. Triaging is required to ensure the appropriate intervention is provided by the appropriate body. According to the most recently released statistics, of the nearly 7,000 referrals made to Prevent in the year to March 2024, just 13% were discussed at the safeguarding support programme Channel as suspected radicalisation, while even fewer (7%) went on to be adopted to receive Channel support.

The largest category of individuals referred to the program (36% of cases) were classed as 'Vulnerability present but no ideology or CT risk', although these cases only represented 6% of referrals to Channel. The use of this category likely does not point towards a coherent analysis of the threat but a situation where new groupings of referrals are bolted on to address the 'everything else' which is referred to the Prevent program (previously the case with 'Mixed, Unclear, Unstable' designations). Furthermore, the low volume of Channel cases resulting from this category also suggests that cases are referred to Prevent due to a lack of other available (or effective) referral options, and then either closed or triaged to more appropriate social care avenues. This approach has not evolved through a carefully considered strategy but through the absence of one, with new and emerging risks funnelled into Prevent because there is nowhere else for them to go. Whilst this may have been more sustainable when numbers were more manageable, it is clearly unsustainable today.

TOWARDS A BROADER VIOLENCE PREVENTION FRAMEWORK

Many individuals referred to Prevent are better served in a broader system of violence prevention and safeguarding support than within a counter-terrorism programme. It is inappropriate to triage many of these cases through a counter terrorism lens when the interventions and support should be situated in a wider programme of care. Whilst incorporation of non-ideologically motivated activity into counter-terrorism strategy may make sense when the terrorism-equivalent harm of the Southport attack is considered, it is challenging conceptually and combines a broader cohort of vulnerable individuals with those on a suspected trajectory towards terrorism. Furthermore, it presents a barrier to the effective operation of the system, with implications for the successful identification and triage of potentially risky behaviour.

The Prevent apparatus ends up managing individuals like Rudakubana by default, not because they fit within their remit but due to the absence of alternative frameworks to address safeguarding in the context of violence prevention. Accordingly, practitioners are left unable to effectively intervene when individuals exhibit warning signs of engaging with mass violence driven by personal grievance, social isolation or psychological susceptibilities. This gap highlights the need both for more effective integration of existing support structures, and a revised strategy to counter serious violence which is connected to, but disaggregated from, counter-terrorism measures.

Operationally there is also a clear gap – a framework set up to tackle terrorism is struggling to address non-ideological risks. In particular, key barriers and challenges posed by the incorporation of non-ideological cases into Prevent include:

- An overburdening of the system with over-referral of non-counter-terrorism cases,
- A dilution of the core focus of the project due to these cases,
- The risk of stigmatising people as potential terrorists,
- The risk that individuals may be emboldened by the label of 'potential terrorist'.

JOINING UP EXISTING CROSS-GOVERNMENT WORK

At a national level, addressing this type of violence will require the close collaboration of numerous government departments, with robust political oversight. A structure for cross-sectoral strategic response should include extremism, community cohesion, health and social care, education, international affairs, digital regulation, intelligence and law enforcement. The growing intersection of violence and women and girls (VAWG) and misogynist violent extremism, as well as the increase of extreme misogyny as a standalone violent extremist

motivating factor, further points to the need for a joined up cross-harm approach. This should include increased information-sharing and co-working between VAWG, counter-extremism and broader violence prevention efforts. The interplay of this spectrum of harms makes countering extremism, particularly online, central to the government's 'Safer Streets' mission. Effective early intervention to support young and isolated people with poor mental health has the strong potential to have downstream impact on violence prevention. Similarly, addressing the mainstreaming of misogyny will not only improve the health of society more broadly but also have a downstream impact on reducing misogyny-related violent extremism.

