MAY 2026

Advancing Response to Sadistic Online Exploitation in Networked Youth Environments

Insights & Recommendations From the Field

Research conducted by Thorn

THORN

Table of Contents

Acknowledgments

We are grateful to the individuals who took the time to participate in this research. Without their gracious participation, we could not have developed the key insights shared in this report about sadistic online exploitation. It's vital we acknowledge the psychological burden of exposure for many involved in these responses.

We are also grateful to the experts who generously contributed their time to review and provide feedback on a draft of this report — special thank yous to Matthew Kriner and Amy Cooter at the Institute for Countering Digital Extremism and Geoff Sidoli, MSW, LCSW.

Thank you.

This report was commissioned and published by Thorn. Thorn is a 501(c)(3) organization with a mission to transform how children are protected from sexual abuse and exploitation. For more information about Thorn, please visit our website: www.thorn.org.

Research team

Amanda Goharian, Thorn
Alexander Slotnick, Independent Threat Researcher & Subject Matter Expert

Suggested citation

Thorn. (2026). *Advancing Response to Sadistic Online Exploitation in Networked Youth Environments.* https://info.thorn.org/hubfs/Research/Thorn_SOEResponse_Report_2026.pdf.

CONTENT WARNING: This report focuses on an evolving threat landscape, inclusive of crimes against children that are disturbing and distressing in nature. The report covers topics associated with child sexual abuse, self-harm, suicide, homicide, gore, disordered eating, animal brutality, and physical acts of violence. We encourage readers to take care while reviewing it.

Executive Summary

Sadistic online exploitation (SOE) reflects a significant shift in how risk and harm emerge for young people in digital spaces. Unlike other forms of exploitation, SOE manifests as primarily youth-driven, networked environments that are socially structured around harm itself, where demonstrated tolerance of, and participation in, harm function as mechanisms for group belonging and status. Within them, adolescents are not only the primary victims but also the primary active participants in harming others, achieving status through escalation. In these environments, harm spreads quickly, intensifies rapidly, and becomes increasingly difficult for participants to disengage from.

SOE manifests as youth-driven, networked environments where engagement is structured through harm, with violence, humiliation, and exploitation functioning as mechanisms for participation, belonging, and status.

Across the globe, practitioners are increasingly encountering SOE cases, often at points of acute crisis, but with limited operational clarity and response cohesion. While reported case volumes are relatively few compared with other forms of child sexual abuse and exploitation, SOE cases already reflect disproportionately severe harm. Moreover, available data related to SOE's scale reflect serious constraints associated with detection, reporting, and classification that suggest significant underreporting.

Building on Thorn's broader portfolio of work addressing evolving forms of technology-facilitated child sexual abuse and exploitation, this report draws on field interviews with more than 30 practitioners across eight countries to understand how SOE is currently encountered in practice.

The report finds that current response systems are under strain and fundamentally misaligned with the nature of SOE. Existing approaches are designed for more discrete threats and clearly defined roles; but SOE operates as a fluid, multidimensional threat ecosystem. Across practitioner interviews, five core challenges consistently emerged:

1. **SOE networks are accelerated social conditioning environments.** Youth engaged in them are rapidly conditioned through exposure to, tolerance of, and participation in harm, resulting in risk progression that is earlier, broader, and more embedded than current systems are designed to detect or disrupt.
2. **Current frameworks fail to capture the threat.** Because SOE spans multiple threat domains simultaneously, existing classification and risk-assessment models, oriented to single domains, are ineffective in addressing the fusion of threat modalities, roles, behaviors, and motivations contained within SOE.

3. **Unified intelligence gets fragmented by design.** Interconnected intelligence signals are splintered at the point of intake across platforms, reporting systems, and agencies, resulting in delayed, disproportionate, and partial investigations.
4. **Coordination is not backed by governance.** No embedded governance mechanisms exist to align response across actors and sectors, resulting in uneven, inconsistent, and fragile forms of coordination and collaboration.
5. **Incentives discourage system-wide adaptation.** Response institutions are optimized for their own mandates, not collective outcomes across systems, resulting in resistance to change and limiting sustained progress.

