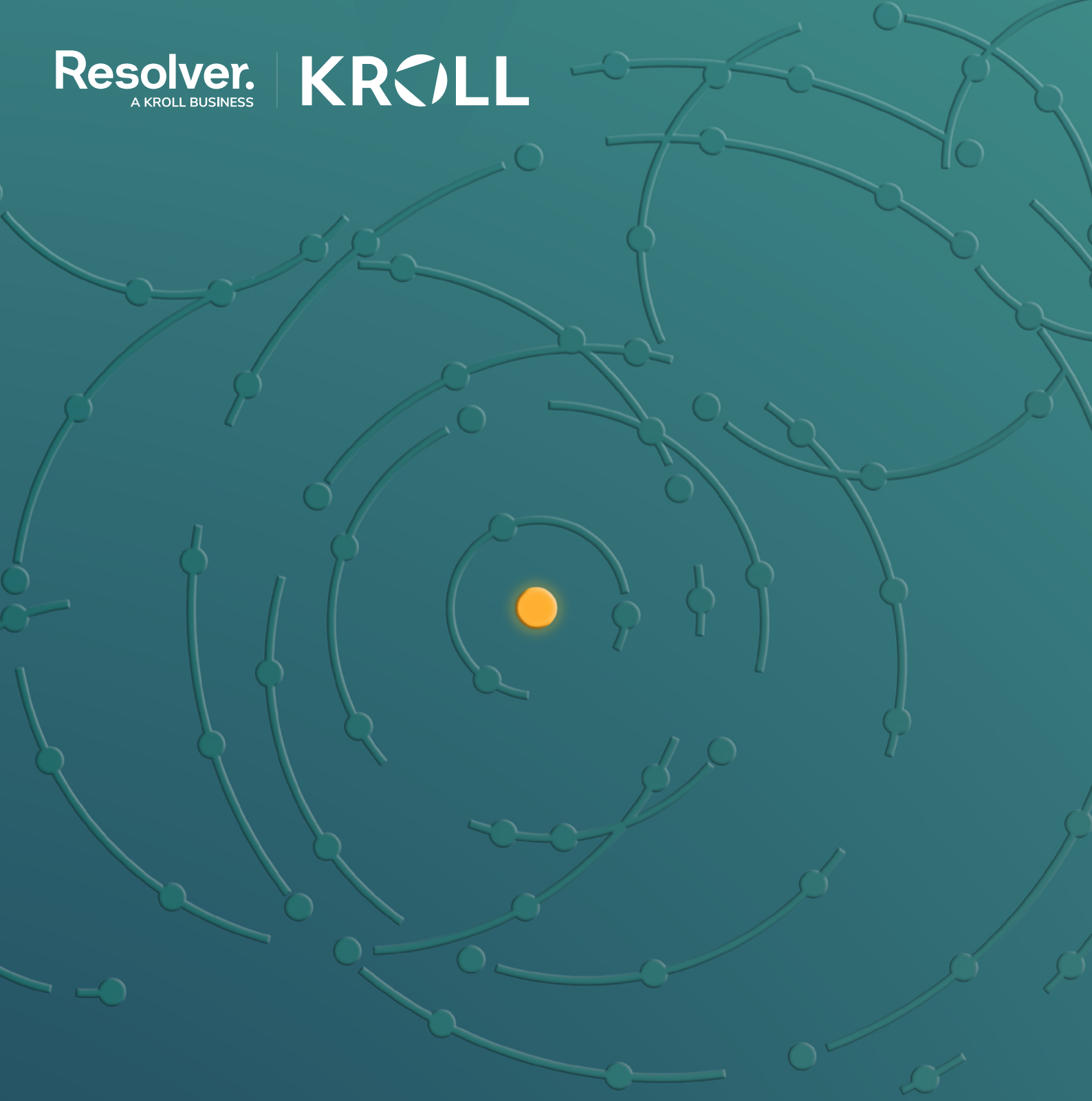
Resolver. A KROLL BUSINESS | KROLL



Critical Harm Intelligence Briefing

WEAPONISED LONELINESS

Table of Contents

CONTENT WARNING

This report details multi-faceted harms including (but not limited to) Child Sexual Exploitation and Abuse (CSEA), self-harm and suicide, hate speech, harassment, violent extremism and graphic violence.

In reading this report, please prioritise your own psychological safety and wellbeing.

Exeuctive Summary

Weaponised Loneliness: A Critical Harm Intelligence Briefing

Executive summary

For several years, Resolver has investigated an increasingly hybrid and global threat. This phenomenon is commonly referred to as the 'Com' amidst many other names. Throughout this report, we refer to the threat subject as 'the Com' for consistency. This label is necessary yet imperfect. It provides a shared way to describe activity that is, in practice, fragmented: a loose but sprawling ecosystem of overlapping internet cultures, subcultures, behaviours, networks, groups and claimed ideologies, within a sprawling ecosystem of harm.

This report examines a decentralised and evolving harm ecosystem that different authorities describe in different ways. The Federal Bureau of Investigation and Public Safety Canada classify elements of this activity as 'nihilistic violent extremism'. The UK's National Crime Agency and Australia's Federal Police have used the term 'sadistic (online) exploitation'. NGOs, technology platforms and other stakeholders in the Trust and Safety community reference 'sadistic harm networks' and 'hybridised threats'.

These distinctions reflect not only attempts to describe the underlying harms, but also the different legal, operational and policy levers available to those responsible for detection, safeguarding, investigation and prosecution.

For Resolver, the specific terminology matters less than recognising a shared reality: the harms facing children* are increasingly hybrid, interconnected and global. Our intelligence indicates that a wide range of adverse childhood experiences and vulnerabilities contribute to patterns of exploitation affecting children and young people at a global scale. These harms do not follow a single pathway, nor do they arise from a single ideology or structure. They emerge through complex, multi-layered dynamics, including the deliberate exploitation of isolation and social vulnerability.

This work is informed by long-standing exposure to how these patterns unfold over time, including the consequences of delayed recognition, the role of power dynamics and clout, fragmented responsibility and inconsistent safeguards. Weaponised loneliness is one contributing factor within this broader threat landscape, rather than a singular or exclusive cause**.

It is our hope that this report supports further collaboration among those with the power and responsibility to protect children worldwide. Our work and that of our partners, continues every day. We thank readers not only for their attention, but for the actions they choose to take in strengthening the global response to this hybrid threat.

**While Resolver's current investigations typically focus on the sadistic and extremist elements of the Com, especially activity targeting children, we recognise that targets vary and elements also include a focus on older individuals.*

***Resolver supports partners to intervene by disrupting pathways to harm and enabling earlier risk identification, particularly where children and vulnerable individuals are targeted. Where this report uses the term 'loneliness', it refers specifically to the deliberate exploitation of isolation and related vulnerabilities as tactical threat vectors within a harm ecosystem, rather than to broader psychological causation.*

Industry position and policy considerations

Based on this intelligence, we identify three priority areas where coordinated policy, operational and regulatory approaches are required across the Trust and Safety ecosystem:

1. Create and strengthen hybrid threat response structures.

2. Promote and enhance proactive signal sharing at local and global levels.

3. Resource and enable trauma-informed support and effective sign-posting.

Intelligence basis

These priorities are informed by consistent patterns observed across Resolver's intelligence:

- Individuals involved in the Com often pursue power and infamy through the perpetration of extreme harms within semi-hierarchical, clout-based social systems spanning multiple online environments.
- These subcultures fracture and re-form within a decentralised, metastasising threat landscape across what we describe as a tripolar spectrum, defying attempts to categorise or define them neatly.
- Psychological, sexual and physical harms are global in scope and escalate at speed, sometimes in a matter of hours, days and weeks.
- There are recurring patterns in the targeting of young girls combined with a concerning decrease in victim, survivor and perpetrator ages worldwide.

Systemic challenges

Across the Trust & Safety ecosystem, several systemic constraints continue to limit current responses:

- Limited efficacy of traditional, siloed investigative and detection approaches
- Group markers, language and risk signals in constant evolution
- Lack of coordinated reporting mechanisms and signal-sharing interoperability
- Significant wellbeing challenges for professionals engaged in addressing this threat

These constraints reinforce the need for coordinated, cross-sector approaches rather than isolated interventions.

About Resolver

Resolver, a Kroll business, has over 20 years of experience in the Trust and Safety sector, delivering global intelligence, technology and advisory services to partners worldwide.

Resolver works with online platforms, technology providers, NGOs, governments and regulators to identify and mitigate a wide range of online harms, including child exploitation, violent extremism, hate speech, graphic violence, suicide and self-harm, and illicit monetisation.

Resolver combines large-scale technology with expert human analysis to assess risk signals, contextual factors and the multi-faceted human impact of online harms. We are founding members of, participate in, and champion a range of sector initiatives focused on online safety, including the WeProtect Global Alliance and the Online Safety Tech Industry Association.

www.resolver.com/trust-and-safety

Acknowledgements

We thank Resolver's analysts and subject matter experts for the discreet, committed work they undertake every day in addressing these threats and the broader Resolver team for supporting the production and dissemination of this report.

We also thank the dozens of global experts and practitioner community consulted during the research, drafting and review process, including contributors from platforms, regulators, law enforcement, NGOs, academia, psychology and related fields, who continue to play a critical role in mitigating harm across this landscape.

Our sincere thanks to the following named organisations, and many more who assisted this work:

Authority for the prevention of online Terrorist Content and Child Sexual Abuse Material

CATS Centre for Abuse Trauma and Suicide Studies

Middlesex University London

Ofcom making communications work for everyone

CHILDLIGHT Global Child Safety Institute

CHRISTCHURCH CALL to eliminate terrorist & violent extremist content online

ICDE Institute for Countering Digital Extremism

INHOPE

IWF Internet Watch Foundation — Working together to stop child sexual abuse online

Molly Rose Foundation

AVYS

With additional acknowledgment to:

NSPCC

Roblox

Tech Coalition

DETAILED BRIEFING

UNDERSTANDING THE COM

Report context

Resolver generally does not publicly share intelligence research and analysis (with the notable exception of our contributions to previous WeProtect Global Threat Assessments). There are good reasons for this, given the sensitivity of our work. However, based on the findings of this report, we believe the severe nature of hybrid threats to children warrants a public warning and clear recommendations for action.

In Resolver's first public Critical Harm Intelligence Briefing we are warning of a threat that is pervasive across the internet. This threat spans child sexual exploitation and abuse (CSEA), suicide encouragement and self-harm, graphic violence exposure, severe harassment, hate speech, extremist ideation and more.

Uniquely, it cuts across the full scope of work undertaken by all of Resolver's specialised intelligence teams. The material we review in these cases is among the most severe we encounter and represents significant trauma to children, families and many others affected.

In this report, individual online platforms and services are not named. This is a conscious choice, for one key reason. Wherever children gather and play, in person as much as online, predators and threat actors attempt to engage with them. We must address this threat in all its forms, in all places. The harms we detail are ecosystem-wide. Few online spaces are entirely unaffected.

We focus on the risk signals and pathways that lead to widespread harms. This is where critical intervention and prevention opportunities arise. We share extracts from our ongoing, global intelligence analysis about the tactics, techniques and procedures, the human traits and behaviours of those exploiting children worldwide.

