

Violence-Fixated Individuals

The effectiveness of current laws, systems and orders

17 September 2026



Agenda

An Introduction to Tech Against Terrorism

- Background
- Our Work
- Our Partners
- Our 2026 Roadmap

Threat Landscape

- Communities, Platforms, Networks
- Tactics, Techniques, Procedures
- Case Study

Regulatory Challenges

- Status of Violent Content
- Comparison with Australia
- Fragmentation of Responsibility

Shaping Responses to VFIs

- Early Assessment
- Challenge Behaviour before Ideology
- Joined-Up Approaches

An Introduction

01



Background

Our work emerged from UN SCR 2129 in 2013, and we have since been referenced in three UN Security Council Resolutions

RESOLUTION 2129 (2013)

Notes the evolving nexus between terrorism and the internet and directs UN CTED to help address this through connecting in consultation with the private sector.

RESOLUTION 2617 (2021)

Recognising the efforts of Tech Against Terrorism initiative to foster collaboration between tech industry, governments, academia and civil society.

RESOLUTION 2354 (2017)

Mandates UN CTED to review developments globally in countering terrorist narratives and recommend ways for Member States regarding capacity building to enhance their efforts in the field of counter terrorism.

SECURITY COUNCIL DELHI DECLARATION (2022)

Recognising Tech Against Terrorism for disrupting the 'ability to use the Internet in furtherance of terrorist purposes, while also respecting human rights and fundamental freedoms.'

PRST6 (APRIL 2017)

Security Council proposal for a comprehensive international framework to counter terrorist narratives - describing Tech Against Terrorism as good practice.

RESOLUTION 2713 (2024)

Encourages UNCTED to work with initiatives such as Tech Against Terrorism to support the government of Somalia disrupt Al-Shabaab terrorist activities online.

MEMORANDUM OF UNDERSTANDING (JUNE 2025)

Provides for close cooperation between CTED and Tech Against Terrorism in technical areas set forth in Security Council resolutions on counter-terrorism, especially those which address the misuse of information and communications technologies and other emerging technologies for terrorist purposes.

Our Partners

We focus on supporting our partners via open-source intelligence and technological developments used to disrupt terrorist use of the internet



Big Tech



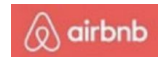
State-led activity



Civil society, Academia, Counter-speech

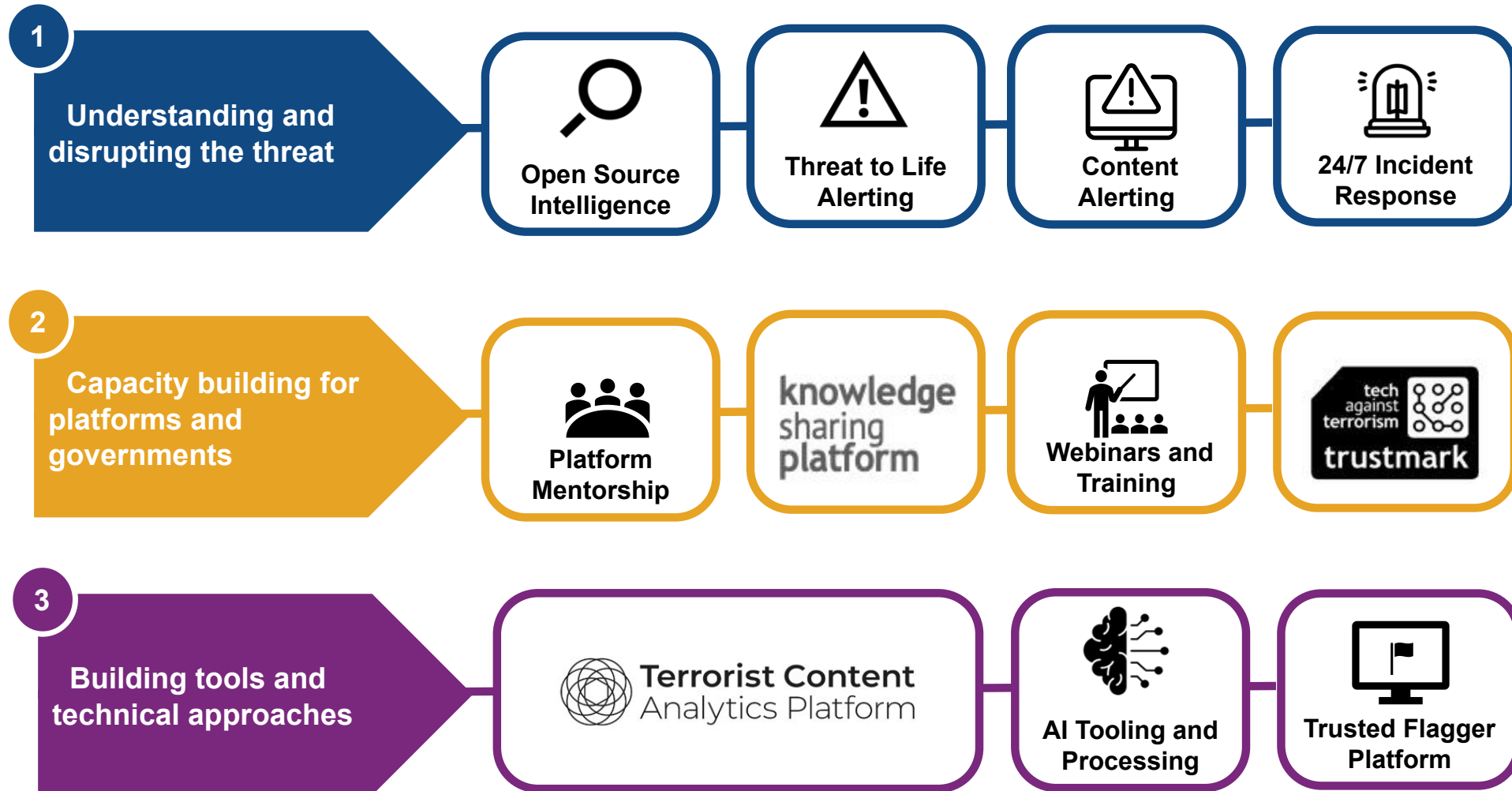


Mentorship of smaller tech platforms



Our Work

We aim to disrupt the terrorist use of the internet through understanding terrorist activity online, intervening, developing technology, and building capacity with governments and tech companies



Our Work

Our OSINT team monitors TVE entities from across the ideological spectrum



Violent Islamist Groups

Violent Islamist terrorist groups remain among the most prolific producers of online propaganda, generating thousands of pieces of content daily across social media, file-sharing, and encrypted messaging platforms.

Platform enforcement is inconsistent, and no single actor has the capacity to address the threat at scale.



Extreme Right Wing Groups

Extreme Right Wing ecosystems rely heavily on Telegram, TikTok, and self-operated websites to disseminate propaganda, glorify violence, and build transnational communities.