Addressing these challenges requires a collective shift from reactive, disconnected responses toward coordinated, system-level approaches. The report outlines priority actions within three key horizons across the life cycle of SOE engagement and disruption:

Horizon 1 — Enable earlier identification

- Anchor awareness in observable behaviors to encourage parents, educators, and others to intervene earlier in the progression pathway.
- Establish media reporting guidelines to reduce amplification of notoriety dynamics while still educating the public about early risk signals.
- Introduce and expand targeted friction in online "gateway" environments[1] commonly used for recruitment by SOE groups.
- Build "linkage literacy" among professionals in common system entry points so digital exploitation dynamics are consistently identified in initial assessments.

Horizon 2 — Unify system response

- Equip specialized responders with SOE-specific assessment models that integrate multidomain expertise into a shared threat perspective.
- Expand platform detection to act on behavioral patterns and network signatures to enable enforcement against coordination dynamics.
- Decouple threat intelligence from evidentiary thresholds to increase disruption effectiveness.
- Build coordinated, hybrid response structures that are capable of preserving and acting on cross-domain intelligence.

Horizon 3 — Build long-term capacity

- Develop and scale "exit pathways" that provide credible alternatives to the social and psychological functions of SOE networks.
- Extend support to secondary victims, including caregivers of engaged youth and first responders with exposure.
- Invest in prevention as a core system function.

[1] *Gateway environments* are identified by SOE groups as places to target recruitment, including specific game experiences within gaming platforms; forum aggregators; and vulnerability-oriented online communities, like those dedicated to specific mental health diagnoses or identity exploration.

Background

Forms of sadistic exploitation[2] involving children have long been around online and even predate the internet. However, within the past decade, new iterations of sadistic exploitation have emerged online that show a clear divergence from previously documented forms (Fig. 1). These emergent forms are characterized by youth-driven, networked online ecosystems with a "nexus to violent online groups"[3] that encourage child sexual exploitation alongside a broader array of high-severity harm types.

SOE environments are defined by two core features: (1) the central role of adolescents, who represent the primary victims and perpetrators within them, and (2) an engagement model structured through harm itself. SOE groups are organized around the consumption and production of violence, humiliation, and exploitation. Within them, harm functions as the entry point into participation, and severity operates as social currency. As behavior becomes more extreme, it signals dominance, with notoriety mediating the assignment of status.

These dynamics establish competitive conditions that rapidly accelerate escalation and produce a higher baseline level of harm severity than more discrete forms of exploitation. Victims may experience significant psychological and physical harm, while participants engaging in harmful behaviors against others face escalating risk, moral injury, and potential durability in their behaviors that resist disengagement.

SOE produces a threat environment that is both diffusely networked and inherently multidimensional. Evolving terminology has been used to describe these dynamics across sectors—including *SOE*, *nihilistic violence*, *violent online networks*, and others[4]—reflecting different institutional lenses rather than fully discrete phenomena. For the purposes of this report, *SOE* is used to center the child safety implications of this broader threat environment.

Understanding the current scale of SOE is both urgent and inherently challenging. According to the most recent CyberTipline report published by the National Center for Missing and Exploited Children (NCMEC), there were a total of more than 1,300 reports associated with SOE in 2024.[5] While the CyberTipline numbers for 2025 are not yet available, it is anticipated they will have at least doubled.

The diffuse and rapidly evolving nature of SOE, limited public awareness, significant barriers to victim disclosure,[6] and the voluntary and uneven nature of platform detection and reporting

[2] Defined as the intentional infliction of physical and psychological harm, humiliation, and degradation as intrinsic to abuse acts for someone else's benefit.
[3] 2024. NCMEC. CyberTipline Report.

[4] E.g., "Com." 2025. Smith, P. Com/764: Transnational Abuse, Extortion, and Cybercrime Networks Targeting Youth. Canadian Anti-Hate Network.
[5] 2024. NCMEC. CyberTipline Report.
[6] This includes both fear of retaliation and exposure, as well as the complex roles some victims occupy within these networks. In some cases, victims may be coerced into, be pressured toward, or become actively involved in the exploitation of others, creating additional barriers to disclosure due to the perceived or actual risk of self-implication.

thresholds all constrain visibility into the full scope of victimization that is occurring.