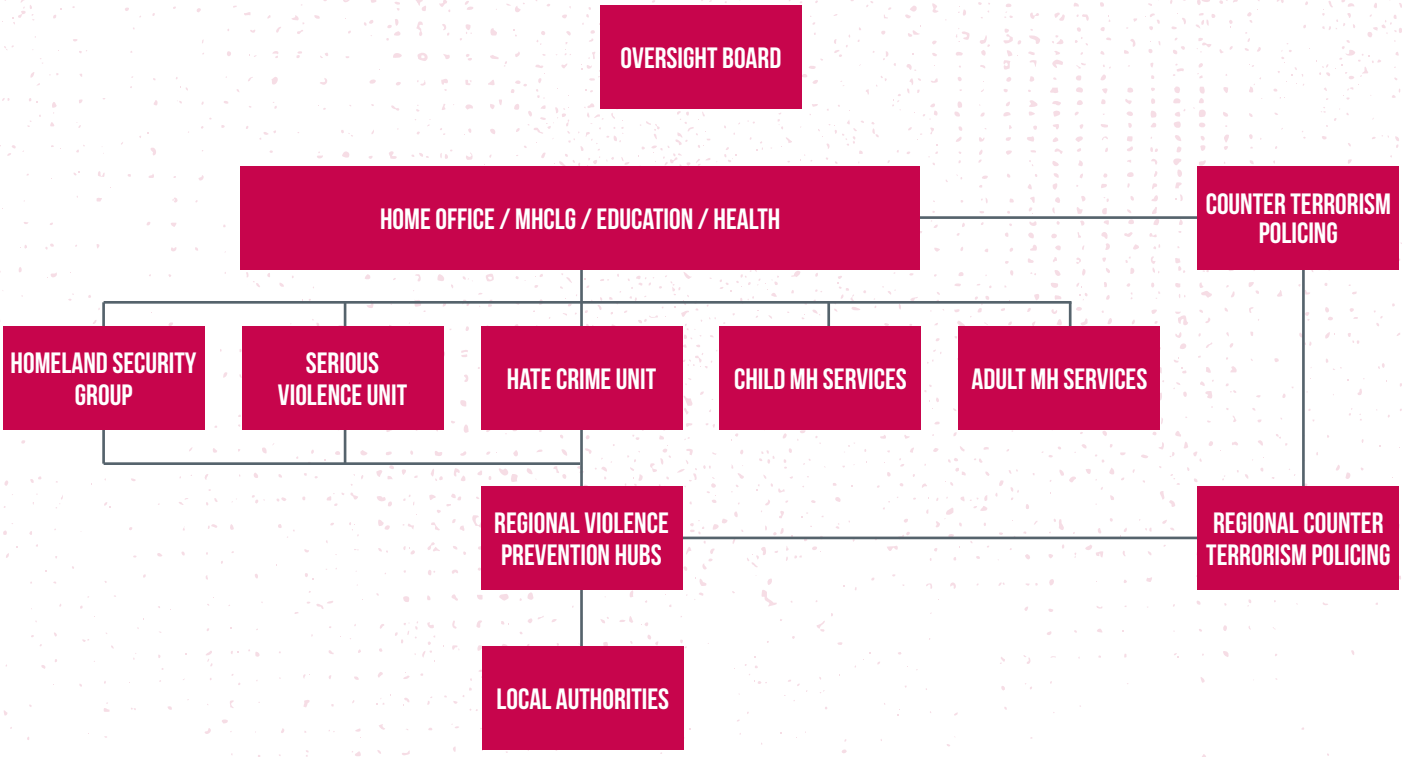
Concerns over funding restrictions need not be a barrier to an overhaul of this nature – all the structures exist already in one form or another. What is needed is a sophisticated plan for knitting them together, with a policy oversight board unifying all stakeholders and strong Ministerial direction and interest that retains a 'hand on the wheel' of this programme of work.

MIRRORING NATIONAL STRATEGIES IN LOCAL STRUCTURES

Integration of local authority safeguarding boards (often called a Multi Agency Safeguarding Hub or MASH) with Channel boards would ensure that all safeguarding cases are dealt with by a unified body capable of determining the best intervention for a young person. By incorporating Channel into the broader safeguarding system, cases can be triaged to the most appropriate support (i.e. mental health services, social care or counter-radicalisation interventions). In many local authorities, Channel will already be involved with other safeguarding responsibilities; this makes it a natural fit which also guarantees wider safeguarding duties can be effectively cross-pollinated with Prevent's counter-terrorism expertise.