Resolver does not hold, nor seeks to hold, primacy on expertise in this hybrid threat. Many others are doing vital work tracking the publicly available data on arrests and prosecutions, undertaking prevention work, conducting deep-dives into selected elements and producing guides for parents and more. We seek to add to this Resolver's intelligence analysis and assessments, to contribute our perspective as a global organisation supporting partners to protect children online.

It is important that this report does not risk leading any child to the threat we warn of. For this reason, we do not disclose specific current threat community names or related named trends. We provide further details to specific trusted parties. Resolver reports high-risk content, behaviours, individuals, groups and networks directly to impacted platforms and, where appropriate, to law enforcement.

Global recommendations

In the course of our day-to-day work, Resolver is asked to make safety recommendations to the platforms and regulators we support. In this briefing, we set out systemic recommendations that could most directly impact the online threat, based on our intelligence picture.

These recommendations are specific to online Trust and Safety interventions, Resolver's core operating area and are by definition about upstream preventative measures. It is for others across the ecosystem to interpret this report and inform their own recommendations and policy positions. This may relate to content discoverability, the extent to which this threat is adequately covered in global regulations, or the strength of existing law enforcement referral mechanisms.

The threat we face targets the most vulnerable in society. In some cases, it draws vulnerable individuals into perpetrating harm themselves by exploiting fundamental insecurities and imposing perverse power dynamics. Communities weigh, measure and trade extreme harms for social clout, allowing the threat to sustain and accelerate. Whether described as sadistic exploitation, nihilistic violent extremism, or the Com, this hybrid threat demands a consistent child protection lens.

This informs our recommendations for the Trust and Safety community:

1. **Create and strengthen hybrid threat response structures:** Addressing this threat more effectively requires situating expertise together across child safety, self-harm, graphic content (gore), violent extremism and cyber-crime, beyond current siloes. Policies, processes, technologies and teams should adapt and collaborate accordingly. This applies equally to technology platforms advancing their defenses and to law enforcement task forces, regulators, legislative efforts and public policy professionals.
2. **Promote and enhance proactive signal sharing on a local and global level:** Early intervention depends on clear, permissive legal, policy, privacy and regulatory frameworks established and aligned worldwide. These frameworks must support timely action to intervene early, protect children and act before harm materialises. No single stakeholder holds all the information required to respond. AI and other forms of automated risk detection play a critical role, but it is trusted frameworks that permit and facilitate the sharing of high-risk signals that will make a meaningful structural difference to immediate preventative action.
3. **Resource and enable trauma-informed support and effective signposting:** The many pathways into this threat can be interrupted and addressed more effectively through stronger foundational sign-posting to online support, before children are harmed. Not all engagement carries equal risk and particular consideration must be given to the most vulnerable, while respecting agency and the fundamental importance of children's rights, including the protection of their online access. In tandem, additional materials and support for caregivers and parents will be vital to aid discovery, prevention and safeguarding.

Understanding the Com

The Community ('Com') is a global online ecosystem associated with extreme forms of cyber-bullying, exploitation, violence, crime, and abuse. Evidence from law enforcement investigations and Resolver's proprietary intelligence work indicates that it is largely composed of young people aged 11–25. The severity of harms linked to the Com, combined with the young and often vulnerable profile of those who engage with it, makes this one of the most pressing challenges for child protection, public safety and countering online harms.

Resolver works closely with technology, social and gaming platforms, as well as the wider online safety community, to disrupt Com-related activity that exploits platforms and their users. In consultation with key stakeholders, this report aims to contribute to a shared understanding of the drivers, dynamics and behaviours associated with the Com, to support the development of coordinated and multi-layered responses.

To cut through the complexity of this threat, our analysis is grounded in three core factors that shape how individuals enter, engage with and are retained within the Com ecosystem.

Motivations and pathways to entry: Effective intervention depends on understanding why children and young people are pushed and pulled into the Com. Engagement is rarely accidental and follows identifiable pathways shaped by social, psychological and environmental pressures. These pathways are driven by a combination of push factors that increase vulnerability, such as social isolation, emotional distress and lack of support, as well as pull factors that attract engagement, including validation, belonging, attention and perceived status.

Many of those who engage with the Com have suffered adverse childhood experiences, perceive themselves as socially excluded, or have been subject to extreme bullying. They are often in search of connection, community, or elevating their social status.

A common denominator within many pathways is loneliness. It functions both as a driver towards participation in egregious harm and criminality and as a point of leverage exploited by predatory members. Intervention is significantly more effective when it occurs before a child or young person is fully drawn in, particularly in the spaces where initial targeting takes place. As engagement deepens, harm escalates and opportunities for prevention narrow.

Behaviours and tradecraft: Com members engage in a broad and severe spectrum of abuse, exploitation, violence and criminal activity. While different segments of the Com gravitate towards particular behaviours, the ecosystem as a whole shares a common set of tactics, techniques and procedures (TTPs) used to pursue objectives and sustain activity.

These shared behaviours and tradecraft enable consistent patterns of harm and escalation, while also supporting risk detection by Resolver alongside the platforms we support. Understanding these common TTPs is critical to identifying signals early, recognising the complex dynamics within the ecosystem and overlap across subcultures and responding early to threats that may otherwise appear fragmented or isolated.

Platforms, functionalities and exploits: Com members operate across a wide range of mainstream and fringe platforms, as well as sites created by core members and intersecting communities. The intensity and form of online threats vary depending on platform functionalities, user bases and the safeguards put in place. Activity observed on any single platform must therefore be understood as only pixels of a broader

intelligence picture. Seemingly discrete and disparate behaviours or incidents may be considerably more significant when viewed in context, particularly where activity spans multiple platforms, migrates over time, or exploits gaps between systems.

Given the Com's amorphous and evolutionary nature, it defies easy definition. To understand the threat, it is important to set out what the Com is and what it is not:

What the Com is not

Not a unitary group: Com ecosystems exhibit hierarchy through the power dynamics that define relationships between members and their victims, but rarely operate as a unified or centrally coordinated group. Dynamics acting within and across these communities make the ecosystem volatile, competitive and transient.

Members may participate in multiple Com subcultures, move from one to others, or create their own, resulting in a decentralised and metastasising threat landscape. Frequently, harms are perpetrated by individuals who adhere to a given subculture, to individuals whom they target within that subculture directly; this is not exclusively a 'one to many' or 'many to many' threat.

Focusing on single named groups often leads to a misleading understanding of the problem as a whole and conclusions drawn are quickly rendered obsolete as the ecosystem evolves. We cannot proscribe or designate our way entirely out of this harm, though this has a place as a strategy.

Not an ideology: Although broad swathes of the Com have adopted the aesthetic, language and tactics associated with violent extremist ideologies and groups, particularly on the far right, the ideological commitment of its members is often superficial and performative.

Ideologies purportedly adhered to by members of the Com are often used to indoctrinate and coerce recruits and victims and to justify illegal and egregious harmful behaviours. This can include leveraging significant shock value for social status within the ecosystem (clout) and intimidation. Rarely do we see clear and coherent ideological commitment as a behavioural basis.

Not a single risk issue: The Com cannot be understood solely as a violent extremist phenomenon. Its risk profile spans the full spectrum of online harms, often to the most extreme extent observed in our work. This necessitates countermeasures and interventions that take a global view of threats and vulnerabilities fundamentally rooted in child protection.

Not a border-bound phenomenon: Parts of the Com originated in Eastern Europe. The Com now impacts five continents, absorbing and adapting the TTPs, aesthetics, culture and ideological veneer of diverse and global criminal, violent and extremist groups and cultures. The online foundation on which the Com operates enables international membership and participation, with criminal activity stretching across global jurisdictions.

Not a clear separation between perpetrators, victims and survivors: Across the Com, grooming and recruitment often involve participation in progressively more egregious acts involving self-harm, violence, cybercrime and abuse. There are documented cases of victims becoming perpetrators of abuse through coercion, desensitisation or efforts to improve their status within a sub-culture. We do not have the benefit of a binary victim and perpetrator status, adding complexity to interventions and countermeasures deployed.

What the Com is

A transnational threat: The Com has spread across Europe, North America, South America and Oceania. Cases of severe, mass child exploitation employing the tactics, techniques & procedures of the Com have also recently emerged in the Middle East, demonstrating significant global reach.

An online ecosystem that engages offline harm: The Com is a decentralised ecosystem of subcultures with power dynamics and subgroup hierarchies established based on social currency gained through acts of violence, criminality and abuse. The notoriety-driven objective is to cause physical, psychological, or financial harm to their targets.

A melting pot of subcultures: The aesthetic, ideological orientation and behaviours of Com ecosystems branch from a broad range of subcultures that share a common root in misanthropy, nihilism and predation. TTPs used by the Com are similarly adopted from a wide array of criminal and extremist communities. This blending of aesthetics and tradecraft elevates the threat by creating multiple vectors for recruitment and grooming from intersecting communities, enabling further propagation across communities.

Dynamic and evolutionary: The Com ecosystem is in constant evolution, with new subcultures and clusters emerging and fragmenting, often faster than legislation and platform policies can be implemented to counter the threat. The lack of centralised structure and the behaviour-driven nature of the Com are a key driver of its transformation and expansion. It defies existing taxonomies of harm.

Targeting the vulnerable: Especially at sadistic and violent extremist poles of the Com spectrum, the majority of victims are children and young people at heightened vulnerability. These vulnerabilities arise from intersecting factors such as, but not limited to:

- Adverse childhood experiences
- Economic disadvantage
- Disability or health-related marginalisation
- Mental health conditions
- Neurodivergence
- Exclusion linked to racial, cultural, religious or social identity, including LGBTQ+ identity
- Prior history of suicidal ideation, self-harm or abuse

Isolation experienced in these contexts increases vulnerability to coercive and exploitative targeting by the Com. Where individuals have experienced, present, or are exposed to multiple factors, this significantly heightens individual vulnerability to Com exploitation.

Broad spectrum of criminality: The Com presents an expansive risk profile that manifests in the widest and most extreme range of illegal and harmful behaviours, including physical violence, sexual abuse, extortion, psychological manipulation and cybercrime. This is driven by its adaptability, notoriety-based power dynamics rooted in nihilistic and predatory behaviour and the appropriation of diverse extremist ideologies and criminal tactics.

Young people are at the core: What makes the Com an especially egregious risk is that the majority of perpetrators and victims are children and young adults. Interventions to the manifold risks presented by the Com, whether countering violent extremism or preventing suicide and self-harm, must place child protection at the fore to be effective.

The Tripolar Harm Spectrum: mapping the Com ecosystem

The Com ecosystem gravitates between poles on a tripolar spectrum with distinct objectives, digital subcultures and aesthetics. However, the Com as a whole shares a consistent behavioural focus on cybercrime, offline harm, shared tradecraft and the pursuit of personal status and power. Myriad subcultures at the centre of this triangle of harms often act as gateways to the Com. Individual groups are often formed of juvenile offenders seeking online notoriety who may be acutely susceptible to online radicalisation and grooming.