For this reason, CyberTipline numbers should be considered alongside other available indicators. Public reporting notes that more than 29 countries have SOE cases, with over 2,700 victims in prosecuted cases[7]; the Federal Bureau of Investigation (FBI) has reported more than 350 investigations across all of its field offices.[8] Most recently, American University's Polarization and Extremism Research and Innovation Lab launched a resource that identifies nihilistic violent extremism incidents across 43 countries.[9]

Importantly, however, these indicators of scale are neither directly comparable nor additive. Each reflects different dimensions of a shared ecosystem rather than a single, bounded threat at scale. As a result, current data should be understood as partial and directional rather than comprehensive. What's clear is that while initial attempts are underway to document its scale, our collective perception of it remains immature and early stage. This also means that in coming years, it is likely that the reported scale of SOE will increase, reflecting potential shifts in prevalence, alongside improved detection, reporting, clarity in classification, and cross-sector alignment.

---

[7] 2025. Argentino, M.A. Beyond the Headlines: Arrest Data and Drivers of Nihilistic Violent Extremism in the Com Network. *From the Depths* (personal blog). 2025. Malkki, L., et al. Violence-Focused Online Communities. RADIA, University of Helsinki.

[8] 2025. National Counterterrorism Innovation, Technology, and Education Center. Prosecuting Nihilistic Violent Extremism: An Examination of Federal and State Charges Against 764 and Related Networks.

[9] 2026. Polarization and Extremism Research and Innovation Lab. The NVE Tracker. American University. Accessed April 30, 2026.

Fig 1 | **Comparative Patterns in SOE: Historical vs. Emergent**

Dimensions	**Historical Patterns**	**Shared Features**	**Emergent Patterns**
Motivation(s)	Primarily sexually motivated (paraphilia-driven)	Intentional infliction of physical and psychological harm, humiliation, and degradation for personal benefit	Centered on social status, belonging, and group acceptance; status achievement is a dominant driver[10]
Offenders	Predominantly older adult male perpetrators	Presence of both individual and networked offenders; some display antisocial or oppositional defiant disorder pathologies	Predominantly adolescent and young adult males (aged 11-25); in some cases, observed neurodivergence and/or underlying mental health concerns,[11] as well as substance abuse or dependency
Offender Dynamics	Often isolated individuals or small groups of coordinated offenders with limited group identity communicating via transactional and opportunistic interactions for selling/distribution of child sexual abuse material (CSAM)	Some degree of coordination and social-reinforcement of offending behavior; shared tactics and techniques (e.g., grooming manuals)	Digitally native, decentralized networked ecosystems with strong and intense group dynamics, inclusive of bespoke group identity, branding, language, and iconography; multiple grievances and high psychological distress and extreme amount of time online (e.g., terminal usage)[12]
Mechanisms for Perpetration	Direct and indirect access to children; offender communities on the darkweb	One-to-many perpetration; grooming, coercion, production and distribution of CSAM, cross-platform clear web dynamics	Many-to-many perpetration; youth-driven exploitation of other youth, victim-to-victimizer offending dynamics[13]; perpetrators will engage in secondary and tertiary harm by directing other youth to perpetrate
Relationship to Broader Online Harms	Generally distinct from other online harm ecosystems	Some overlap in tools (e.g., VPNs, spoofing, personally identifiable information exploits) and platforms (e.g., gaming and social media, Telegram)	Convergence with subversive violent online subcultures (not always ideologically driven) and cybercrime communities (e.g., hacker and/or crypto scam communities)

[10] There appear to be some parallels here with prior conceptions of sadistic personality disorder (SPD). SPD was proposed in the DSM-III-R as a diagnosis warranting further study, defining it as "characterized by a pervasive pattern of cruel, demeaning, and aggressive behavior, not directed toward only one person, and not only for the purpose of sexual excitement." 1987. Diagnostic and Statistical Manual of Mental Disorders (DSM), Third Edition (III), Revised (R). Pg. 430. SPD was not carried forward in subsequent editions of the DSM based on clinical concerns with its perceived overlap with other diagnoses, lack of empirical support, and concerns with how the diagnosis could be used in legal proceedings. Also see, 2004. Millon, T. Personality Disorders in Modern Life. John Wiley & Sons. Pg. 535.

[11] The prevalence and significance of these factors are not yet independently supported by robust evidence and require further empirical research to evaluate any potential associations.

[12] 2025. Rousseau, C., et al. Ideological and Nihilistic Violence in Adolescents Referred to a Specialized Clinic for Violent Extremism. *Canadian Journal of Criminology and Criminal Justice*. Pg. 40.