Additionally, local authority Prevent Oversight Boards and Serious Violence Boards should be integrated with Community Safety Partnerships, providing regular updates on local risk, threats and programme delivery. These overarching partnerships already understand that no single agency can tackle crime and anti-social behaviour. They unite police, fire and rescue authorities, local authorities, health partners, and probation services with senior oversight to deliver hyper-localised strategies tailored to the needs of their communities. This will become more pressing with the continued regionalisation of Prevent. As Prevent Coordinators lose central government funding in many areas and the portfolio is subsumed into broader community safety responsibilities, local authorities require closer collaboration between intersecting responses on hate crime, serious violence and radicalisation.

Figure 6: A potential model for greater cross-departmental collaboration at both national and local levels.



The Strong Cities Network – an international network of more than 200 cities hosted by ISD, including Manchester, Leeds and London – has piloted promising models for such national-local cooperation. Strong Cities' local prevention frameworks provide a model for local government, practitioners and communities to co-create evidence-based responses to local challenges, including developing strategies for mitigating the impact of online harms fuelling real-world violence at a local level. Local action planning and risk assessment approaches can engage a broad range of local stakeholders including youth engagement services, local education committees, children and family services, social workers, religious institutions, local businesses, community policing teams and local councils.

PREVENTION AND INTERVENTION

PUBLIC HEALTH APPROACH

ISD has long advocated for a 'public health' model for curbing extremist violence. Rather than focusing narrowly on addressing ideologies driving violent engagement – which would struggle to capture the contemporary threat landscape outlined above – a public health approach focuses on behaviours, minimising risk factors while boosting protective factors. Such an approach serves to strengthen individuals and communities holistically, building resilience and reducing the opportunities for extremists to leverage grievances or social challenges. Its strengths include a non-securitised, ideology-agnostic approach which offers the flexibility needed to adapt to new forms of extremism.

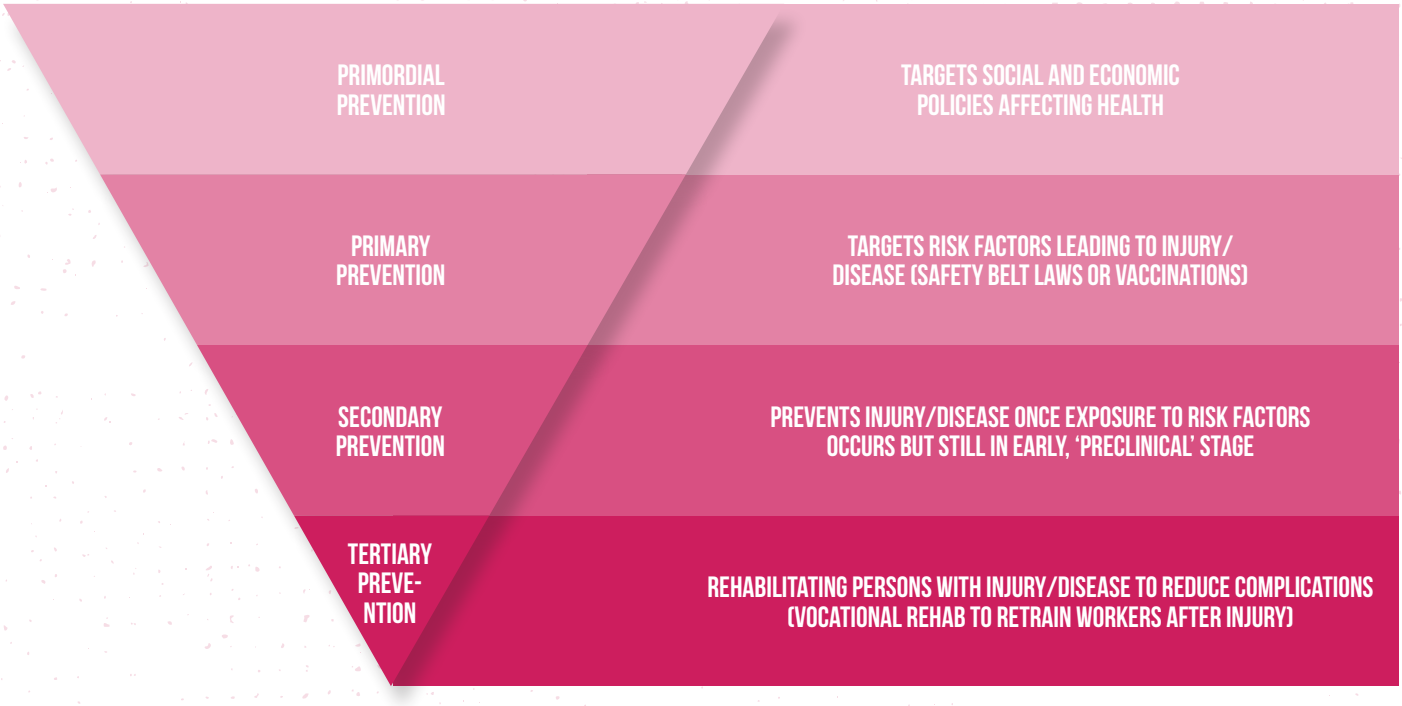
Increasing cross-department cooperation – including between the Department for Education (DfE), Department of Health and Social Care (DHSC) and the Home Office – framed around a common public health mission would provide an efficient way to leverage existing programming, rather than recreating prevention systems from the ground up. Rather than seeking to expand counter-extremism to stretch across all parts of government, such an effort should instead be framed around addressing the intrinsic interplay between healthier societies and violence reduction.