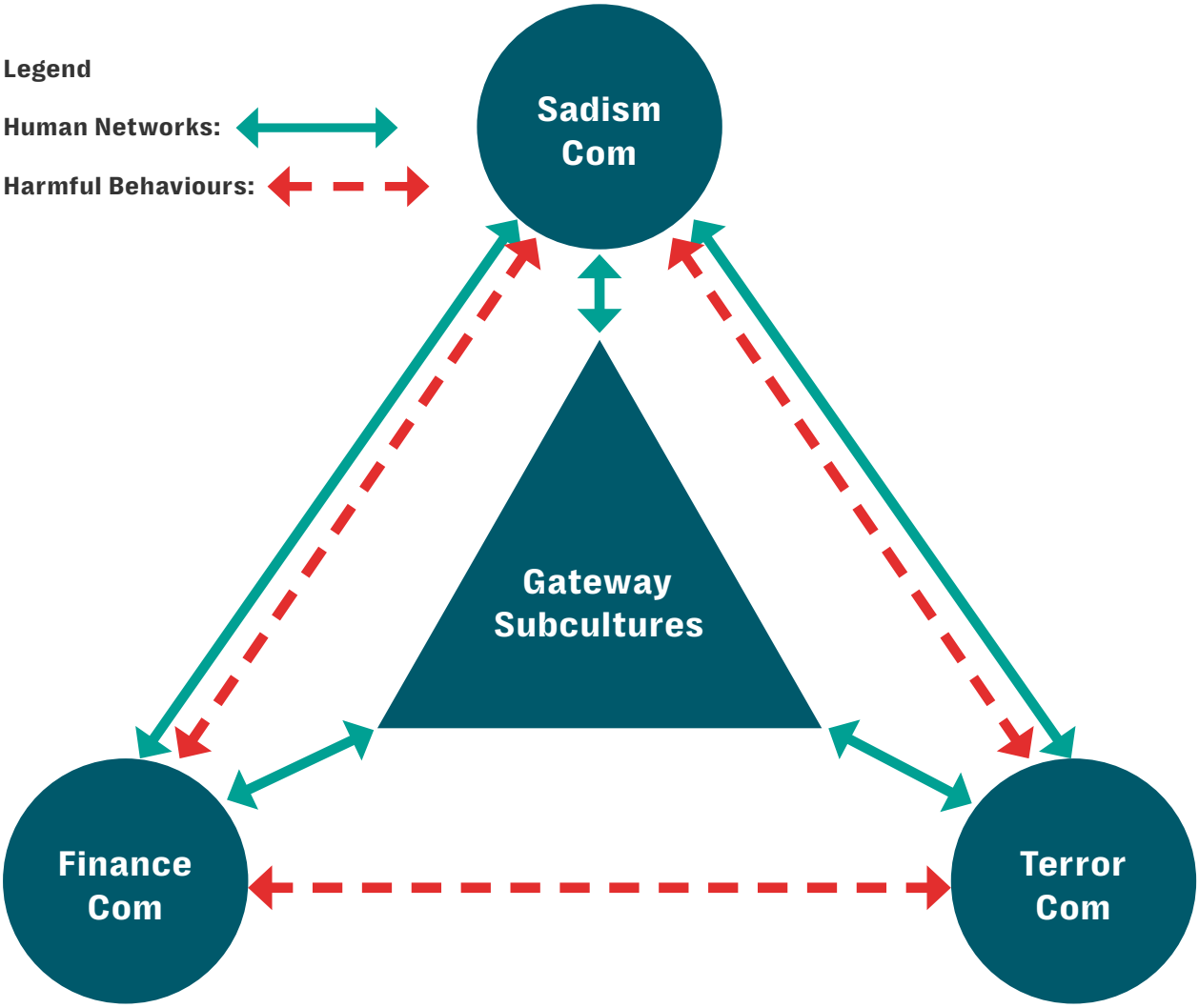


Figure 1: A visualisation of the Tripolar Harm Spectrum, illustrating the intersections between membership and behaviours across the Sadism, Terror and Finance Com subcommunities.

Sadism

Associated with sexual extortion, grooming and Child Sexual Exploitation and Abuse (CSEA) and the encouragement of suicide and self-harm, this pole is composed of decentralised cells of predators. Many of these are direct or indirect offshoots of the most well-reported cases involving the Com.

While the Sadism Com is behaviourally distinctive from other poles due to the widely documented sexual exploitation of victims, participation may also be driven by other factors. These include desensitisation, coercion, a search for notoriety or attraction to the shock value of extreme harms within these communities.

Terror

Seen as the more political wing of the ecosystem, this grouping adheres to, promotes or has an aesthetic attraction to nihilistic or far-right accelerationist ideologies, including white supremacy, occult neo-Nazism, militant accelerationism and violent antihumanism. As it engages in a greater proportion of offline activity, this cluster can be understood in more geographic terms, with notable hotspots for Terror Com activity identified in Europe, South America and the US.

Finance

Members who gravitate towards this pole are primarily driven by monetary gain (particularly cryptocurrency) and clout, engaging in cybercrime to achieve these aims. They attract significant attention in the media for their attacks on major companies, but also carry out cyber and physical attacks within the Com itself. Investigations by Resolver have identified (rare) links between individuals within the Finance and Sadism Com, while overlap between the Finance and Terror Com is principally behavioural through shared TTPs.

Overlap and nuance

It is common for individuals and groups to shift between extremes on this spectrum, creating and breaking links between seemingly disparate cells that form the Com. For example, one active sub-group incorporates the sexual extortion and exploitation elements of the Sadism Com, while also adopting the neo-Nazi aesthetic and language of well-known far-right extremist groups, which in turn influences the Terror Com.

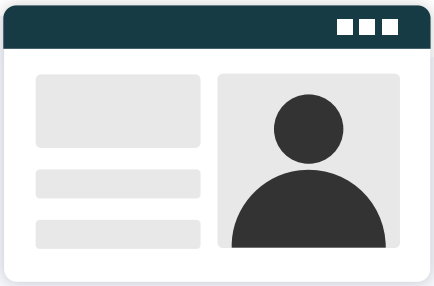
At the individual level, investigations by Resolver into a high-profile former member of a Com ransomware group found that they also engaged in sexual extortion and grooming on children's gaming platforms, unrelated to their financially motivated cybercriminal activities.

There is significant nuance across these poles. Some financially motivated groups do not identify themselves as part of the Com, despite a clear overlap in TTPs, membership and a drive for online clout. This is likely due to the Com's association, through subcommunities on the Terror and Sadism spectrum, with violent extremism and child sexual exploitation.

Financially motivated members of the Com may see these as moral red lines personally, or as harmful to their ransomware operations. They may perceive that targeted corporations would be less inclined to pay ransom fees to groups even indirectly linked to terrorism, grooming and the distribution of child sexual abuse material (CSAM).

CASE STUDIES

Victims as perpetrators, perpetrators as victims



1

Initial contact:

Person X, a teenage girl, joined a Sadism Com chat room when looking for ultra-graphic violence online. She was befriended by other members and groomed into an online relationship with Person Y, an adult male believed to be in his twenties.

2

Grooming and radicalisation:

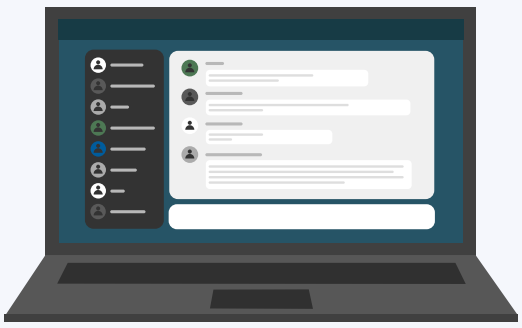
Person Y groomed Person X into sending self-generated Child Sexual Abuse Material (CSAM) using abuse and manipulation. In this time, Person X joined other Sadism Com fora. For validation, she was encouraged by members to use racist slurs, commit acts of fire-setting and groom other victims into suicide, self-harm and other forms of exploitation and abuse.

3

Exploitation and networking:

Person X made contact with Person Z, a transgender adult who was experiencing a severe mental health crisis. She asked them to be her friend, initially discouraged their suicide and invited them to join a chat room with other Sadism Com members.

Person X and Person Y then manipulated Person Z into travelling to a remote location in another country where they self-immolated (setting oneself on fire) on a livestream. This was watched by other members of the chat room, who celebrated Person Z's death.



4

Rehabilitation:

Law enforcement confiscated Person X's mobile phone after it was reported that she had sent self-generated CSAM on one of her social media accounts. She was psychologically evaluated, diagnosed with a personality disorder and enrolled into a therapy programme. She left the Sadism Com chat rooms, deleted her social media accounts linked to the Com and has since expressed regret over her actions.

Cross-group membership

Discovery:

In spring 2025, Resolver identified a chat room operated by an anti-Com vigilante group, which had doxed a member of a prominent Finance Com ransomware group.

The Doxing victim was themselves the owner of a Doxing-focused pastebin, an anonymous text-based site, and had been reportedly involved in cyberattacks and extortion targeting transnational companies.

The dox included social media and gaming accounts, home address and vehicle registration number.

Investigation:

When analysing and verifying these accounts, we found that this member of the Finance Com was also engaged in tactics and behaviours associated with the Sadism Com.

In one leaked conversation, he described how he had groomed a young girl, raped her and extorted her into acts of self-harm.

In self-uploaded videos, he recorded himself publicly broadcasting pornographic content on a metaverse gaming platform for children.

He also had several accounts on platforms considered to be at-risk for child sexual exploitation.

Analysis:

As well as being able to map the publicly known links between different Com subcultures, our intelligence team has been able to use open-source intelligence (OSINT) to identify and document the private links between members of the Finance, Sadism and Terror Coms.

Public-facing harmful behaviour creates visible connections across the Com as a whole, while private, person-to-person connections create deeper links between the Sadism Com and both the Finance and Terror Com.

These links are rare proportionately, but demonstrate the care we must take in our attempt to define this threat.

Emergence, contagion and evolution

Emergence:

Group A, which is considered to be one of the earliest iterations of the Com, was created as a political extremist chat room. Its owner, who was in their mid-twenties, groomed a teenage girl and blackmailed her into sending self-generated CSAM and photos of self-harm. He encouraged other members to target primarily female children with similar techniques, producing handbooks detailing his tradecraft.

Contagion:

A member of Group A founded their own offshoot, Group B, which focused on sexual extortion and blackmail rather than political extremism. As other members of the group wanted to expand their control and status within the ecosystem, they created new chat rooms to exert power and demonstrate their clout, forming new subcultures in the process. This resulted in a splintering and spread, with membership and relationships between them often overlapping, as well as victims targeted.

Fragmentation:

Other groupings splintered off from their precursors due to internal divisions and law enforcement action. Members of Group B left to form Group C, which wanted to distance itself from CSEA and focus more on violent extremism, shifting itself from the Sadism Com towards the Terror Com. There is a realistic possibility that Group C also distanced itself from CSEA due to concerns about law enforcement agencies focusing on sadistic sexual extortion groups.