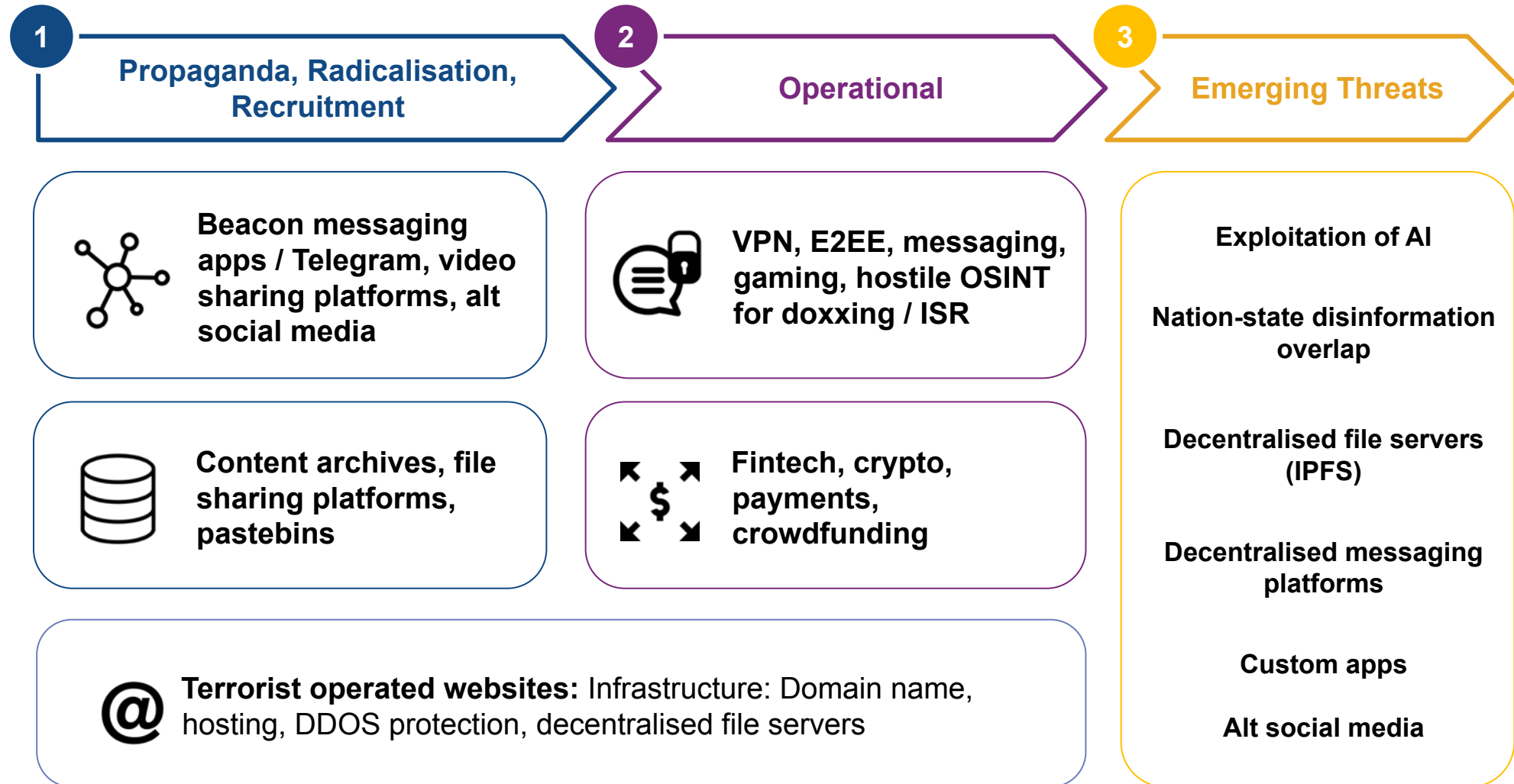


Nihilistic Violent Extremist

Nihilist violent extremist milieus linked to the True Crime Community and the COM network primarily use Tumblr and TikTok (TCC), and Discord, Roblox, and TikTok (COM) as key spaces for networking, recruitment, and content sharing.

These groups poses a distinct challenge: the decentralised structure and lack of formal ideology complicate detection and disruption.

There are a multitude of strategic and operational objectives driving the terrorist use of the internet



We deliver real-world impact through a mission-driven approach to countering terrorist use of the internet

Mission: Saving lives by disrupting the terrorist use of the internet

2025 Achievements

- Incident Response Team triaged 5,000+ potential terrorist incidents with real-time analysis
- Issued 20+ threat-to-life alerts to law enforcement; over 50% resulted in active investigations
- TCAP reported tens of thousands of verified terrorist content pieces (IS, Al Qaeda, Al Shabaab)
- Shared hashes and URLs with major technology companies; majority of content subsequently removed

Emerging Threats in 2026

- High-volume terrorist activity persists across major platforms
- Radicalisation accelerating; self-radicalised threat actors likely to increase
- State-sponsored amplification of extremism creating new threat nexus (e.g. HAYI)
- AI agentic capabilities emerging - automated orchestration, content production, and dissemination at scale

2026 Priorities

- Expand TCAP AI real-time archiving and discovery capabilities
- Deepen AI engagement with frontier model providers to prevent terrorist exploitation
- Launch the CT-AI Benchmark
- Increase efforts to investigate and identify radicalisation pathways to improve early-warning detection
- Build AI-assisted content classification partnerships with technology companies

Terrorist Content Analytics Platform

The Terrorist Content Analytics Platform (TCAP) plays a leading role in disrupting terrorist exploitation of the internet by supporting our analysts in discovering, archiving, hashing, and alerting terrorist content to platforms

84,312

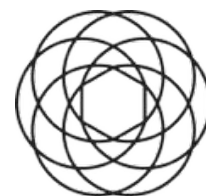
URLs submitted

304

platforms alerted

56,432

files in the archive



Terrorist Content Analytics Platform

Tier	Terrorist entity	Source	Date	Status
Designation	Jama'at Nusrat al-Islam wal Muslimin (JNIM)	Facebook	 Submitted: 20/04/2026, 16:09:00	Pending

Tier	Terrorist entity	Source	Date	Status
Promotional	Islamic State (IS)	TikTok	Submitted: 20/04/2026, 10:24:40	Pending

Tier	Crisis	Source	Crisis Status	Date	Status
Crisis	Buffalo 2022	TikTok	Historical	 Submitted: 20/04/2026, 10:22:26	Pending

Threat Landscape

02



Key Online Communities, Networks, Subcultures and Ecosystems

While these networks are fluid and adaptive, the wider VFI ecosystem is shaped and sustained by a number of core, interconnected groups.

The True Crime Community

A broad online ecosystem centered on true crime content and communities. At its most extreme, it fosters fascination with perpetrators, normalises violence, and contributes to the glorification of mass attackers, creating pathways into wider networks that celebrate, justify, or encourage harmful behaviour.