[13] Clinical practitioners noted that within this dynamic, offending motivations may also include pressure to comply alongside self-protection and appeasement.

Research Methods

This report draws on a qualitative research design combining a targeted literature review with semistructured interviews with practitioners across the response ecosystem. This approach captured both documented knowledge and practitioner insight within a rapidly evolving threat landscape.

LITERATURE REVIEW

A comprehensive literature review of more than 50 publicly accessible reports and documents related to SOE was undertaken.[14] The corpus of review included academic research, government threat assessments, nongovernment organization (NGO) and industry reports, investigative journalism, and criminal legal filings across multiple countries. Multiple key terms[15] were used to identify sources, with additional literature identified based on its inclusion as citations within other primary sources.

QUALITATIVE INTERVIEWS

Hour-long, semistructured interviews were conducted with 35 participants across eight countries[16] between January and March 2026. A network-based recruitment approach was applied and yielded participation that covered a range of roles and expertise across the ecosystem. Inclusion was exclusive to individuals with direct or adjacent professional experience responding to SOE.

Specifically, the sample included:

Expertise Category[17]	Number of Participants
Academics	4
Frontline responder (non–lawenforcement)[18]	7
Industry	4
Law enforcement	10
Nongovernmental organization	10

The privacy of individuals who participated in this research remains essential. All participant responses have been anonymized and aggregated within this report. Formal consent was required and secured prior to participation in the research.

APPLIED THEORY

The presentation of insights in this report applies an adapted socioecological systems approach, used here to examine how interconnected actors, across platforms, policy, law enforcement, and civil society, interact within a broader response architecture. The report uses *systems* as an umbrella term to refer to this set of actors and structures collectively, unless otherwise specified.

[14] For a list of the literature reviewed, send a request to research@thorn.org.
[15] Including SOE, nihilistic violent extremism, violent online groups/networks, and the Com network, as well as the specific names of SOE "groups" within the broader network.
[16] Geographic coverage included practitioners working in Australia, Belgium, Canada, Denmark, Finland, France, the United Kingdom, and the United States of America. All interviews were conducted in English.
[17] Many of the participants interviewed have areas of expertise that cross multiple categories. Primary categories were determined based on the perspective shared during the course of each interview.
[18] Including clinicians and those working at advocacy or reporting organizations.

Current State of Challenges

Across field interviews, practitioners described strain surfacing from five key hurdles: digital environments that operate as developmentally harmful social conditioning mechanisms; existing conceptual frameworks poorly calibrated to emerging threat patterns; vertically organized response structures that institutionally fragment threat intelligence; an absence of governance mechanisms to champion coordination across domains and jurisdictions; and institutional incentive structures that constrain adaptation.

Viewed collectively, these challenges reflect a structural misalignment between a rapidly evolving threat landscape and the response systems designed to address it. What follows is an examination of each challenge in turn, outlining its underlying dynamics and the operational effects it produces.

HURDLE 1

SOE networks function as accelerated social conditioning environments for youth

A central challenge identified in both the literature and practitioner interviews is the nature of SOE networks themselves, representing forms of "dystopic youth culture."[19] These environments operate as rapidly evolving subcultures characterized by the rejection of conventional norms and the use of transgression as a marker of status. In this way, SOE networks function as high-intensity social conditioning environments, where social connection is structured through coercive forms of belonging that are reinforced during a key point in development: adolescence.[20]

Social connection is structured through harm, representing coercive forms of belonging that are reinforced during a key point in development: adolescence.

Many practitioners described how SOE networks do not emerge in isolation and instead operate within mainstream digital platforms (e.g., Discord, Facebook, Gmail, Instagram, Snapchat, Roblox, TikTok),[21] conditions, and norms that shape how young people experience connection, visibility, and social standing more generally. These conditions include:

- **Persistent and ambient forms of connectivity**, including defaulted notifications, "always-on" group chats and direct messages, and interconnectivity across platforms;
- **High-volume content sharing**, including sharing sensitive and personal information with online-only contacts and high-volume image sharing among youth;
- **Status visibility**, including likes, followers, views, virality, and "influencer" status; and

[19] 2025. Rousseau et al., Pg. 32.