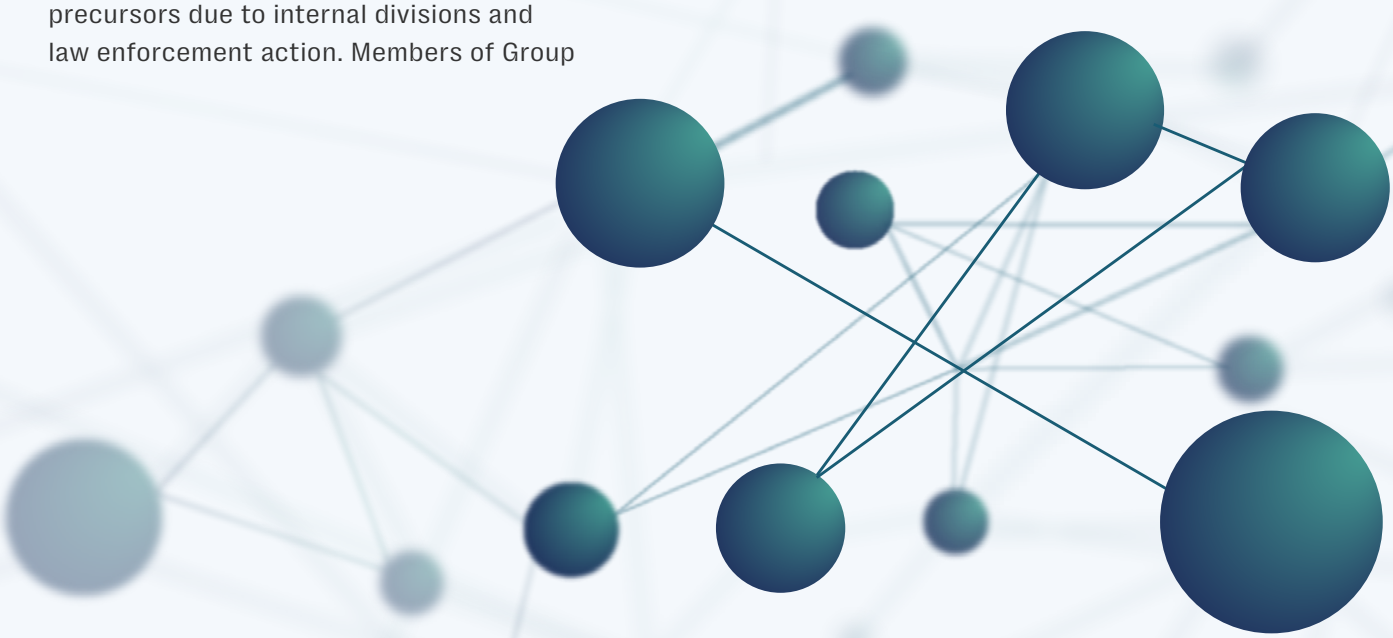
Cooperation:

Group C has worked together with Group D, an established far-right Terror Com group based in Russia and Group E, the online group of a neo-Nazi extremist organisation based in Europe. They have promoted each other on encrypted messaging apps, encouraging acts of physical violence targeting ethnic and religious groups.

Evolution:

Following the separate arrests of their leading members, both Group A and Group B have been in decline. However, as these groups tend to splinter and multiply before their decline, the ecosystem as a whole continues to grow at a rapid rate.

Many older groups continue to have a legacy within the Com, with new members and groupings naming themselves in tribute to former groups, including both Group A and Group B. Importantly, whilst this case study refers to groupings, the Com is often much looser, including purely individual engagement with the subcultures involved.



Victim characteristics

Different parts of the Com select targets that align with their motivations, creating varied and distinct potential victim profiles that range from vulnerable minors to multinational corporations.

The Com as a whole is predatory and often driven by clout, which means perpetrators target victims based on opportunism and perceived value within a subculture.

Sadism Com victims

Victims targeted by Sadism Com activity online are primarily young people, particularly minors. Offline, there is a trend towards encouraging physical attacks against older people. In Romania and Sweden, media reporting has linked Com-related activity to attacks on elderly people.

Neurodivergent and LGBTQ+ people face increased risk of physical abuse and violent crime due to discrimination, social marginalisation and barriers to reporting abuse. Some Com-linked predators create fake support groups as fronts for Sadism Com cells, while others exploit existing support forums on social media or dedicated spaces for marginalised groups. This underscores the need for clearer signposting to official help centres on platforms used by parents and potential victims.

Online communities remain a consistent focus for Sadism Com activity, across both dedicated platforms and mainstream spaces. These environments are used to identify, isolate and groom people, including those in self-harm, eating disorder and related sub-communities. This pattern has been corroborated through law enforcement investigations, including statements from a Sadism Com member arrested in the UK, who confirmed targeting of people with mental health conditions.

Victim targeting within the Sadism Com is gendered. Female victims are treated as higher-value targets by predominantly heterosexual male perpetrators. They are disproportionately subjected to sexual and physical violence, often described within the community as ‘Com Girls’ or ‘Cut Whores’.

Male victims are more commonly subjected to psychological harm and suicide encouragement. These distinct patterns reflect Sadism Com origins in a group whose founder authored a

Online intervention opportunities

Reduce gateways

- Gateway content detection & moderation
- Off-siting link disruption
- Digital literacy education
- Preventative support & signposting

Shrink operating space

- Enhanced signal sharing
- Early risk detection
- Disruptions and takedowns
- Rapid response protocols

Increase exits

- Clear reporting routes
- Signposted support and risk recognition
- Parental & first-line guidance

handbook on sexual extortion, promoting sexual and psychological violence against female minors.

Terror Com victims

The overlap between far-right ideologies and the Terror Com is significant. Nihilistic extremists often co-exist in the same online communities as the political far right, adopting its symbolism and language for shock effect. In some instances, the two ideologies combine into forms of neo-Nazi or white supremacist accelerationism. Since 2023, a prominent Terror Com group has collaborated with an online-based neo-Nazi group and Eastern European white supremacists, co-authoring a violent extremist handbook with the latter.

As a result of this ideological overlap, members of the Terror Com tend to target groups also targeted by far-right extremists, including Jews, Muslims, 'non-whites' and LGBTQ+ people. They also target people experiencing homelessness, frequently referring to them as parasitic and subhuman. Due to increased exposure to random violence, they are disproportionately attacked by Terror Com groups and singled out as undesirables to be 'culled'. However, this targeting may also serve to ideologically justify opportunistic and predatory attacks on vulnerable people, rather than representing a purely ideological motive.

Finance Com victims

The most well-known entities associated with the Finance Com are ransomware groups. They have targeted national retail chains, multinational technology companies and US federal agencies, extorting hundreds of millions of dollars across many different jurisdictions and currencies since commencing their operations. Targeting has focused primarily on large multinational companies that are capable of paying high ransoms.

Similar to traditional criminal dynamics, rivalries and tension within the Finance Com create opportunities for intra-Com cyberattacks and 'In Real Life' (IRL) violence. Members may achieve notoriety by stealing cryptocurrency from other prominent figures and by targeting rivals through a range of online techniques.

Membership, recruitment & global scale

The Com is primarily made up of boys and young men aged between 11 and 25, though participation also includes female, transgender and older individuals. Members commonly share interests in gore, illegal and harmful sexual content, gaming, technology, cryptocurrency, meme culture and engagement with cyber criminality and delinquent behaviour.

The Com has roots in mass attacker fandoms, gore forums, CSAM and bestiality communities. As a result, many members, particularly within the Terror and Sadism Com groupings, come from niche, extreme interest communities. These include fandoms for the 1999 Columbine High School shooters and other mass murderers, particularly far-right terrorists, as well as forums that host gore, narco (cartel) footage and animal crushing videos.

Recruitment

As the Com functions as an ecosystem rather than a unitary group or network, there is no formal recruitment or joining process. Individual Com groups may impose specific requirements, such as documented violence for Terror Com cells or in private chat rooms for Sadism Com sexual extortion rings. Participation in Com-related activities or engagement with the wider Com ecosystem

can be said to be a member of the Com. Just as a traditional criminal does not need to be a formal part of a group to be part of the local criminal ecosystem, a member of the Com does not need to be part of a recognised Com group to be seen as part of the wider Com ecosystem.

Membership can instead be understood as participation. Those with high centrality are those who engage in extreme forms of criminality, including extortion, terrorism and high-impact cyberattacks. At the periphery are those who engage in glorification, aesthetic promotion and juvenile delinquency that serves as a pathway for radicalisation and political extremism.

Types of members

Attention gravitates towards active participants of Com culture, who engage in the most egregious violent, predatory and criminal behaviour. However, the Com ecosystem includes relatively passive participants who adopt the aesthetic, lurk in public Com-linked chat rooms and glorify violent members across social media through fan-cams, music and other content. This periphery plays an auxiliary role, providing entry points that sustain and expand the Com.

Active participants

Active participants are members who engage in direct criminal activity, including terrorism, sexual extortion and exploitation, and cybercrime. They are the most prominent members of the community, frequently glorified by other users and among the most identifiable targets for law enforcement agencies. Their activities are well documented by law enforcement, the media, supporters and other active participants, and include intra-Com crimes such as doxing, robberies and cyberattacks.

When an active participant achieves a certain level of notoriety within a group, they are often included in the ‘roster’: a list of aliases used by prominent figures within a particular cell. This can include owners, administrators and other well-known participants while protecting anonymity. Rosters are shared across social media platforms, often using extremist, Satanic and violent symbology to glorify the group and members who carry out violent or criminal acts in its name.

Semi-active participants

Semi-active participants are members of the Com who support, rather than directly carry out, extreme forms of criminality. This includes individuals who consume harmful content, such as livestreamed abuse coordinated by active participants, and those who enable activity indirectly by providing services such as ransomware-as-a-service to Finance Com groups.

These individuals do not necessarily seek personal notoriety. Their motivations for engagement may range from financial gain to sexual or sadistic gratification. While these participants are not always directly involved in the most extreme acts, their presence and engagement reinforce and support active participants who commit more severe and directly harmful criminal acts.

Semi-active participants are commonly present in semi-public chat rooms and, in some cases, private channels. However, access to many private chat rooms is restricted to active participants, both to limit infiltration by undercover law enforcement and to encourage the production and circulation of new extreme content.

Aesthetic participants & lurkers

As the Com and its constituent groups have attracted increased attention in recent years, their aesthetic has developed a perceived ‘edgy’ appeal among individuals who do not themselves engage in violence or criminality. While this attention does not imply direct participation, the promotion and glorification of the group can reinforce internal status dynamics, indirectly encouraging violent behaviour by active

participants and contributing to further radicalisation within the ecosystem.

When challenged, some members feel pressure to demonstrate commitment to the community. This dynamic can encourage peripheral supporters to move passive engagement into more serious delinquent, and ultimately criminal, behaviour.

Similar to cartel culture, the Com ecosystem also creates space for individuals affiliated with the wider community to promote non-criminal cultural activity. This includes music, artwork, videography and graphic design. Com symbology and references have appeared in independent music on user-uploaded streaming platforms, as well as in artwork, cover images and profile pictures used by individuals who do not necessarily engage in Com-linked criminality.