The Com Network

A decentralised adaptive ecosystem intersecting multiple violent subcultures. Characterised by fluid affiliations, shared aesthetics, and recurring themes of nihilism and performance-based violence. Core groups include Order of the Nine Angles, No Lives Matter, Maniac Murder Cult, 764 and many new generation and splinter networks.

Gore focused ecosystems

Online environments where graphic violence, injury, death, or bloodshed is a central feature of the content, discussion, or shared identity.

Violence-fixated individuals

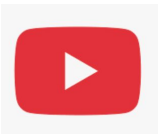
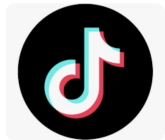
Individuals whose behaviour is characterised by an obsessive preoccupation with violence and attackers. The defining feature is behavioural fixation rather than formal extremist ideology.

Platform Ecosystems

Nihilistic violent extremism (NVE) does not exist on a single platform. Instead, it operates through an interconnected ecosystem of platforms, each serving a different function, with users and content continuously moving between them.

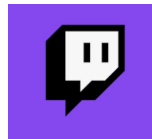
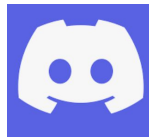
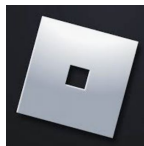
Social Media

Purpose: Discovery, amplification, networking, and propaganda dissemination



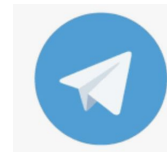
Gaming Ecosystems

Purpose: Community formation, socialisation, and networking, gamified content



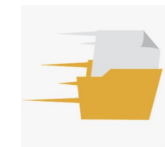
Decentralised & Encrypted

Purpose: Resilience, operational security, and content preservation



Hosting, Archival & File Sharing

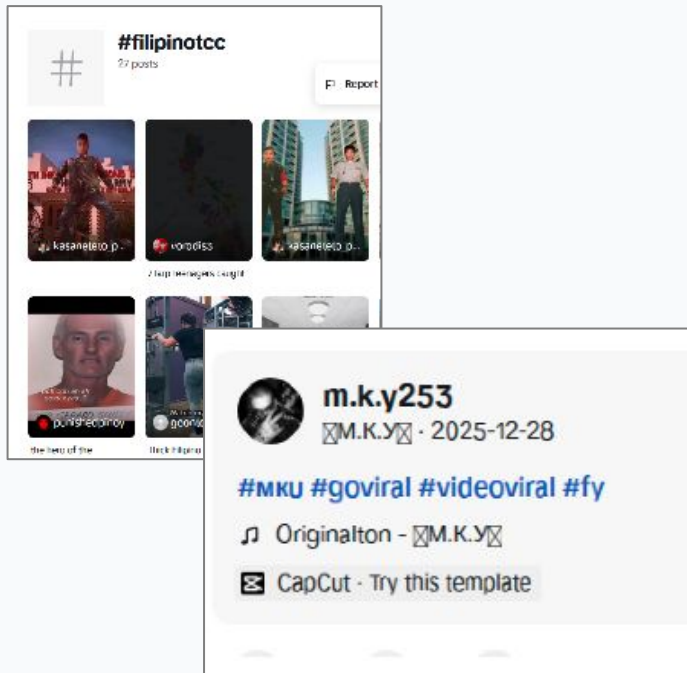
Purpose: Storage, circulation, preservation, and downstream dissemination of removed or extreme material



Key Tactics, Techniques, and Procedures

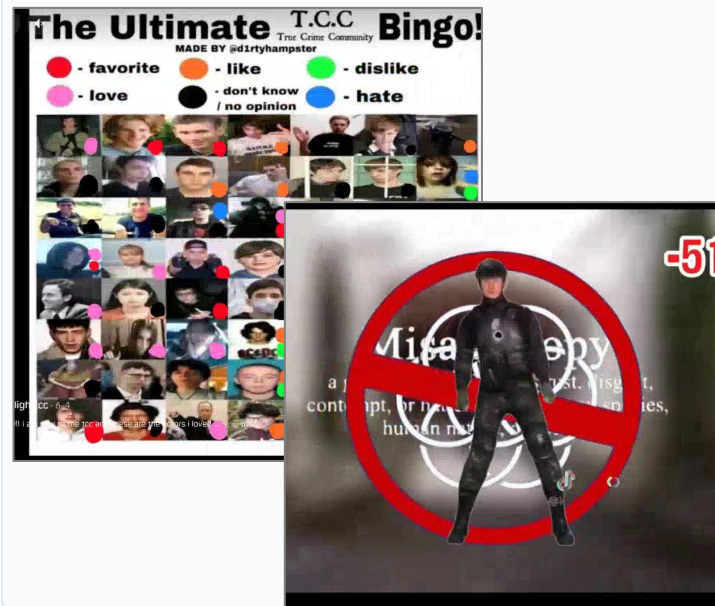
Signalling and algorithmic push

Exploitation of platform features and engagement mechanics to amplify reach, increase visibility, and circumvent moderation through coordinated signalling and adaptation.



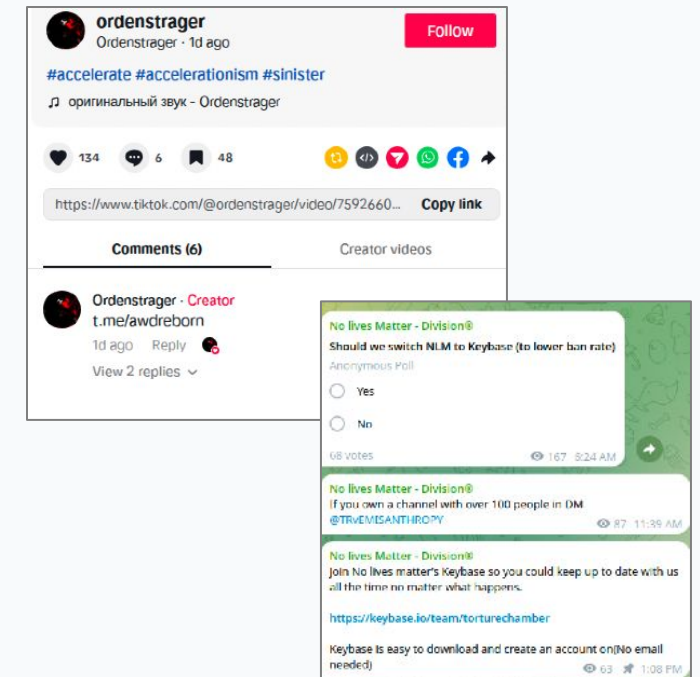
User generated content

The creation and circulation of customised media serves to aestheticise violence-supportive narratives, strengthen in-group identity, and reinforce community cohesion. By incorporating memes, humour, irony, and gamified elements, content becomes more accessible, shareable, and engaging for participants.