The public health approach is framed around three main tiers of prevention programming:

- Primary or primordial prevention to build healthy societies with resilience to extremism,
- Secondary prevention to interrupt the growth of extremism and provide targeted interventions for vulnerable individuals,
- Tertiary prevention to mitigate the impacts of extremism and engage with those who have become involved in harmful movements.

Primary prevention incorporates resilience-building initiatives such as digital citizenship and media literacy, as well as youth engagement programming to foster resilience. To future-proof against new forms of extremism, and enhance critical thinking more broadly, such programming should look not to teach not what to think, but how to understand harmful or manipulative

Figure 7: Visualisation of the public health model of prevention (David Eisenman, 2016, National Academies of Sciences).



behaviours and strategies. Pre-bunking and inoculation strategies have also been successful in building resilience among young people towards the forms of online harm they are likely to encounter.

Secondary prevention focuses on interrupting the spread of extremist ideas or targeting interventions to support vulnerable individuals. This includes the provision of support services to offramp those at risk, as well targeted messaging aimed at delegitimising extremist ideas and providing positive alternatives.

Tertiary prevention looks to mitigate the impacts of extremism and reintegrate its perpetrators into society. Here it is crucial that wrap-around services aimed at mitigating extremism threats should be sufficiently integrated with broader violence prevention at a local level to mirror the contemporary landscape of risk factors common to both phenomena.

LEARNING FROM STRATEGIC COMMUNICATION EFFORTS

Strategic communications programmes aimed at countering new forms of extremism should learn the lessons from previous generations of efforts to undermine extremist narratives. This means campaigns not just building tailored and appropriate messages but ensuring that they are being delivered by the most effective messenger. Historically, when delivered by the wrong conduit, counter-messaging campaigns have been ineffectual and have even backfired. For innovative counter-messaging campaigns targeting emergent forms of extremism, such as the Manosphere, relevant influencers may for example include sports clubs or gaming influencers. ISD's Campaign Toolkit provides a framework for developing impactful campaigns, and has developed insights on credible messengers for online engagement with extremist communities.

Considering new forms of extremism which are driven by aesthetics, memes and subcultures rather than specific groups, ecosystem level interventions are likely required which look to disrupt extremist communities across interconnected mainstream and fringe platforms. Interventions which harness coalitions of volunteers and allies – such as the EU-wide campaign group Ich bin heir – have proven effective models for mobilising broad communities for coordinated counter-speech across platforms.