The relationship between art and extremist symbolism is long established. It is well documented in relation to Nazi symbology and certain metal scenes in North America and Europe. The emergence of Com-linked themes in online independent music and art represents a continuation of this pattern.

Interest in the Com is also driven by morbid curiosity. The group is frequently discussed in podcasts and webcasts focused on true crime, meme culture or disturbing online trends. Many public and semi-public Com chat rooms and servers attract amateur investigators, researchers and curious bystanders who join to observe rather than participate. These users are commonly referred to as 'lurkers'.

Lurkers face a heightened risk of exposure to graphic, extreme and often illegal content. In some cases, they may be minors, which increases their vulnerability to further exploitation by Com members.

LARPers

As a result of this taboo appeal, some individuals engage in 'LARPing' (Live Action Role Play). In this context, the term refers to people who claim to be something they are not, such as a sexual extortionist with substantive links to prominent Sadism Com groups.

These individuals may engage in juvenile delinquent behaviour to attract peer attention or use the group's reputation to inspire low-level fear, but they do not typically participate in serious criminal activity. However, they face risks of self-radicalisation through desensitisation and exposure to political extremism and illegal or harmful content. Their behaviour may also contribute to harm by normalising, promoting or glorifying Com aesthetics and actions.

Vigilantes

Across multiple platforms, we have identified communities that have been set up to oppose different elements of the Com, particularly the Sadism and Finance focused sub-cultures. While they claim to be in opposition to the Com, they are a noteworthy part of the ecosystem that overlaps with it in terms of motivation and techniques. As they operate outside of the law, promote themselves online and target alleged Com members with doxing and cyberattacks, they can be seen as mirroring the Com even while being morally opposed to its more predatory members.

Geography

The Com does not exist as a phenomenon in one part of the world. It has a global presence that crosses borders and language barriers. While Com activity has spread throughout Eurasia, the Americas and Oceania, correlating with global internet penetration rates, our intelligence shows particular concentrations of activity in the United States, Russia and Brazil.

Contextual drivers of regional Com activity include:

1. The prevalence of far-right communities: While much of the Com is superficially ideological, there are overlaps between the Com and the far-right in terms of victim selection, language and functionalities. Countries where the Com has manifested have extensive far-right communities that have influenced the development of its identity and TTPs.

2. Political polarisation and angst: The emergence of the Com overlaps with online trends towards nihilistic and misanthropic outlooks as well as general 'doomer' unease. These have gained traction since the COVID-19 pandemic over perceptions of political polarisation, geopolitical instability, economic prospects, climate change and the future of society with advancements in AI.

3. Hacker subcultures: Countries such as Brazil and Russia have long-standing and notable cybercriminal subcultures from the 1990s onwards, while the US has been the origin of many digital subcultures since the 'phreaker' movement of the 1980s. The Finance Com has notable presences in the US, Russia, as well as Western and Northern Europe, likely borne in part from this history.

4. Proscription, designation and law enforcement measures: Policymakers and law enforcement agencies in some jurisdictions have identified the Com as threats to national security. As such, they are more likely to identify Com-related violence and crimes, whereas other investigating agencies may describe and counter domestic Com activities as isolated, conventional crimes.

While these factors contribute to concentrations of activity around the world, they also explain the Com's geographic spread across Europe, the Americas and Oceania, which have all experienced growing far-right communities and political polarisation in recent years.

The unequal impacts of COVID-19, with some countries reporting significantly higher levels of isolation during lockdown measures, may potentially contribute to the geographical spread of the Com worldwide.

Tactics, techniques & procedures

Resolver's active investigations span the tripolar spectrum of the Sadism Com, Terror Com and Finance Com, with daily operations focused primarily on the first two. Com activity draws on intersecting extremist, violent and criminal influences to pursue notoriety, financial gain or gratification. While motivations vary, harmful behaviours share common TTPs. For example, communities focused on sexual extortion also employ cybercriminal and violent extremist TTPs, while recruitment practices of Terror Com cells often mirror participatory grooming tactics of the Sadism Com. These TTPs frequently cross the online–offline divide, with some forms of online offending requiring physical action, and vice versa.

Based on our tracking of Com activity, the following diagram illustrates Resolver's intelligence assessment of pathways and shared TTPs across the ecosystem, showing how gateways from adjacent online subcultures gravitate towards specific poles of the tripolar spectrum and the offline harm that we have observed.

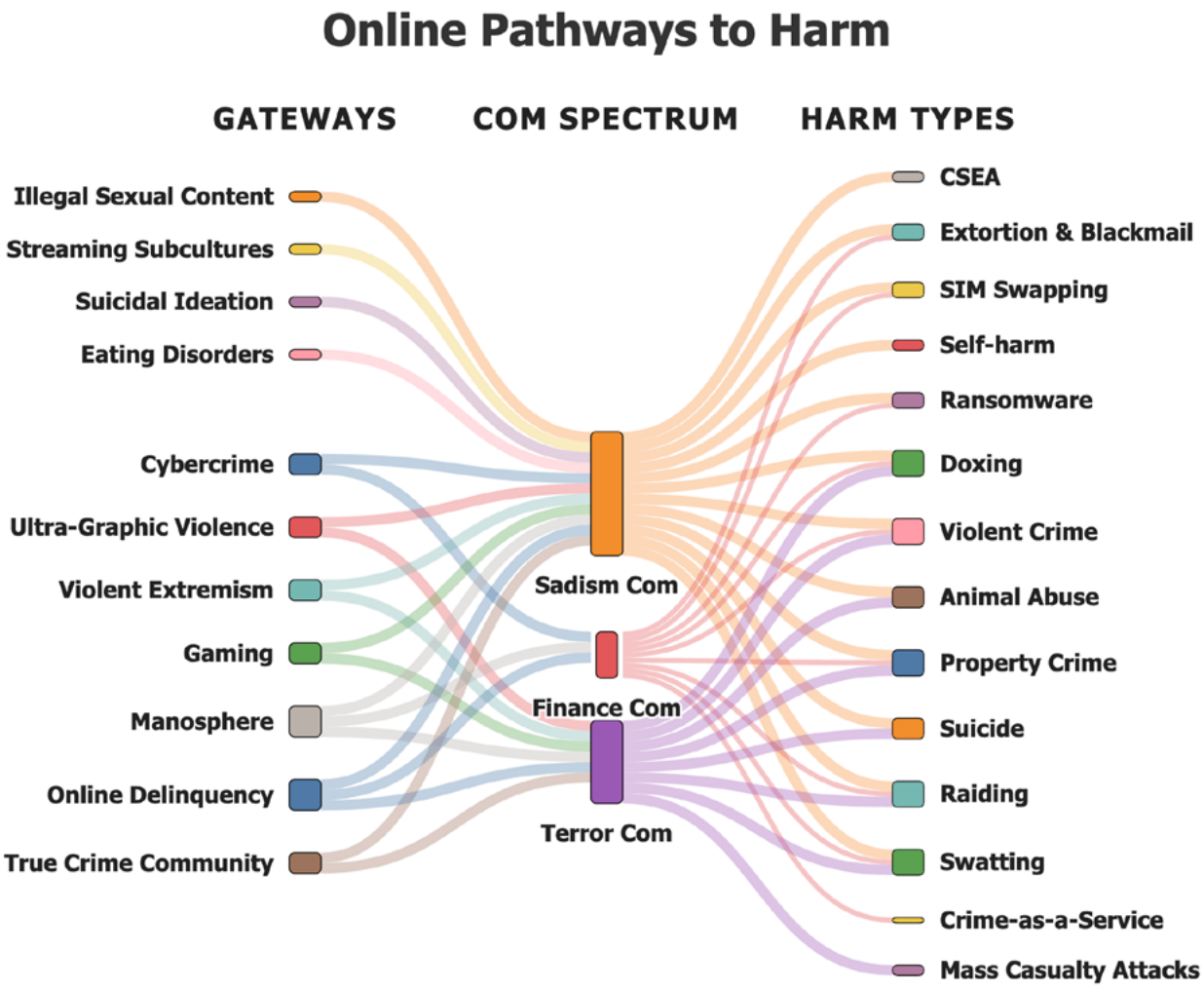


Figure 2: *Gateway subcultures, interests and behaviours provide pathways into the Com ecosystem, gravitating towards intersecting parts of the tripolar spectrum and generating significant overlap in resulting harms, primarily due to shared exploitative and notoriety-driven TTPs. Notably, the Sadism Com has the greatest number of entry points and exhibited harmful behaviours observed by Resolver.*

Grooming and CSEA

Grooming tactics practised in the Com are gradual and participatory, with victims typically coerced into performing progressively more harmful and illegal acts. Although grooming is most commonly associated with the abuse perpetrated by members of the Sadism Com, similar tactics are adopted by the wider ecosystem in recruitment and establishing dominance. Additionally, as grooming primarily occurs online, it can take place transnationally, across global jurisdictions.

Grooming tactics employed by the Sadism Com broadly reflect those used by other offenders who exploit children for sexual gratification or extortion, but demonstrate a more consistent focus on sadistic exploitation. Extremely detailed guides exist within the Com instructing new entrants on how to identify, select and groom victims at scale. Initial contact may occur through infiltrating or creating digital 'watering holes' that attract potential victims, particularly online communities intersecting with gateway subcultures or vulnerable groups. Other methods involve directly seeking out and contacting targets perceived to be more vulnerable to exploitation.

Following initial contact, sexual extortion in the Sadism Com often initiates grooming with emotional and material inducements to establish a rapport with victims at the initial stages of contact. These tactics range from 'lovebombing' to offering digital currencies and rewards. The aim is to make the victim believe that they have an emotional connection with the offender, often romantic. Dependency is further developed through the performance of acts framed as demonstrations of loyalty, progressing towards increasingly more harmful acts.

The ability to elicit and obtain the first explicit image of a victim is a critical pivot point in extortion strategies. Once perpetrators have such material, they gain significant real and perceived power to exert control over children and vulnerable adults, consistent with established patterns of sexual offending. Compromising images and sensitive personal information are then used to blackmail victims through threats of exposure, coercing them to produce further explicit content, engage in self-harm, abuse others or animals, or take their own life.

The participatory nature of grooming within the Com is central to perpetrator-victim bonding. This dynamic fosters desensitisation, shame and fear, which inhibit victims' ability to disengage from or report abuse. For victims of the Sadism Com, this can further blur the lines between abuser and abused, with some individuals not recognising themselves as victims while exploitation continues.

Suicide and self-harm

Most prominent within the Sadism Com, suicide and self-harm are actively encouraged by members. The sadistic orientation of these communities draws on the ritualised elements associated with violent extremist Satanist ideologies, as well as extreme and illegal sexual content. Victims are coerced, often through extortion, into acts of self-harm as demonstrations of loyalty. This includes the creation of 'cutsigns', self-inflicted cuts of an abuser's online alias or group-symbols, used as proof of submission and control. As such, the coercion of victims into self-harm and in cases ultimately suicide, is a means through which perpetrators gain social clout and sadistic gratification.