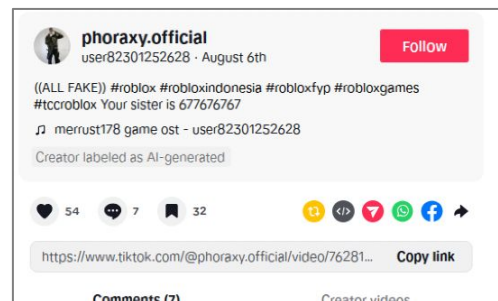
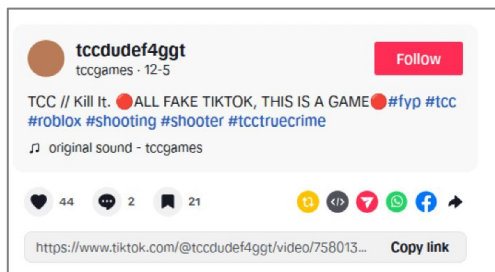
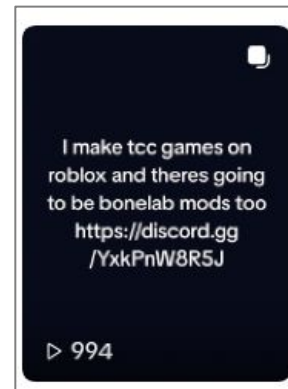
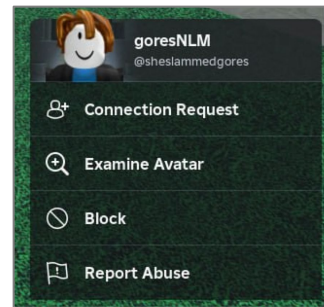
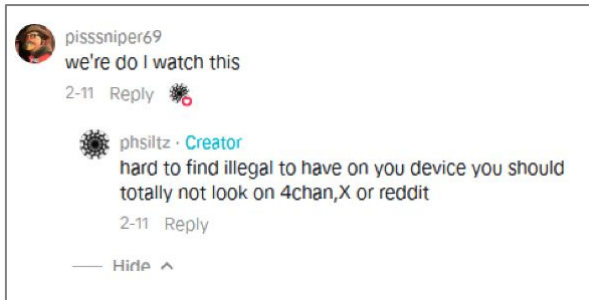
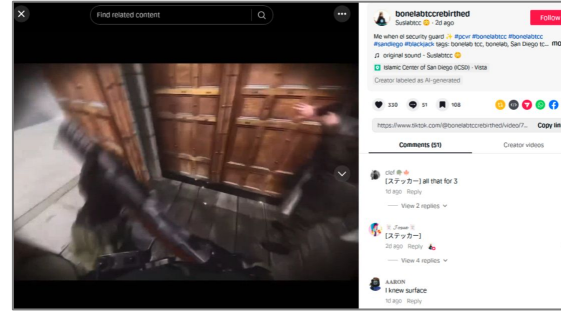


Cross platform activity

The ecosystem relies on fluid cross-platform movement, with outlinking facilitating the transfer of users, content, and engagement between multiple services.



Gamified Pathways to Exposure



Challenge: VFI content is frequently embedded within interactive online environments.

- Exposure can happen through gamified formats, not just text or images
- Ideological messages are folded into gameplay, teamwork, and competition
- Content may feel like entertainment rather than propaganda.
- Repeated exposure can occur without deliberate intent
- This normalises contact with NVE-aligned narratives

Case Study: Construction of the “Kadenholic” Network

764 Terror

764 is officially back under REAL ownership by kadenholic himself, all the previous ones are larp'd, riley's, woken's, auora etc etc, we are here to stay and promise to fulfill our wishes, kadenholic and us are here again to rule com of an iron fist and cause as much havoc we can, p terror to com and outside com, and again anyone kadenholic will feel it either u are ext com, dox o AE etc, no one is safe.

HOLIC

since i have the power to run multiple groups at once i'll be releasing my own group called "holic" the very first letter only ext/dox group in com, i wasn't planning on releasing it but been seeing hella people repping holic and begging me to join it, so here we go, the terror begins.

Identity Construction and Persona Development

- Developed a highly recognisable online persona centered on the "kadenholic" identity
- Leveraged shock content, controversy, and claims of harmful activity to generate attention and notoriety
- Cultivated an exaggerated image of power and influence despite limited verifiable offline authority



kadenholic's victim

extortedpup

22 Following 378 Followers 4987 Likes

Follow

Message



@kadenholic little victim ^_^
2 owners
tiktok im 19

Telegram

kadenholic kids

@evilgroomer



VIEW CHANNEL

1985 edited 10:18 AM

Community Building

- Followers adopted "kadenholic" branding, fan accounts, and community identifiers such as "kadenholic kids"
- Supporter and impersonation accounts amplified the persona across platforms
- Community identity increasingly centered on the individual rather than the broader network or ideology

kadenholic kids

list isn't even released yet and their already fighting over me 🤔🤔
<https://t.me/holicplayroom>

Telegram

HOLIC playroom
JOIN IN CASE OF TERM @cutsignholic
@cutsignholic for stages
no nsfw...



VIEW GROUP



7

1279 kade..., edited

kadenholic kids

kid #2 (kadenholic's loli) promoted to kid #1 surpassing kadenholic's pup (pup got sent to a mental hospital on the first day so i was waiting for someone to surpass her so i can drop the list)



12

1213 kade..., edited 12:45 AM

Digital Authority

- Influence was derived primarily from online reputation, visibility, and perceived status
- Exclusivity, follower engagement, and claims of harmful behaviour reinforced authority and legitimacy
- The persona became a focal point for recognition, loyalty, and behavioral influence within the community

Broader Harm Profile Beyond Ideology

[764]

764 is coming back,
once again,
ready to show terror.

~X~ REQUIREMENTS

<> BLOOD CONTENT:

<> 2 // 3 // PIECES:

<> CUTSIGNS (DEEP CUTS);
<> BLOODSIGNS;

MUST INCLUDE!!!

- Your alias + LACK/ GUNSHOT
- 764 OR the SYMBOL
- MUST show cuts + record videos horizontally & vertically

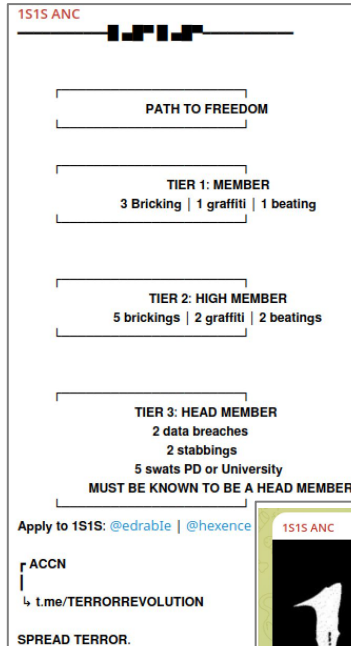
<> SUICIDES.

<> IRL CONTENT:

<> 2 // 1 // 2 // 3 PIECES:

<> BRICKING (must show 1 piece of a bloodsign, applies to graffiti as well.)
<> ARSON
<> STABBING
<> GRAFFITI

DM us with content READY!