[20] A developmental period shaped by identity formation, peer influence, and sensitivity to status.

[21] 2025. Institute for Strategic Dialogue (ISD). Networks of Harm: A Victim-Centric Information Resources on the 764 Sextortion Network. This is also well documented in criminal court filings associated with SOE cases that were included in the literature review.

- **Algorithmic exposure to subversive norms and harmful content**, including misogyny, hate speech, gender-based violence, self-harm, and nonconsensual intimate imagery.

Together, these conditions create an enabling environment for SOE networks. They make harmful groups easier to encounter and engage with, while also becoming harder to recognize early. In practice, this compresses the timeline from initial contact to active involvement, accelerates escalation, and creates conditions in which a young person's vulnerability can be more easily targeted and exploited.

The role of "gateway" environments was also elevated throughout interviews, including gaming spaces,[22] vulnerability-centered communities,[23] and extreme content ecosystems.[24] Practitioners specifically identified the role these environments play within SOE as places that concentrate vulnerable youth and serve as tactical access points for recruitment.[25]

Certain foundational vulnerabilities were also discussed in this context, with adolescence itself emerging as the most consistently elevated risk factor.[26] As a critical developmental stage, adolescence is marked by heightened sensitivity to belonging and social status, increased reward-seeking behavior, and reduced capacity for risk appraisal. Within SOE networks, these traits are actively exploited, making adolescents particularly susceptible to rapid conditioning and coercive group dynamics, and escalating harm.

Practitioners also anecdotally noted a higher prevalence of some underlying cognitive and mental health vulnerabilities among individuals involved in SOE, both as victims and perpetrators. These included autism spectrum disorder (ASD), anxiety, borderline personality disorder (BPD), depression, eating disorders, oppositional defiant disorder (ODD)/psychopathy, substance abuse, and suicidal ideation. Practitioners described how these conditions may further heighten susceptibility to manipulation, intensify dependency on group validation, and reduce resilience to coercion.[27]

Practitioners described victimization within the groups as often following recurring patterns, where participation in harm becomes both a mechanism of control and a pathway for threat propagation. Initial engagement often begins with attention and validation to rapidly establish trust and emotional dependence. This is followed by a request for content, often benign content involving a demeaning "task,"[28] self-generated CSAM or self-harm content, or petty forms of nonsexual criminal activity,[29]

[22] E.g., Fortnite, Minecraft, Playstation Network, Roblox, Steam, Xbox Live. 2025. ISD. Networks of Harm. Pg. 7. This is also documented in criminal court filings associated with SOE cases that were included in the literature review.
[23] E.g., targeting certain mental health diagnoses, sexual identity, or eating disorders, as well as forum aggregators, like Disboard.
[24] E.g., dedicated to "awful but lawful" content like gore, death videos, rape videos, and school shooting games.
[25] 2025. ISD. Networks of Harm. Pg. 9. This is also documented in criminal court filings associated with SOE cases that were included in the literature review.
[26] 2025. Rousseau et al.

[27] The specific targeting of these vulnerabilities by SOE groups is also highlighted in the literature (2025. ISD. Spotting the Signs: Recognizing and Responding to Subcultures of Nihilistic Violence. 2025. Resolver. Critical Harm Intelligence Briefing: Weaponized Loneliness.) and is documented in criminal court filings associated with SOE cases.
[28] E.g., "write/carve my name on your body and send me a picture."
[29] E.g., slashing tires, breaking windows/"brickings," graffiti/"tagging."

which is then used to establish submission and secure sustained compliance and control. Risk and harm become rapidly escalated through competition and reinforcement.

Practitioners were careful to note that levels of participation span a continuum of roles, including passive observers, active participants, victims, and perpetrators. For some, victimization and perpetration become intertwined, as young people are both exploited and incentivized to exploit others to secure their own status within the group. At more advanced stages of engagement, a young person's identity becomes fused with their participation, increasing the durability of antisocial behaviors and making disengagement significantly more difficult.[30]

At more advanced stages of engagement, identity becomes fused with participation, increasing the durability of antisocial behaviors and making disengagement significantly more difficult.