Although suicide is not central to the Terror Com's TTPs, at least two mass shootings involving perpetrators linked to the Com ended in attacker suicide. This reflects a pattern consistent with the glorification of violent attackers within the Com and intersecting subcultures, including fringe elements of the True Crime Community (TCC) that venerate or aestheticise perpetrators of such attacks.

Animal abuse

Many participants in Com-activity, particularly on the Sadism spectrum, have engaged in, or coerced others to engage in, acts of zoosadism targeting wild animals and domestic pets. This fits the overall trend of opportunistic targeting of the vulnerable. Members of the Sadism Com will coerce their victims into harming animals, particularly pets, to satisfy their desire for physical harm against an animal and psychological harm against the coerced individual.

Although a direct line cannot be drawn from animal abuse to harming humans in the absence of additional risk factors, such behaviours can act as a stepping stone in the escalation of violent fantasies, particularly as animal victims are more accessible and are incapable of reporting abuse.

Random acts of violence

At least two attacks on schools in the US and Russia have been directly linked to the Com and multiple other attempted mass casualty events and terror attacks by members have been preempted by law enforcement and counterterrorism agencies. Most of the planned attacks have focused on schools, intended to be carried out by radicalised students, but there have been two notable exceptions. These include a bomb plot at a Lady Gaga concert in Brazil and a mass poisoning plot planned by members of nihilistic Terror Com group originating from Eastern Europe, which targeted children from ethnic and religious minority backgrounds in New York.

Fire-setting

Fire-setting is a tactic used primarily by the Terror and Sadism subcommunities for different but overlapping purposes. Within Sadism Com groups, fire-setting often has an antisocial element, meaning that it can be untargeted and still earn clout among other members of the ecosystem.

For example, participants have documented themselves setting wildfires in rural areas to gain the respect of other Com members. However, fire-setting can also be targeted at specific demographics or rival Com groups. Among members of the Terror Com, fire-setting can be used to covertly attack homeless people, as well as ethnic and religious minorities.

Robberies and brickings

Finance Com groups and individuals have physically attacked each other in order to steal cryptocurrency. Rivals have been targeted at their homes and subjected to violence, including torture, to obtain access to cryptocurrency wallets.

There have been instances of Com members using impersonation to get access to targets, who are attacked, tied up and tortured into giving up their passcodes for cryptocurrency wallets. In early 2024, there was a spike of intra-Com robberies and violence, referred to by some as a ‘Com World War’, in which groups targeted each other with cryptocurrency-focused home invasions.

Similarly, rivals have tried to intimidate each other with ‘brickings’, essentially throwing bricks or other heavy objects at the windows of cars and homes. The purpose of the attack is to demonstrate knowledge of a victim’s location, implying the potential for further and more extreme violence. This is sometimes recorded and shared online to further harass and intimidate their rivals.

Vandalism

Much like traditional criminal groups, the Sadism and Terror Com ecosystems frequently engage in acts of vandalism, including graffiti and tagging. They often target abandoned buildings, spray-painting the names and symbols of groups as well

as call for certain arrested members of the Com to be freed from custody or prison. Acts of vandalism are recorded or photographed and then shared across various platforms. In some groups, this activity is used as an initiation, inviting new members to carry out vandalism, before encouraging progression to more extreme acts, such as fire-setting, assault or murder.

Raiding

Raiding and brigading are among the most introductory behaviours into the Com, often bridging the gap between online delinquency and Com activities. At lower levels, raids may resemble juvenile 'trolling', with users coordinating to spam and prank random or rival chat rooms, livestreams, forums and other online communities. Raids can escalate into overtly hateful or 'edgy' conduct, incorporating racist slurs or extremist symbols like the Nazi swastika. In these cases, the intent is principally for shock value rather than the expression of a coherent and deeply held political ideology.

At its extreme end, raids by intersecting subcultures and Com members distribute ultragraphic violence ('goreposting'), CSAM, bestiality and other forms of distressing and illegal content.

The relative anonymity of this coordinated group action provided by raiding can serve as a disinhibitor and a source of peer pressure. Over time, this contributes to the desensitisation of participants to gore, racism, bigotry and political extremism, increasing the risk of radicalisation and normalisation in the long term.

Groups that focus primarily on 'edgy' raiding tend to exist as gateways at the centre of the tripolar harm spectrum, providing entry points into the Com ecosystem, particularly due to overlaps in membership, the networking involved in coordinating raids and shared interests.

Doxing

Doxing involves the exposure of personally identifiable information (PII) and is a TTP practised across the Com. It serves multiple functions within Com power dynamics, including harassment, extortion and retaliation against rivals. Although doxing can involve sophisticated techniques, such as infecting a target's device with information-stealing malware, it generally has a low technical barrier to entry, particularly in jurisdictions where PII is accessible in the public domain.

The 'quality' of a dox, determined by the volume and sensitivity of exposed personal information, often including details about a target's family, acts as a metric for establishing notoriety among peers. The exposure of personal information is not an end in itself, but is intended to attract further harassment or law enforcement attention, with the latter primarily observed in doxing between rivals.

Within the Sadism Com, doxes of victims are compiled into 'lorebooks', which can include content depicting self-generated sexual imagery, self-harm and acts of abuse, used both to extort the victim with the threat of exposure and increase social status amongst members.

Swatting

Swatting is a practice of submitting a false police report, typically alleging a hostage or active-shooter event, with the intention of attracting an armed police response to a target's location. This tactic is typically practiced within the Com as a form of harassment against victims or rival members.

Com members often livestream swatting calls and share the content within their own groupings or post it publicly on online platforms to gain notoriety. Swatting within the Com has evolved, growing in

scale and severity as well as being carried out for financial gain. For example, one group conducted multiple hoax active shooter reports at US universities while also advertising swatting-as-a-service for payment. Resolver observed significant clout-seeking behaviours by this group, including publishing polls to allow followers to select future targets and engagement with prominent media outlets to increase their visibility.

SIM swapping

SIM swapping is a cyberattack in which a target's phone number is transferred to an alternative SIM, enabling control over the victim's device and data. SIM swapping is a foundational TTP within the Com's cybercriminal activity and has also facilitated networking between members in cybercrime-focused online communities. Although SIM swapping is traditionally used for financially motivated crimes, both the Finance and Sadism Com have adapted the tactic for harassment and extortion. While Finance Com members remain principally focused on using SIM swapping for monetary gain, the Sadism Com has used SIM swapping attacks to gain control over victims' devices and to extort them using private information.

Ransomware

At present, cyberattacks carried out by Finance Com groups rank among the most significant cyber threats. Prominent Com groups have publicly declared their collaboration and perpetrated high-profile cyberattacks against major corporations and government entities. These attacks have demonstrated a high degree of sophistication, employing a wide range of attack vectors to gain access to systems. This typically involves social engineering, followed by extortion under the threat of releasing sensitive data.

Crime-as-a-service

Many of the TTPs detailed above have been monetised by members of the Com, who claim to offer criminal services in exchange for payment, often in cryptocurrency. While some individuals advertise specific crimes, such as doxing-as-a-service, others promote 'menus' of criminal acts for commission, including both physical and cybercrime. In some instances, crimes like swatting attacks can be commissioned for as little as $10 for a residential address, with other locations, such as airports and hospitals, priced significantly higher. While many that claim to offer these services are likely inauthentic, some have provided verifiable proof, including media reports, of crimes committed in order to establish credibility with potential customers.

Currency and clout

As a semi-hierarchical ecosystem, the Com has its own preferred forms of monetary and social currency that determines an individual's place within the system as a whole. While these are separate things, they feed into each other. Members may show off their cryptocurrency balances to establish credibility or compile and distribute lorebooks of victims to increase prestige. Those with more online clout have a greater chance of pressuring victims into paying them or becoming central within a sadistic exploitation group. Individuals without established status are unlikely to be included in high-value ransomware operations or the inner circles of Sadism Com groups.

Online infamy, often referred to simply as 'clout', functions as a metric of social status. It combines elements of the notoriety associated with traditional criminals, comparable to outlaw status in the American Old West combined with the online culture of contemporary social media influencers. In some instances, Terror Com groups have created their own trackable metrics for clout, used to assess a member's

commitment or standing. Acts such as fire-setting and vandalism accrue points, with verified homicides or assaults assigned significantly higher values, gamifying the group's activities.

Similarly, non-consensual intimate imagery (NCII), CSAM and original self-harm or suicide content is used used as a form of currency within the Sadism Com, with members trading this material between one another. In particular, cutsigns are commonplace in private Sadism Com chat rooms as these images provide verifiable clout for the abuser named in the image.

In monetary terms, cryptocurrency is especially popular within the Com, primarily for its relative anonymity but also for its popularity and adoption within younger tech communities, with some members observed sharing their account balances in order to increase their clout. Cryptocurrency can be taken as payment for crime-as-a-service or extracted from victims of high and low-level extortion. It also introduces challenges for law enforcement when it comes to tracking proceeds of crime; however, it also provides opportunities for law enforcement to detect transactions when Com members attempt to 'cash out.'

Gaming currencies and other purchasable items on gaming platforms are more popular within the Sadism Com. They can be used to groom potential victims through gifts of digital currencies or gaming accessories or using them to purchase intimate imagery from minors.

The Com as an evolution of crime

The manifold threats emanating from the Com may appear novel, due to the wide ranging and egregiousness of harm, the young demographics of victims and offenders, and transnational contagion online. However, its tactics, motivations and power structures largely mirror those of traditional criminal subcultures and organisations. In many respects, the Com shares similarities with a range of extremist and criminal groups, from cartels to cults. What distinguishes the ecosystem is the blending and evolution of these tactics, ideologies and aesthetics.

Like traditional criminal organisations, the Com contains an intricate web of rivalries, splinter groups and alliances. Resolver is actively mapping these evolutions, with rivalries between Com groups comparable to criminal violence, substituting drive-bys and turf wars for doxing and online raids. Online infamy, which drives much of the Com's actions and allows members to understand their position in a semi-hierarchical ecosystem, acts as a digital form of 'street cred'. Pathways from juvenile delinquency to criminal violence are mirrored online within the Com, with newcomers starting with lower-level trolling, cyberbullying and raiding rival online communities prior to escalating to violent extremism and child predation.

TTPs used by Sadism Com in particular manipulate victims into recruiting and abusing friends and siblings, mirroring peer-to-peer recruitment tactics observed in human trafficking and sexual exploitation networks. This can blur the line between victims and perpetrators, with some victims groomed into committing acts of abuse themselves. Within the Com, victims of abuse may be further exploited to recruit and harm others, including inviting them into online chat rooms operated by predominantly male predators. We must take care not to oversimplify 'offender' status.

Both the Sadism and Terror Com intentionally draw on techniques and aesthetics associated with cults, combining occult and pseudo-religious narratives to exert control and power over members. For example, a newly formed and expanding offshoot that claims people 'respawn' after death. This mirrors beliefs observed in suicide cults, including claims that people's souls and consciousness would be transferred to their 'Next Level' after death, with suicide promoted as a faster route to ascension.

Com groups have evolved suicide-promotion tactics used by cult leaders by exploiting gaming terminology and platforms, posing significant suicide and self-harm risks among a new generation.