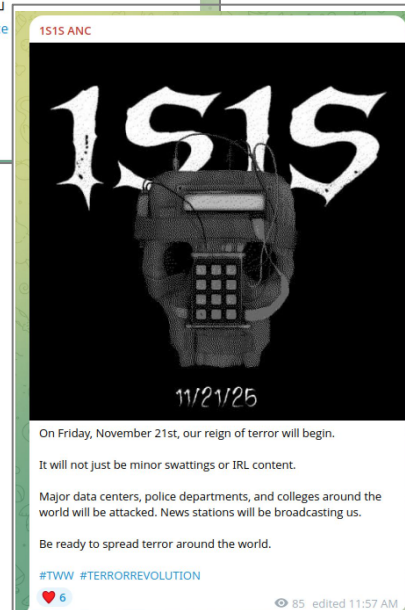


When Extremists Go Technical: NVE–Pro-Iranian Hactivist Convergence

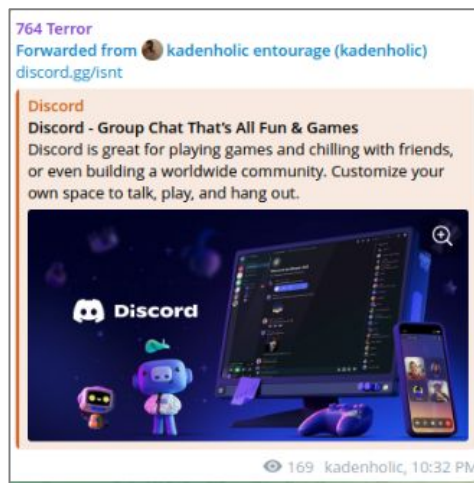
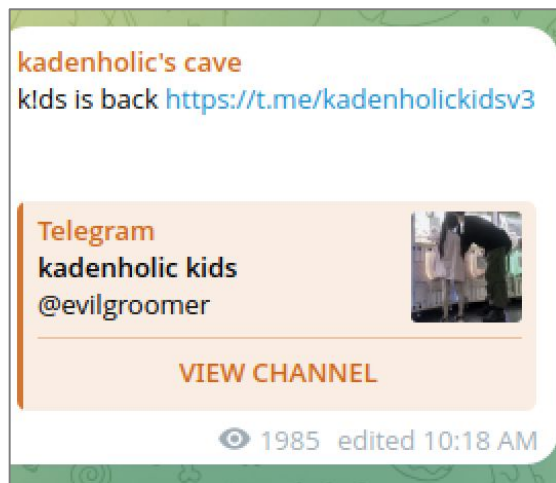
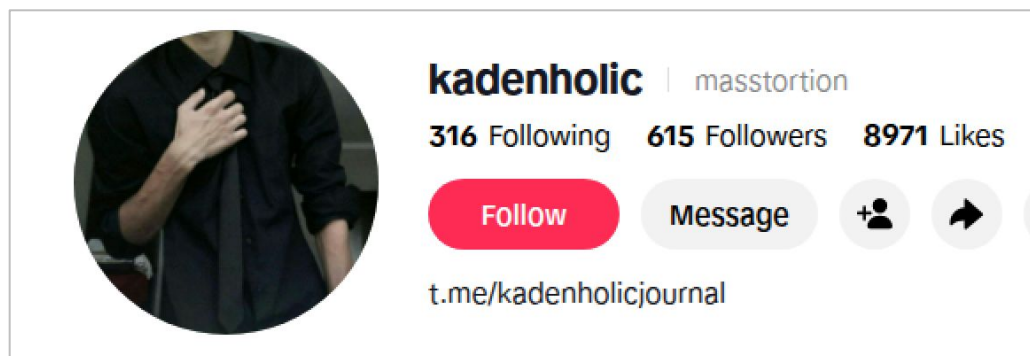
How NVE actors are building ties with pro-Iranian hactivist and Islamist extremist ecosystems on Telegram—creating new pathways between ideology, access, and capability.

Challenge: Diversified harm profile requires response beyond terrorism-specific frameworks

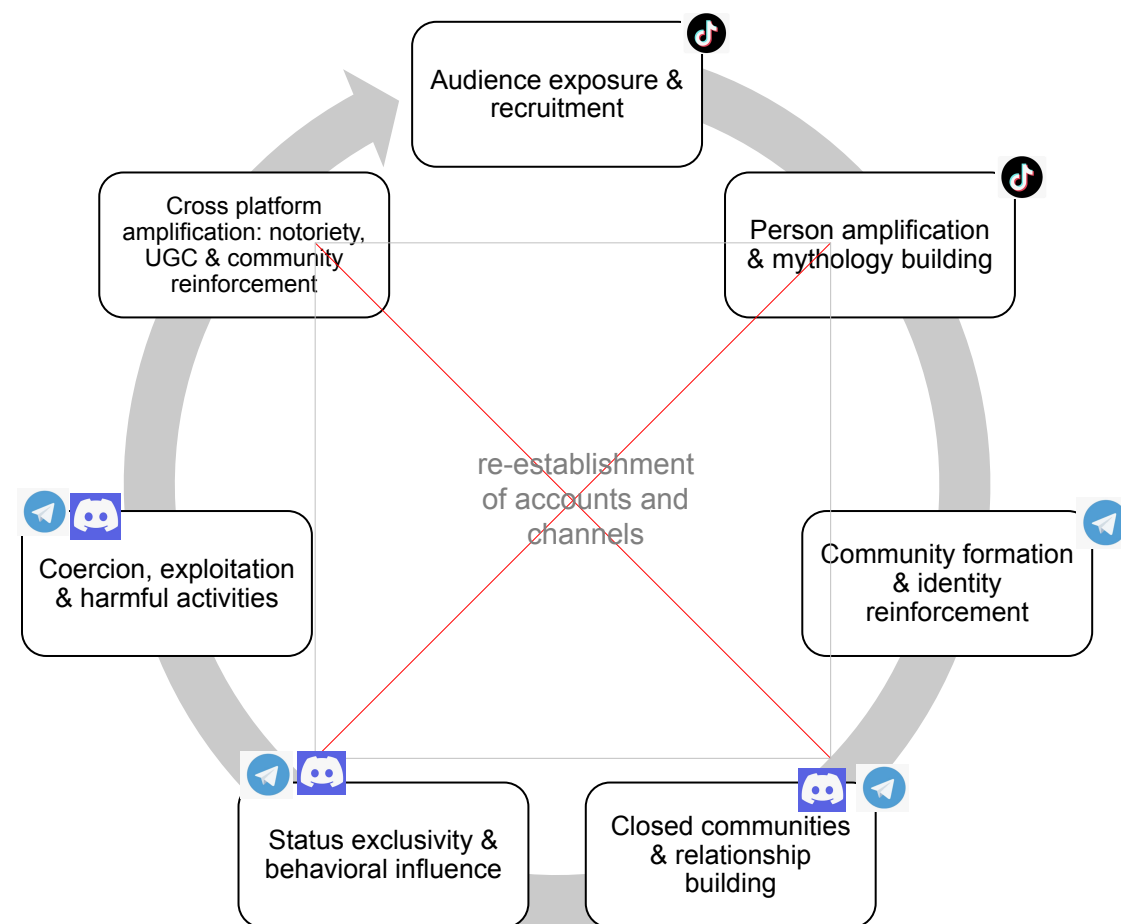
- **VFI is associated with a broad spectrum of harms.** It can overlap with harassment, child exploitation, self-harm, animal cruelty, cyber-enabled abuse, and other forms of online and offline harm that extend beyond ideologically motivated violence.
- **Individuals may occupy both victim and perpetrator roles.** Those involved in VFI ecosystems can be vulnerable to exploitation, coercion, and harm while simultaneously engaging in harmful behaviors towards others, creating complex safeguarding and intervention challenges.
- **Prevention requires a wider safeguarding response.** Effective interventions must combine safeguarding, mental health support, victim protection, and behavioral risk management rather than relying solely on counter-terrorism approaches.