EDUCATION AND YOUTH ENGAGEMENT

ISD's decade-plus experience of youth engagement programming shows the value of providing young people with the skills, agency and opportunities to engage with their peers on their own terms when designing responses to extremism. To understand young people's experiences and insights, New Zealand and Australia have recently set up Youth Advisory Panels to inform youth radicalisation efforts. These working groups keep up to date with issues impacting young people and the efficacy and appropriateness of counter-measures. Ofcom similarly consulted children on their children's safety codes. The UK should also look to systematically engage youth perspectives to ensure policymaking and law enforcement is fit for purpose for evolving threats to young people.

Given the spread of new and traditional forms of extremism across society, education-based prevention programmes should be scaled not just for young people but also among adults. ISD's Business Council for Democracy has had significant success in Germany by harnessing workplaces as opportunities for engaging adults around citizenship education and democracy protection, including around emerging extremism risks, providing a scalable model for adult-focused prevention programming.

THE NEED FOR ROBUST SAFEGUARDING APPROACHES

The unique and diverse set of threats posed by Com networks demand targeted interventions, rather than bolt-ons to existing counter-extremism programming or policies. Non-ideological threats, by nature, cannot be addressed by policies and programmes focused on ideological disengagement. Instead, primary and tertiary prevention will be crucial focal points for building awareness and bridging victims to support services respectively. Given Com network participants' commonly self-identified mental illness and social isolation, addressing underlying vulnerabilities should focus on community-based interventions. Strong linkages with grooming or other forms of manipulation demand bespoke, expert safeguarding support for the children involved. The spread of harms emanating from Com networks demand strong multi-agency collaboration at both a national and local level. This should include both those typically involved in Channel panels, but also integrate expertise from anti-grooming, child abuse, and VAWG sectors.

ISD analysis suggests that lack of ideological motivations can shorten the timeline to violence, with aesthetics and memes spreading quicker than complex ideological doctrine, providing fewer opportunities for intervention. Public awareness communications both to at-risk communities and their caregivers should focus on identifying signs of involvement in Com networks and

first-response routes. The March 2025 FBI communication sets out relevant potential indicators and warning signs. Such information should be packaged and communicated to key stakeholders through schools, informal community settings and parent groups, as well as on social media.

There are a number of steps which intervention providers can take to protect the wellbeing and safety of practitioners working to combat new forms of online extremism. Risks could include virtual harassment and threats, exposure to harmful content including potential trauma, and physical threats. This is particularly acute given the proximity of many of these new forms of extremism to deeply traumatic material such as CSAM content. Measures with proven impact in reducing the effects of viewing harmful content include limiting the duration and purpose of viewing, using specific devices, removing audio, reducing screen brightness, isolating text from visual content, turning off auto-play, blurring obscene imagery, accessing professional wellbeing support, and creating peer support communities.

The transnational nature of threats like 764 and Com networks also demands coordinated responses from international governmental partners. Inter-governmental cooperation will be vital to comprehensively address the transnational nature inherent to such new forms of extremism. The UK should look for opportunities to pioneer thought leadership among European and Five Eyes partners facing joint challenges by sharing insights, building collaborative strategies and developing joined-up counter measures around shared emerging threats such as nihilistic violence.

HYBRIDISED EXTREMISM AND DIGITAL REGULATION

Given the centrality of online spaces to the new forms of extremism outlined above, it is of central importance that the UK's emerging regime of social media regulation is effectively designed and enforced in a way that responds to today's extremism challenges, as well as future proofed for emerging extremist threats to online safety. Extremists increasingly toe the line of legal boundaries and platform terms of service, as well as game the algorithmic systems of platforms to engage ever wider audiences. Traditional digital policy approaches rooted solely in content removal of illegal terrorist material from proscribed groups are clearly unfit to respond to the hybridised threat landscape we face today.