The emphasis on recorded ultraviolence and extreme sadism, shared online for self-glorification and intimidation of rivals, is as prevalent within Latin American cartels as it is within the Com. This parallel includes the evolution of cartel propaganda from direct self-promotion to the use of artists and influencers to promote leaders and groups without openly engaging in criminality.

This is also true of the Com, whose 'edgy' brand has been adopted by non-criminal social media users across art, music and other forms of content creation. This trend illustrates how criminal ecosystems like the Com benefit from external promotion and fandoms, which can reinforce cycles of criminality. This evolution of crime, incorporating cybercriminality, extreme sadism, social status and digital subcultures, is not limited to Europe and the Americas.

Similar evolutions that mirror the Com have emerged in Japan, where decentralised networks provide cybercrime-as-a-service, as well as Central and West Africa, where scammers combine sexual extortion to earn money and clout within occult-influenced criminal subcultures. We have also identified cases of monetised sexual extortion in South Korea and the arrest of a metaverse-based cult leader in Iraq. While these regional variations may lack direct human network ties, the trends remain closely aligned through shared TTPs, motivations and online-enabled criminality.

Ultimately, the Com is less a new trend than a remix of existing ones. Much of the tradecraft contained in handbooks shared within the Com draws on techniques for violence and control used by previous extremist and criminal groups. However, this continuity demonstrates that countermeasures deployed by platforms, Resolver and law enforcement to combat these organisations are likely to have some application to the Com.

Ideological appropriation

As the Com has its roots in far-right extremism, militant accelerationism and Nazi occultism, it adopts ideas, language, aesthetics and symbols from a wide range of ideological sources.

Ideologies: Resolver have identified Com groups, particularly among the Terror Com, that claim to adhere to a range of extremist ideologies, including white supremacy, neo-Nazism and nihilistic violent extremism. Within the Sadism Com, members frequently reference Satanic neo-Nazi ideologies that originated in the 1960s, as well as other Western esoteric belief systems.

Aesthetics: When creating rosters, profile pictures and video edits of criminal activity, Sadism and Terror Com groups will use 'edgy' and transgressive iconography, from white supremacist and neo-Nazi images (swastikas, Celtic Crosses, Sonnenrads) to Satanic symbols (pentagrams, Baphomet, inverted crosses). Anti-Christian imagery is also encouraged, with one notable roster image shared online including a crucifix made from razor blades featuring an inverted Jesus Christ.

Language: Individual cells within the Sadism Com are commonly referred to as 'nexions', a term originally used to refer to violent occult extremist chapters. Other terminologies of precursor Satanic violent extremist ideologies are further adopted by the Com, such as 'opfering', to frame the harming of victims as a sacrificial rite. When creating usernames for social media accounts, members sometimes include references to ideologies they appropriate, using dog whistles (e.g. '1488' to reference the neo-Nazi phrases 'the 14 Words' and 'Heil Hitler') to both evade moderation by platforms and attract attention from other users that are part of the in-group.

Influential figures: Due to its partial overlap in mass murderer fandoms like the TCC and far-right online communities, elements of the Sadism and Terror Com have appropriated mass murderers, fascist dictators, as well as violent attackers. 'Saint' culture that glorifies the perpetrators of far-right terrorist attacks exerts significant influence within Com culture.

Additionally, former Nazi minister Heinrich Himmler, considered to be the 'chief architect' of the Holocaust and who is associated with esoteric Nazism, is a prominent feature in some Com chat rooms.

Objectives: Many Terror Com groups claim that the ultimate objective of their accelerationism is 'system collapse', which takes the misanthropic nihilism of far-right accelerationism a step further by removing the ultimate objective of rebuilding society into a white supremacist utopia and instead seeks anarchical collapse for its own sake. They also share targets with the far right, including Jews, Muslims, ethnic minorities, feminists and homeless people.

However, Resolver's investigations into Terror Com groups have assessed there to be a much lower commitment to the underpinning ideological tenets and objectives of militant accelerationism relative to violent extremists at its core.

While it is unclear as to what extent members of the Terror and Sadism subcommunities genuinely believe in their claimed ideologies, they still promote and normalise extremist beliefs online and create unsafe digital environments for vulnerable users that far-right extremists frequently target.

Com members who self-identify as neo-Nazis have shown limited knowledge or understanding of their adopted ideologies, suggesting that, for many, the appropriation of neo-Nazism and its symbols is intended more for shock value rather than an expression of genuine political beliefs.

Within the Terror and Sadism Com poles, cells tend to borrow from other extremist organisations as well as from each other. Terror Com groups have distributed handbooks taken from jihadist groups like Islamic State as well as from white supremacist terrorists and mass murderers.

Equally, more Com-specific tradecraft, such as sexual extortion procedures, are shared between groups. Newly emerged groups overtly copy techniques and procedures used by those groups.

Exploitation of platforms and features

The Com is dependent on online platforms to operate. Core characteristics of the Com, including membership, power dynamics between subgroups, exploitation of victims, and criminal and harmful acts, are shaped in part by the functionalities of the platforms they use.

Resolver's work tracking Com activity has found that platforms become preferred by Com adherents based on the functionalities they offer and the user bases they attract. When Com activity is disrupted on one platform, groups and individuals adapt their behaviours to evade further detection while remaining within that platform. This depends on what they perceive to be the greatest targeting or co-ordination benefit, with some choosing to migrate to similar platforms or create their own spaces.

As shown in the functionality heatmap below, our intelligence-based assessment indicates that no functionality facilitating user interaction is immune from misuse, and that features carry differing levels of risk depending on how they are exploited.

These functionalities can enable the Com ecosystem to sustain itself and expand online. Investigations by Resolver have found that platforms possessing a greater number of the functionalities highlighted in this heatmap face higher risk of elevated Com activity, due to the perceived advantages they present for victim selection and exploitation, as well as for maintaining internal cohesion and networking.

Given the wide range of platforms exploited by the Com, it is operationally useful to

Severity Index: 1 Low Risk | 2 Medium Risk | 3 High Risk | 4 Critical Risk

Functionality	Initial Contact	Grooming & Radicalisation	Harm & Abuse	Internal Networking & Conflict
Online Gaming	4	3	2	3
Group Chats & Servers	3	4	4	4
Direct Messaging	3	4	4	4
Livestream	3	4	4	3
Video Hosting	3	3	2	2
Social Networking	3	3	2	2
Microblogging	3	3	2	3
Forums & Imageboards	3	4	3	4
Pastebins	1	1	4	4
Websites, Landing Pages & Blogs	3	2	4	3
Digital Currency	4	4	3	3

focus on the pull factors created by platform functionalities at different stages of activity. This enables the development of appropriate safeguards and interventions to disrupt, dismantle and pre-empt their ability to operate. While the functionalities discussed in this report may better reflect the core features of certain platform sectors, Com activity is observed across a wide range of services, and any platform enabling user-to-user connectivity is at risk of exploitation.

Games with high levels of user interaction and predominantly young player bases have attracted significant Com activity, particularly for initial victim contact and networking with other members. Gaming-focused marketplaces and platforms have also been exploited, with the Sadism Com in particular using features such as in-game currencies to lure players into further contact for grooming.

Other features, including customisable character skins and the ability to create bespoke environments, have enabled Com members to project distinctive and 'edgy' identities and aesthetics to appeal to vulnerable individuals. Within the online gaming sector, metaverse gaming platforms have been particularly targeted by the Com, as these features are inherent to their infrastructure and player experience.

Group chats and servers
Central to the Com's online activity are public and private chat groups and servers. These chat rooms serve important functions for Com subcultures. For example, role permissions often correlate to in-group hierarchies, with those possessing admin permissions taking leading roles. Platforms with advanced settings for creating multilayered chat rooms with varying levels of access and user permissions as well as video calling and livestreaming features have been especially favoured by Com cells for maintaining social cohesion and conducting abusive and illegal behaviours and events.

Direct messaging
Com members use direct messaging features to communicate with victims and other members. Once a target is identified and initial contact is made, Sadism and Terror Com members often use direct messaging features on mainstream platforms before moving victims or prospective recruits to more privacy-enhanced messaging apps or chat rooms. Additionally, Finance Com groups have used instant messaging to contact potential corporate insiders to gain access to systems or employees, or to threaten and harass targeted businesses into accepting extortion demands.

Encryption and enhanced privacy settings
Core members of the Com favour platforms with enhanced privacy features or encryption for communication and the exchange of illegal content. Although early Com activity showed relatively lax operational security, increased law enforcement action and platform moderation have led more subgroups to use privacy settings and implement gatekeeping measures to vet prospective members. Members of the Com have also long used encrypted darknet protocols such as Tor and I2P to facilitate criminal and harmful activity, ranging from consuming and sharing illegal content to hosting community-created sites.

Livestream
The Com have exploited livestream features to capture acts of violence and abuse. For example, Sadism Com communities have streamed their victims creating self-generated CSAM, engaging in self-harm, or dying by suicide, as well as abusing others and animals. Platforms that enable private or members-only streaming have been key for Sadism Com practices such as 'cutshows', where members collectively view and coerce a victim to carry out acts of abuse, self-harm or to kill themselves. Within the Terror Com, members encourage livestreaming of criminal and violent acts as part of initiations or to gain clout within the ecosystem.

Social networking, microblogging and video hosting platforms
Although Com members often use more private online spaces for their most egregious activities, they remain active across a wide range of mainstream social media platforms. Com members exploit these platforms to identify and contact targets, post self-promoting content, and signpost invitations and links that direct off-site users to their core online spaces.

The emergence of LARP and fandom content presents additional challenges by increasing Com visibility on social networking, microblogging and video hosting platforms among potentially vulnerable users who may seek to emulate or join these communities. Additionally, the extensive features offered by these platform categories, including the functionalities discussed above, have also been exploited.

Forums and imageboards
The Com create, target and exploit forums dedicated to discussing topics that attract vulnerable people, such as suicidal ideation or those engaging with intersecting subcultures. The topic-focussed nature of these platforms is used for bespoke networking and target identification.

For example, suicide-focused forums attract those experiencing suicidal ideation and mental health conditions, while individuals with confirmed links to the Com have administrated prominent cybercriminal forums dedicated to sharing leaked data, exchanging tradecraft and networking.

Additionally, the emergence of new forums that are focused on Com-adjacent subcultures, where moderators and administrators actively promote harmful behaviours, provides significant recruitment and grooming risks.

Pastebins
Pastebins, which are text-based websites hosted on the surface web and darknet, are used to anonymously share personal and sensitive data. They act as a keystone in the Com's online infrastructure by enabling doxing. Pastebins dedicated to doxing are used both to control victims with threats of exposing their personal information as well as to inflict harm to rivals in conflicts between members. There are several active doxing pastebins that have been created by prominent Com members or figures in adjacent subcultures.

Bio-link and landing pages
Websites that allow users to create landing pages with links to multiple social media profiles, gaming accounts, chat rooms and third-party websites are exploited by members to signpost new servers and forums related to the Com. This provides an alternative avenue to circumvent off-siting moderation on mainstream platforms, with users referencing the name of commonly used bio-link websites alongside a username or keywords to avoid using URLs.

As some platforms let users customise their landing page with graphics and music, Com-affiliated profiles can be identified by their aesthetic style as well as by references to Com culture in the username and profile text.