Case Study: Operationalisation of Influence



Cross-platform ecosystems facilitated a progressive user journey from open exposure to increasingly closed and controlled environments, while account migration and platform redundancy ensured continuity despite moderation and enforcement actions.



Regulatory Challenges

03



CSAM & TVEC are priority illegal harms for all users, but violent content is not

	Users under 18	Users 18 and over
ILLEGAL CONTENT DUTIES Section 59 and Schedules 5 to 7		
Terrorism content Priority offence, Schedule 5	Must be prevented and removed for all users, regardless of age	
Child sexual abuse material Priority offence, Schedule 6	Must be prevented and removed for all users, regardless of age	
CHILDREN'S SAFETY DUTIES Section 62		
Violent content Legal but harmful, not an offence in itself	Risk must be mitigated on services likely to be accessed by children	No duty to restrict or remove

Age assurance changes who can see violent content. It does not change the obligation on terrorism content or CSAM, which must be kept off the service for everyone.

The position in Australia is significantly more advantageous

	Users under 18	Users 18 and over
CLASS 1 MATERIAL, REFUSED CLASSIFICATION Removal notice, 24 hours to comply		
Terrorism material Advocating or instructing in terrorism	Must be removed for all users, regardless of age	
Child sexual exploitation material Reported to the Australian Federal Police	Must be removed for all users, regardless of age	
Gratuitous violent material Including abhorrent violent conduct	Must be removed for all users, regardless of age	
CLASS 2 MATERIAL, R18+ AND X18+ Removal or restricted access system		
High impact violence Below the Class 1 threshold	Must be removed or placed behind age assurance	May remain behind age assurance

Classification, not harm tiers Scope follows the National Classification Scheme rather than a list of offences plus a children's tier.	Complaint led, content level eSafety issues notices on named URLs, alongside industry codes and the Basic Online Safety Expectations.	Under 16s off social media The social media minimum age framework started on 10 December 2025.
--	---	--

There is a philosophical difference between UK and AUS approaches

	United Kingdom Online Safety Act 2023, offence based	Australia Online Safety Act 2021, taxonomy based
Test applied	Does the content amount to a criminal offence	Would the material be refused or restricted classification
Source of the categories	Priority offences in Schedules 5 to 7, plus any other offence with a victim	Classes drawn from the National Classification Scheme for film, games and publications
Judgement a platform makes	Reasonable grounds to infer the elements of the offence, including intent and available defences	What the material depicts and how strongly, judged against descriptive impact categories
Effect on violent material	Outside the illegal content duties unless it meets a separate offence	Inside the highest class where gratuitous, or where it depicts abhorrent violent conduct
Where it strains	Harm that Parliament has not criminalised falls out of scope for adults	Category boundaries are contested, as the Wakeley litigation showed

Offence based scope moves with the criminal law and gives platforms a defensible test. Taxonomic scope reaches harm the criminal law has not, and pays for it in argument about where the categories end.

The UK test displaces the responsibility to adjudicate illegality and complicates the test for doing so

United Kingdom Reasonable grounds to infer that content amounts to a terrorism offence

- 01 Which offence could this content amount to
- 02 Is the organisation proscribed, and under which jurisdiction
- 03 Does the conduct fit encouragement, dissemination or glorification
- 04 Can intent or recklessness be inferred from what is visible
- 05 Would a defence apply, such as reasonable excuse, journalism or research
- 06 Does a news publisher or free expression protection attach
- 07 On the information reasonably available, are there reasonable grounds to infer

Seven judgements per item, at volume, in seconds, with no disclosure, no evidence from the poster and no hearing.

Australia Classification categories

ONE QUESTION

Is this material restricted

Class 1, refused classification, remove

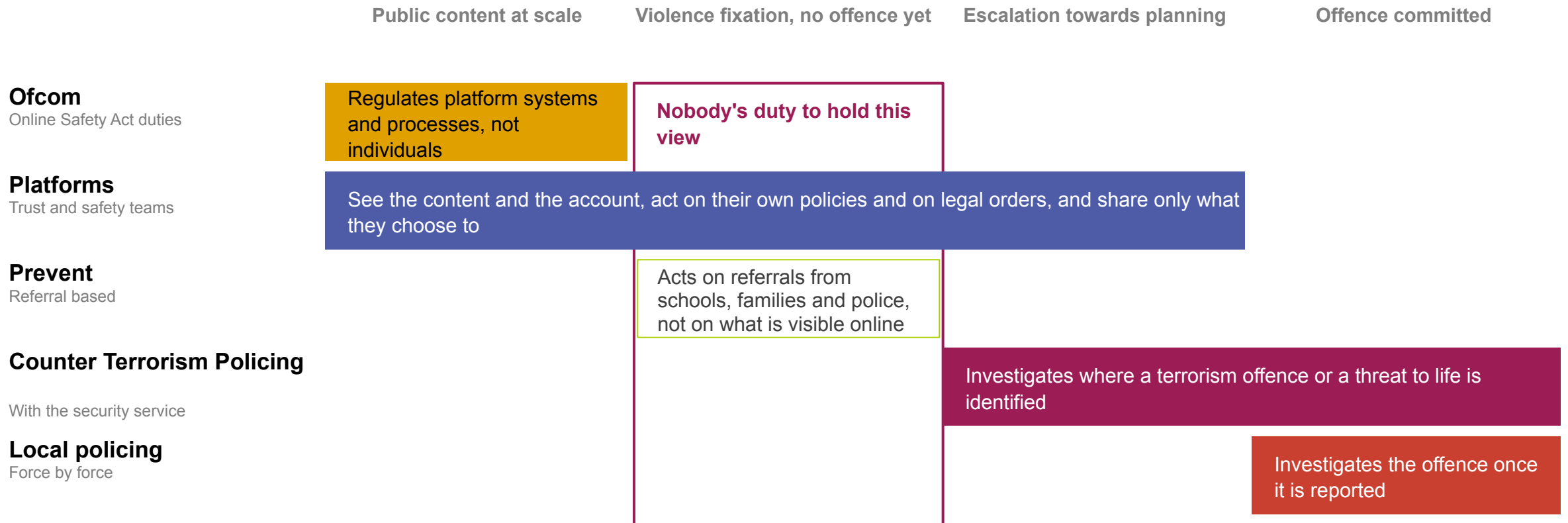
Class 2, R18+ or X18+, restrict access

Neither, leave in place

No offence to construct, no mental element to infer, no defence to weigh. The category is published and eSafety holds the call.