In this context, digital regulation must be framed around opportunities for addressing the full lifecycle of online harms related to extremism. This includes mitigating digital technology's harmful role in production (such as the use of Generative AI for extremist propaganda), distribution (including the algorithmic architectures of platforms), and consumption (the exposure of vulnerable individuals to harmful content). This will require a highly targeted approach to balancing efforts that address the proliferation of illegal content, regulation geared towards dealing with distortive platform systems artificially amplifying harmful (but potentially legal) extremist content, as well as efforts specifically focused on risks to minors.

As the UK's social media regulator, Ofcom's enforcement of the Online Safety Act (OSA) provides an opportunity to ensure more systemic approaches to platform regulation, rooted in effective risk assessment and safety-by-design rather than simply removing illegal or harmful content. Specifically, extremism adjacent threats like 'Com networks' are likely to cut across different elements of the new regulatory Codes of Practice introduced by Ofcom. This includes child safety duties and corresponding Protection of Children Codes – which require platforms to take proportionate measures to protect children from accessing harmful material – as well as duties requiring proportionate measures to protect users from illegal content, including terrorism and child sexual exploitation and abuse content. It will be crucial that the efficacy of these codes in addressing new extremism challenges is assessed to ensure such threats are not falling between gaps.

The prominence of alternative platforms within the extremist ecosystems outlined above means it is essential that Ofcom is effectively resourced to deal with a longer tail of smaller platforms, which are increasingly seeing platform migration and displacement effects from larger social media sites. While the OSA enables Ofcom to assess the effectiveness of the efforts of certain larger, higher-risk social media platforms ('Category 1' services) in enforcing their own Terms of Service, it is not clear whether smaller or medium-sized (but nonetheless high risk) platforms such as Telegram will meet the proposed user number thresholds. Telegram has a track record of failing to moderate extremely harmful, violent and often illegal material, either by design or lack of capacity to respond to the challenge. While there are positive initial signs from Ofcom (such as the standing up of a 'small but risky taskforce') it is vital that such platforms are also a key focus of Ofcom's efforts to enforce the OSA, using the full range of powers available to them where platforms refuse to engage or cooperate fully.

Finally, effective transparency is the sine qua non for systematically understanding the evolution of these online threats, interrogating how platform systems are serving to amplify harmful content, as well as scrutinising the efficacy of platform responses and the impacts of regulation. Having been omitted from the original OSA, provisions for legally mandated platform data access for researchers have been included within the Data Use (and Access) Bill which recently received Royal Assent. However, the Act does not set a clear timeline for implementation. With Ofcom recently issuing options for researcher data access, it crucial the government ensures a swift timeline for the development and implementation of a suitable data access regime to ensure the necessary independent scrutiny of online platforms. Until then, UK citizens will be more in the dark to digital threats to safety and national security than their EU counterparts, which has already seen major strides towards systematic transparency under the provisions of the Digital Services Act.

CONCLUSION

The July 2025 'Lessons from Prevent' report investigated how the murders of Sir David Amess MP and three girls at a Southport dance class slipped through the net of a system designed to protect them. With the increasing diversification of violent threats facing the UK, it is insufficient for policy responses to simply bolt on new threats to a counter-terrorism apparatus which, 20 years after its inception in the pre-social media age, is struggling to handle a qualitatively distinct landscape of threats, such as nihilistic violence.

This policy paper has proposed a vision for a response framework geared towards the spectrum of different forms of extreme violence and their associated harms, often motivated and mobilised in similar online environments. Rather than being framed as the build out of expensive new infrastructure, this can present a proportionate and cost-effective means of re-calibrating and knitting together existing policies and programmes.

Together with our recommendations for how the UK's digital regulation can respond to the full lifecycle of extremism-related harms, we envision a collaborative system which protects the UK both on- and offline, with the safeguarding of rights and democracy at its core.

As we approach the one year anniversary of the horrific Southport attack, we remember the victims of such extreme violence and consider opportunities to policymakers to take the necessary bold steps required for making our national prevention infrastructure fit-for-purpose.

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Washington DC

www.isdglobal.org