Com-created sites
To circumvent moderation, members of the Com have created their own websites hosted on the surface or dark web. These primarily take the form of pastebins, forums and leak sites, which have low barriers to entry and require minimal resources when it comes to creating and hosting them.

While these can still be disrupted, whether by law enforcement operations, hosting provider takedowns or cyberattacks by rivals, they are more persistent and have an elevated risk of being used to facilitate extreme harm. Activity on these websites focus on internal networking and conflict. The Finance Com also uses leak sites to promote themselves, facilitate contact with their victims and publish breached data.

Challenges, wider risks and sensitivities

Detection and intervention
Consistently identifying the risk signals and early warning signs of Com activity, targeting, vulnerability and exploitation are a central part of Resolver's work in this space. Here we detail the challenges that platforms and investigators are encountering when engaged in detection, especially at global scale.

Discovery by group or ideology has limited efficacy
Subcultures, group names and aligned (or aesthetic) ideologies used are changing constantly and the ecosystem is highly decentralised. Whereas more traditional groups can often be disrupted through removing key leaders, the Com ecosystem is more resilient to both detection and disruption techniques.

Language is unfixed and in constant evolution
Beyond group names, the associated vernacular used within groups, the meme culture and the content are constantly changing. Individuals involved are borrowing mature techniques used in other parts of the internet to circumvent detection, including dog whistles, unique (but evolving) coded references, etc.

Shared Child Sexual Abuse Material (CSAM) is typically unknown (novel)
Key CSAM detection technologies such as hash-matching struggle in this setting, where a very high proportion of content discovered by Resolver does not match any known hash databases. The proportion of newly extorted, novel, CSAM is extremely high and limits the efficacy of many existing technological measures.

Siloed threat detection is inherently weaker
Single-point detection, such as classifiers which can only find self-harm references, or only find gore content, are typically unable to collectively score Com risks appropriately. For smaller platforms, access to multi-layered detection systems can be a significant technical barrier. For larger platforms, creation of hybrid threat detection engineering and policy teams presents additional investment requirements and operational complexity.

Signal sharing requirements are complex
These groups are continuously migrating between and across large, small, surface and deep/dark web platforms and services. The critical context required to identify Com activity is often only achievable where Resolver or other parties have visibility across the ecosystem. This requires careful consideration by legal counsel at platforms to enable sharing and coordinated action; and clearly depends on legislative, policy and regulatory alignment.

Aesthetic engagement with Com demands nuance
More recent appropriation of Com-style behaviours, 'roleplaying' into 'edgy' communities and non-criminal engagement poses challenges to differentiation between low-risk and high-harm behaviours online.

Progressively younger offender ages
Estimated ages of users identified, especially perpetrators, have decreased as the hybrid threat has grown. Fundamentally, these users present a safeguarding challenge, in addition to resulting harms they may be groomed to perpetrate. This adds complexity to triage, enforcement and safeguarding.

Preserving space for rehabilitation
Many, if not most of those involved in these harms present potential for rehabilitation. The key is early intervention. The necessity to not only enforce content and conduct policy, but also provide appropriate, localised and accurate sign-posting to support services adds to the detection and response challenge.

Lack of co-ordinated reporting mechanisms
There are multiple lines of effort in countering Com activity and supporting victims; however, the lack of global and local coordination impacts effective prevention, response and rehabilitation pathways. The lack of clarity of definitions and inherently cross-risk nature of the Com complicates escalation. Formalised definitions and escalation frameworks that account for the often multi-jurisdictional and hybrid threats that manifest from the Com can further refine the effectiveness of interventions, be that rehabilitation and support, or prosecution.

Risks for investigators and Trust & Safety teams

Vicarious trauma of content
Individually, the content types Resolver identifies when tracking these threats tend to represent severe manifestations of each harm category. Self-harm is amongst the most brutal imagery we see. CSAM is of an extremely young age, deeply sadistic and overlaps with self-harm content. The gore and graphic content used to desensitise victims includes deeply disturbing imagery and videos.

Taken together, sustained investigation of this activity presents significant wellbeing risks for Trust and Safety teams, law enforcement and other stakeholders involved in investigative processes.

Concerns for reprisal
In recent years, Resolver has tracked an increase in threats to Trust and Safety teams, an area on which we directly support platforms. The heightened use of doxing and other forms of harassment within Com activity poses an additional risk of reprisal for platform teams taking more active measures against these threats. We have already seen reports of law enforcement officers allegedly being doxed.

Additional red-teaming demands
Members of the Com have proved themselves to be adept at exploiting new features and defenses. A new bar is required in crucial safety-by-design and safety-by-default approaches to match this capability, not as a one-time investment, but continued proactive intelligence development and risk detection evolution.

Sensitivity and nuance
We must treat this threat with sensitivity, not sensationalisation. Global public awareness and participation in interventions is important to their success. Sensationalisation of the threat can lead to a counteractive response.

On the one hand, it risks creating ‘moral panics’ focused on individual platforms that decreases understanding of the nuanced risks to vulnerable individuals; on the other it may increase the notoriety that members of the Com seek and risk creating unintended pathways to radicalisation. Resolver will continue to approach this work in a careful, intelligence-led manner.

Contact Resolver

Thank you for taking the time to read our report and for the work you do, or will do, to protect children from this threat.

For further engagement or enquiries on this or other matters:

Media: mediarelations@kroll.com

Platforms, regulators and other stakeholders:
com-report-enquiries@resolver.com

Resolver: further background

Resolver, a Kroll business, draws on 20 years of experience in the Trust and Safety sector to deliver global intelligence, technology solutions and advisory services to our partners. Our Trust and Safety division was founded in Leeds, UK, in 2005 to protect people and platforms from harmful online content and now has offices in Leeds, London, Hyderabad, Mexico City and Manila. The overwhelming majority of our analyst cadre is based in the UK and operational management functions are performed from the UK.

We work with social media companies, search engines, app stores, games platforms, Generative AI model makers, NGO partners, governments and regulators to deliver our mission. We specialise in core online harm identification and mitigation including, but not limited to: child safety, mis and disinformation, hate speech, violent extremism, suicide and self harm, adult content and illicit monetisation.

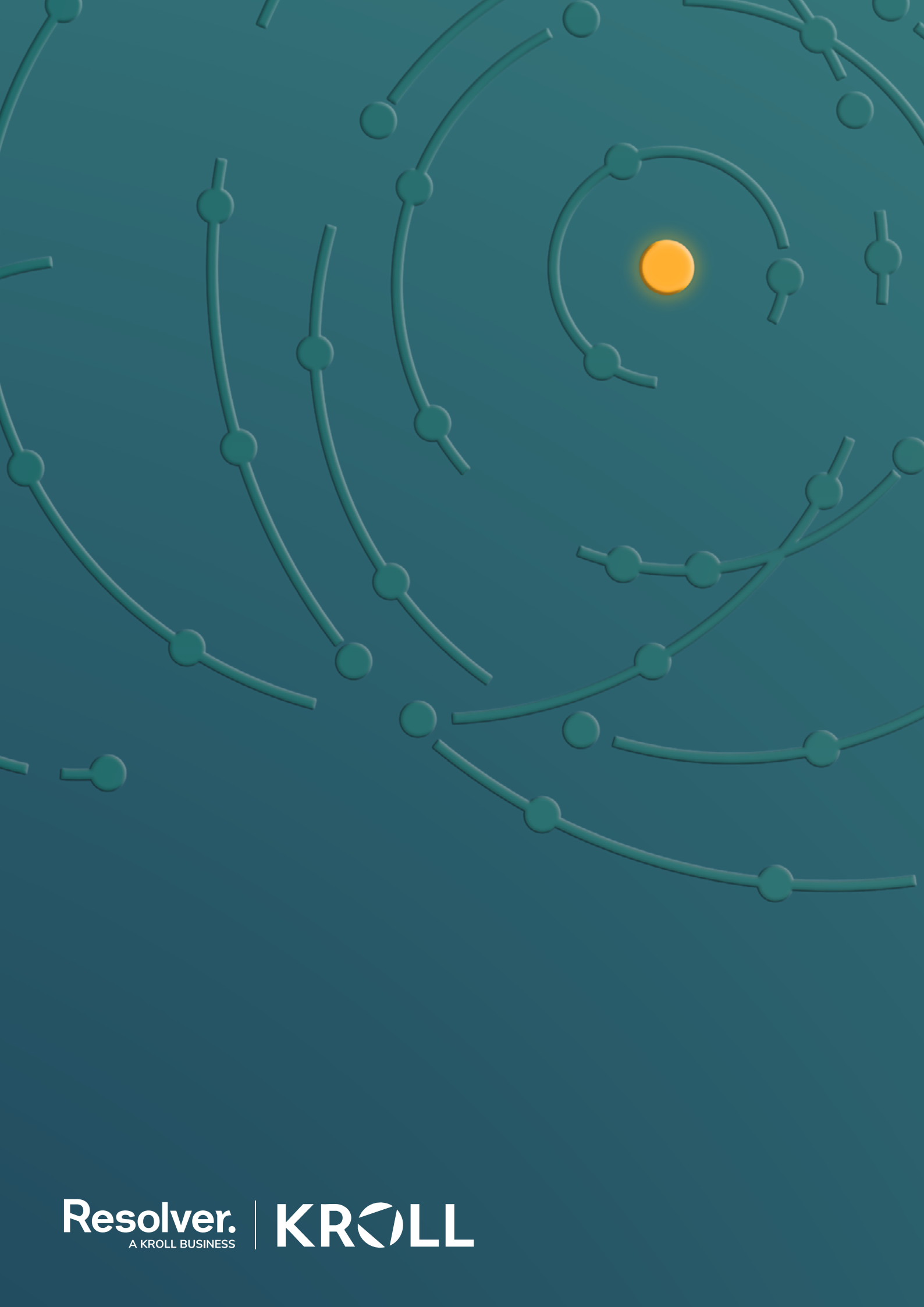
A particular area of focus for Resolver is the overlap of these risk types, contextual analysis depending on jurisdiction and the connection of online harms to human and social impact. Our approach is unusual in that we combine a large and sophisticated technology platform which can collect, process and analyse large quantities of data in real-time, with over 180 expert analysts who add context, subject matter expertise and deep open source intelligence capabilities to our reporting.

We understand that the online environment is complex and context-dependent. Our technology platform is designed to achieve scale and precision and our human expertise to overlay contextual and regional understanding alongside deep knowledge of the human and social impact of online risks.

Resolver participates extensively in industry and NGO initiatives and groups addressing online safety. Resolver is a founding member of the Online Safety Tech Industry Association and WeProtect Global Alliance, providing vital research to its Global Threat Assessment.

Resolver is also a long-term member of the Family Online Safety Institute (FOSI), the Internet Watch Foundation (IWF) and supports, partners or otherwise sponsors initiatives by INHOPE, the Trust and Safety Professional Association (TSPA) and many other organisations. Resolver is a committed and authoritative voice in the field of Trust and Safety.

Learn more at
www.resolver.com/trust-and-safety



Resolver.
A KROLL BUSINESS

KROLL