The UK test hands a private moderator a conclusion the criminal courts reach with evidence, disclosure and a defence. Penalties fall on leaving content up, not on taking it down, so the platform's safe answer is removal and the adjudication of illegality moves off the state.

The UK's present fragmentation of responsibility



The regulator looks at systems, the police need an offence, and Prevent needs a referral. Assessing surface web violence fixation as a risk picture is nobody's statutory job.

An avenue for reforming the Online Safety Act

THE TEST TODAY

Map the material onto an existing offence, then infer intent

Violent content sits in section 62 as priority content harmful to children, so the all-user duties reach it only through terrorism, public order or incitement offences.

THE TEST WITH THE PROPOSED OFFENCE

Does this material glorify, trivialise or normalise serious violence

National Security Bill, King's Speech, 13 May 2026. A named offence can be added to the priority list by regulations, which is what carries violent content into the illegal content duties.

01

Duties for every user

Illegal content duties do not turn on age assurance, or on whether a service is likely to be accessed by children.

02

Systems, not takedown requests

Risk assessment, proportionate design measures and the illegal content codes, including hash matching, would apply.

03

One threshold across platforms

Ofcom enforces a single standard with comparable transparency, instead of variation policy by policy.

04

A route for the VFI picture

Publicly visible glorification of violence gains a named offence, so what is observed has somewhere to be referred.

The gain depends on the drafting. Glorifies, trivialises or normalises is wider than anything now in the illegal content duties, so the public interest and journalistic protections promised alongside it will decide whether the test is administrable at scale.

Platforms must be encouraged / compelled to be more transparent

THE COMPLIANCE CYCLE

01 Material posted in public view

02 Detected under the platform's own risk assessment

03 Removed to discharge the duty

04 Compliance shown by following the code

05 Footprint gone, nothing referred on

The platform

Throughout

Sees the account, the network, the recommendation history and the context, at every stage

Ofcom

Systems and processes

Sees the risk assessment the platform wrote, and the record of the process it followed

Police, Prevent, researchers

Outside the regime

Sees only what is public, and only until removal

Understanding is blocked

Prevalence, growth and network shape can be measured only from inside. Removal deletes the observable record before anyone else has counted it.

Disruption is blocked

Identity, continuity across accounts and behavioural history stay with the platform, and no duty requires it to pass any of that to anyone.

The Act rewards removing content and documenting the process. Neither obligation produces intelligence about the individual, so a platform can be full compliant while the picture of violence-fixated activity gets harder to see.

Practical Measures

04



Early prevention – upstream education



Focus: Building resilience before radicalisation takes hold

Prioritise early prevention: Apply layered violence-prevention measures grounded in public health principles, focusing on reducing risk factors before they escalate into crises.

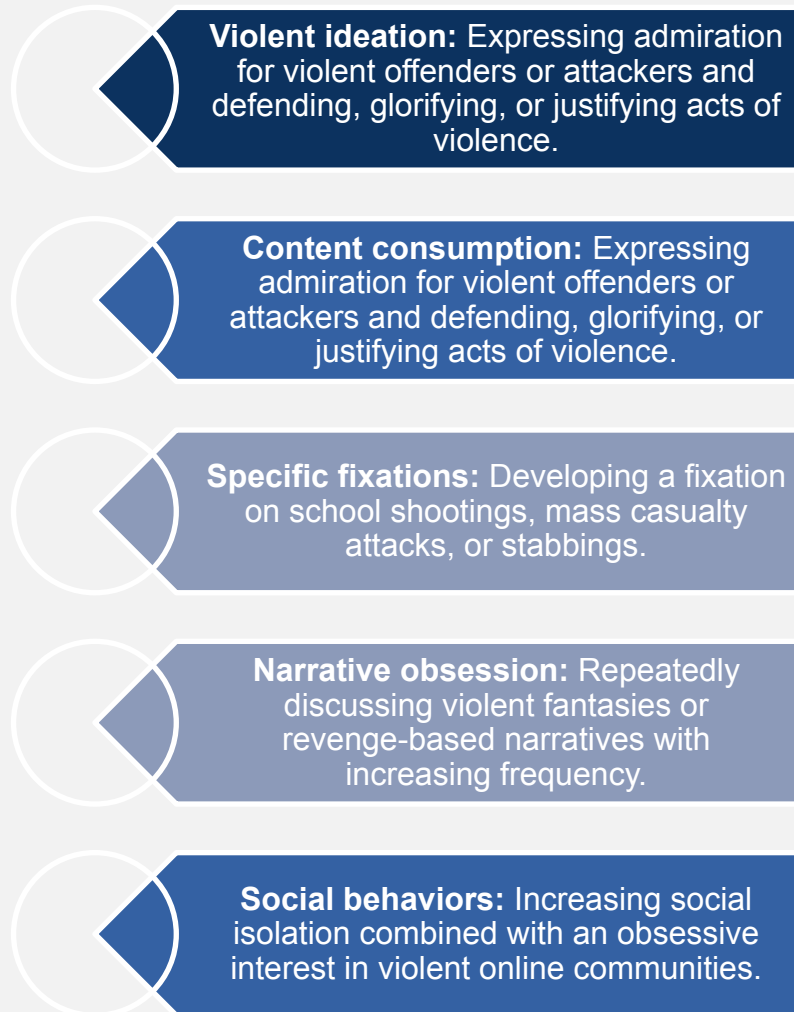
Strengthen resilience through education: Deliver learning programmes that build critical thinking, digital literacy, and emotional resilience, while using inoculation approaches to prepare young people for exposure to VFI content.

Address rapid escalation pathways: VFI engagement can progress from curiosity to harmful behaviour within days or weeks, making proactive intervention essential.

Use learning as a protective factor: Equip young people with the skills to recognise manipulation, assess online content critically, and discuss grievances in safe and constructive environments.

Provide clear reporting guidance: Establish clear thresholds and pathways for reporting concerns, helping frontline practitioners, educators, and families respond confidently and consistently.

Assess risk through behaviour, not ideology



Focus: Replace ideology-focused models with behaviour indicator systems

Adopt behaviour-focused risk assessment: Move beyond ideology-centred frameworks and prioritise models that identify behavioral changes, engagement with violent content, emerging online networks, and indicators of escalating harm.

Monitor behavioral indicators over time: Assess patterns such as social withdrawal, changes in peer groups, altered online activity, fixation on violence, and shifts in identity presentation rather than relying on ideological affiliation alone.