Impact

These dynamics fundamentally shift where and how risk develops. SOE is not simply a content problem, but a networked social system that produces and sustains harm through social stratification. Within broader digital norms, SOE networks operate as conditioning environments, functioning, for some participants, as primary peer systems. Through offering highly interactive subversive subcultures, SOE spaces actively shape and reinforce identity development, hierarchy, social standing, and power dynamics. In them harm, humiliation, escalation, and extreme forms of violence are commodified into currencies for status and acceptance within the group. As a result, critical stages of risk progression occur well before existing systems are designed to detect or respond to them.

Current response frameworks remain oriented toward high-certainty indicators, such as CSAM or credible threats of violence, that typically emerge at later stages of escalation. Earlier signals, including behavioral shifts, preoccupation with harmful content,[31] and initial participation in network dynamics, occur prior to these thresholds and are rarely recognized or interpreted as actionable.

This misalignment creates a systemic delay in collective response. By the time interventions activate, the underlying socialization process is already well established,[32] and existing interventions are not designed to disrupt it or support disengagement with prosocial alternatives. Presenting cases are frequently interpreted as isolated or spontaneous, rather than as products of a social system that conditions and reinforces harm, resulting in ineffective threat disruption.

[30] Participation at this level of engagement typically represents an overwhelming and significant amount of daily time (e.g., more than 10 hours a day).

[31] E.g., gore, violence/death videos, mass casualty footage or simulator games, animal cruelty/crushing content, sexual and gender-based violence.

[32] Some clinical practitioners shared experiences in treating SOE-engaged youth, where the child knew which treatment strategies would be used (e.g., trauma measures) because the group had proactively prepared them to specifically resist them.

HURDLE 2

Existing classification frameworks fail to capture the multidimensional nature of SOE

A second challenge lies in the limitations of existing classification frameworks. Practitioners consistently described a mismatch between the hybrid threat environment of SOE and evaluation models designed for discrete threat categories. While overlap across threats is not new, SOE reflects a convergence of multiple high-severity behaviors[33] that current frameworks are not equipped to assess simultaneously.

Many practitioners described this challenge in the context of risk assessment.[34] Current risk-assessment frameworks are generally aligned to specific domains — typically either child safety or counterterrorism[35] — that rely on assumptions about the nature of the threat and follow relatively distinct models with identifiable roles, progression patterns, and intervention points. Practitioners described how these models break down in the context of SOE, where roles, behaviors, and motivations may be interdependent and intertwined across both domains. This is further exacerbated by the dominance of youth actors within SOE environments where developmental vulnerability complicates perceptions of culpability, susceptibility to influence, and the complexity of determining proportionality in response.

This challenge also extends into victim service frameworks where eligibility, assessment, and intervention models often rely on clear distinctions between victims and offenders.[36] In SOE, this distinction breaks down where roles overlap and, in some cases, may be cyclical. In interviews, practitioners consistently described "victim-to-victimizer" progression pathways, where a young person may initially be victimized and go on to actively participate in, and even direct, the victimization of others. This dynamic produces role ambiguity and uncertainty in whether related cases fall within victim services or justice pathways.[37]

Practitioners further described a lack of evidence-based service protocols that encompass victim-centered care when a young person is both harmed and causing harm — particularly in cases where offending behavior is severe, prolific, prolonged, and/or has become central to their identity.[38]

Impact

This challenge results in investigations and assessments that are incomplete and variable from the outset. Responses often begin

[33] Often integrating child sexual abuse and exploitation, sadistic violence, extremism, cybercrime, and high coercive control dynamics.
[34] 2025. Rousseau et al.
[35] 2026. UK House of Commons. Combatting new forms of extremism.

[36] E.g., Forensic specialist interviews may be procedurally required to cease when a victim reveals offending behavior, due to conflicts of interest for the forensic interviewer.
[37] For some, this role duality, where one individual is both a victim and a subsequent victimizer of others, has some similarities to the "enforcer" or "bottom girl" role dynamic within sex trafficking. Practitioners also pointed to this dynamic as one of the most frequently encountered challenges in early intervention, with victims presenting as active participants in SOE offending at the point of first contact with services or law enforcement.
[38] There is some literature that explores victim-to-victimizer dynamics in other contexts: 2014. Ruback, R.B., et al. Why are crime victims at risk of being victimized again? Substance use, depression, and offending as mediators of the victimization-revictimization link. *Journal of Interpersonal Violence*. 2018. Plummer, M., et al. The Cycle of Abuse: When Victims Become Offenders. *Trauma, Violence, & Abuse.*

with attempts to reconcile competing frameworks, requiring elements of the threat to be translated across domains. This process is neither immediate nor standardized. Rather than producing a unified understanding of progression, some aspects are overemphasized, while others are deprioritized, mistranslated, or missed altogether. As a result, broader SOE risk trajectories remain obscured, limiting the effectiveness of imposed interventions.