Recognise a broader range of harms: Assessment frameworks should account for links between VFI and behaviors such as harassment, self-harm, child exploitation, animal cruelty, and other forms of violence, rather than focusing solely on terrorism-related risks.

Embed trauma-informed practice: Prioritise approaches that address grievances, vulnerabilities, and underlying trauma, supporting individuals through safeguarding and intervention rather than relying primarily on ideological counter-messaging.

Multi-agency response: cross-sector collaboration & frontline training

Focus: Strengthening multi-agency prevention and early intervention

Respond through coordinated partnerships

Emerging threats such as VFI require a whole-system response, as no single organisation can effectively identify, prevent, and address risks in isolation.

Build a shared prevention framework

Effective prevention depends on collaboration between schools, families, safeguarding, mental health, and community/statutory agencies for a consistent response.

Empower frontline professionals

Teachers, healthcare workers, and practitioners are best placed to recognise behavioral changes and raise concerns before risks escalate.

Invest in specialist training

Professionals need up-to-date knowledge of VFI, online radicalisation, and unclear ideological influences to identify emerging risks with confidence.

Clear referral & safeguarding pathways

Establish clear thresholds for concern and explain referral processes to enable timely and appropriate intervention by trained practitioners.

Platform response: moderation, government partnership & cross-platform coordination

Culture, Slang, and Aesthetics	
Sinister	Term from O9A/Tempel ov Blood culture describing a transgressive, violent or anti-social ethos; widely used across the broader Com Network.
333	Numeric tag that appears in some O9A and Tempel ov Blood materials and in wider Com-network content as an esoteric or in-group marker.
136	Numeric tag used by Temple of Hate.
CVLT	Stylised spelling of cult, commonly used in names of extremist or abuse-oriented online communities.
H3LL	Stylised spelling of hell, often used in usernames, channel names or slogans to convey an edgy or violent brand.
MVRDER	Stylised spelling of murder used in com-aligned usernames, slogans, and channel titles to glorify killing and content moderation
BI00d	Stylised spelling of blood, almost certainly used in content moderation mechanisms. Commonly used in usernames and to refer to bloodwalls/signs.
mvrder4svtvn	MVRDER4SVTVN is an underground heavy/hip-hop and "antimusic" project often shared in com-aligned spaces, particularly MKY content.
моподежькоторауныбаётся	Russian dialect which translates to "youth who phrase commonly used in MKY aligned content.

Group Terminology	
ANNC	Abbreviation for "announcements", often used for channels dedicated to updates and information sharing.
EXT	Abbreviation for extortion, often used in channel or account names to identify as a pro-extortion entity
IRL	In real life, often referring to offline violence
Splinter group	Refers to a new group formed from an existing com-group, typically maintaining ties and alliances with the original group.
Oldgen	Refers to groups and users that were active in the Com ecosystem before roughly 2021.
Midgen	Refers to groups and users that emerged around 2022–2023, between earlier "oldgen" actors and newer entrants.
	Refers to new groups and users.
	A system of points that assesses the status and productivity of each member, most commonly used by entities within MKY. Acts of online and offline violence have different values.

Abuse & Extortion Practices	
Cutsigns	Practice of forcing a victim to cut an <u>extorters</u> or group's name into their own skin; images or videos of the act are often shared in com-aligned spaces, and the practice is used as social currency.
Bloodsigns, Blood wall	Form of coerced content in which a victim is forced to write usernames or group names in blood obtained through self-harm, typically on a wall or visible surface, for documentation and intimidation.
CVTS	Stylised spelling of cuts, typically referring to self-harm wounds featured in Com-aligned propaganda and extortion material.
Cutshows	Livestreamed or recorded sessions in which a victim self-harms under pressure from perpetrators or audiences in Com-aligned spaces.
Fansign	Image or video where a victim holds or displays a message with a group's name, handle or slogan, used as proof of control and for propaganda.
Manhunt	Organised search for a chosen target whom members stalk, attack and sometimes kill, while recording the process as propaganda and proof of action; promoted in NLM "manhunt" guides.

Focus: strong moderation, government collaboration, shared intelligence and fluid network disruption

Shape moderation systems to identify VFI ecosystem patterns by incorporating indicators of moderation evasion, regrouping behavior, coded language, key words, phrases and terms and coordinated account reuse

Work with governments and regulators: Partner with policymakers and regulatory bodies to align safety measures with legal requirements and develop coordinated responses to emerging platform exploitation tactics

Share intelligence on platform exploitation: Provide up-to-date information to platforms so they can maintain current keyword lists and understand how their systems are being misused by VFI networks

Enable cross-platform information sharing: Build coordinated data-sharing mechanisms between platforms to track and target the fluid, shifting nature of decentralised VFI networks that move across multiple sites

Counters multi-platform spread: Platform safety measures need coordination across mainstream sites, encrypted channels, and niche spaces where VFI spreads, using collaborative frameworks for network-wide disruption

Multidisciplinary response: cross-harm integration & disengagement

Focus: Integrating Cyber Crime, Child Sexual Abuse, and Behavioral Units for Disengagement

1. Combine multiple disciplines

Effective disengagement requires integrating expertise across cyber crime, child sexual abuse, behavioral units, and terrorism prevention rather than working in separate silos.

2. Diversified Harm Profile

Since VFI overlaps with harassment, self-injury, and exploitation, prevention needs a broader scope than terrorism-only approaches.

3. Behavioral Unit Insights

Specialised behavioral teams understand violence patterns, risk escalation, and intervention timing beyond ideological motivation.

4. Cross-Sector Partnerships

Strong connections between safeguarding, mental health, and child protection ensure appropriate support before risks grow.

5. Parental Support

Assisting parents in understanding psychological impacts of violent online content creates early intervention opportunities.

An OSINT fusion centre could close the gap by building a single and actionable picture of risk

INPUTS THAT ALREADY EXIST

Surface web collection

Public posts, channels, aggregators and archives

Platform signals

Referrals, transparency data and researcher access

Regulatory findings

Ofcom risk assessments and enforcement evidence

Public reporting

Schools, families, civil society and hotlines

ONE STANDING FUNCTION

OSINT fusion centre

Standing capability, not a case queue

Collects from open sources at scale

Assesses against one shared taxonomy

Triages to the body able to act

Reports trends and gaps in scope

WHAT THAT MAKES POSSIBLE

One picture, continuously held

Violence fixation in public view is assessed as a standing risk picture rather than one referral at a time.

Warning before an offence

Communities, aggregators and imitation patterns surface while intervention is still available.

Nothing falls between remits

Cases route to Prevent, Counter Terrorism Policing or platform action against a recorded threshold.

Evidence back to the regulator

Systemic findings support Ofcom enforcement and give platforms signals they can act on.

The gap is not a shortage of data. The material is public. What is missing is a body with the remit to collect it, assess it against one standard, and pass to whoever can act.

THANK YOU

Adam Hadley

Executive Director

adam@techagainstterrorism.org



For more information on our products
and services visit our website

techagainstterrorism.org