For instance, in child safety frameworks, children are *prima facie* victims: nonculpable, manipulated, and coerced. In contrast, extremism frameworks, primarily directed to adult populations, are oriented to the individual as an active agent, making choices within a broader environment of extremist or ideological influence. These contrasting perceptions of agency meet inherent tension in application to SOE, where they produce conflicting understandings of the same individual and behaviors.

Role ambiguity creates additional variability. In the absence of a clear evidence base, practitioners rely on adapted or improvised approaches, with decisions around support, diversion, and/or prosecution often made ad hoc. This increases the risk of potentially harmful outcomes.

Critically, effectively addressing role fluidity in SOE does not diminish victimization or justify harm. Rather, it reflects the need for assessment models that are capable of addressing both experiences simultaneously without defaulting to frameworks that exclude one in service of the other (i.e., models that are capable of treating behavior as both problematic and symptomatic).

HURDLE 3

Unified threat intelligence is structurally fragmented by design

A third challenge emerges as conceptual misalignment becomes embedded within operational systems. Across platforms, reporting mechanisms, and law enforcement, threat intelligence is organized within domain-specific categories, each aligned to distinct mandates, legal thresholds, and areas of expertise.

Platforms function as both the primary detection layer and the first point of fracture in unified threat intelligence. Trust and safety operational functions are typically structured around discrete policy categories for their products and services. Often this involves distinction between misuse types, including child safety, fraud, and extremism, with specific detection systems, escalation protocols, and enforcement actions calibrated accordingly. In SOE, where behaviors span multiple categories and often migrate across platforms, interdependent signals are processed within separate workflows on separate platforms, limiting the ability to identify broader patterns of coordinated harm.[39] This challenge is exacerbated by uneven industry awareness of SOE; some platforms have developed specialized detection approaches, while others remain unaware of the functional role their platform has within SOE networks.

This hurdle also extends into public reporting mechanisms and law enforcement investigations, which adhere to strict operational mandates. In reporting systems, submission requirements align with specific threats or types of content; thus,

[39] 2025. Resolver. Critical Harm Intelligence Briefing: Weaponized Loneliness.

content types that are interrelated in SOE often get separately routed to different institutions. In law enforcement, initial case classification impacts jurisdiction, authority, and resourcing, determining which legal statutes, evidence, and remedies are applicable and prioritized in the immediate response.

In practice, this often manifests as a divide between counterterrorism and crimes-against-children investigative powers, each with distinct thresholds, authorities, evidentiary requirements, and investigative approaches. Cases that present with ideological signals or pathway-to-violence indicators are routed through counterterrorism channels, where action depends on demonstrating ideological motivation or material support. This is difficult in SOE cases, where ideological elements are often performative,[40] inconsistent, or lacking material to support violations. Conversely, cases that present through explicit content detection or sexual exploitation are processed through crimes-against-children channels, where intervention is tied to the presence of CSAM or clearly defined sexual offenses, and does not extend to recognizing or addressing associated extremism elements.

The transnational nature of internet-based crimes generally, and SOE in particular, layers on additional structural tension within this challenge. In some countries, criminal threat classifications are handled by law enforcement, while counterterrorism classifications are handled by intelligence agencies — often with strict operational mandates that are intentionally regulated to be disconnected. In SOE cases this means that not only are cases not likely to be investigated by a single unit, they may even be fractured across agencies or branches of government within a nation, and then again, across regional boundaries.

Impact

Across these critical layers, the same structural pattern emerges: operational response is organized by presupposed threat categories.[41] Put simply, SOE threat networks operate horizontally across systems that respond vertically. In the context of SOE, this results in the deconstruction of a unified intelligence picture in order to make its component parts actionable within a specific operational domain. In practice, this results in partial case construction at the point of intake, where the full context of harm and future risk become incapable of preservation as different signals get routed through different systems or disconnected altogether. Ultimately, partial cases result in partial investigations, which result in partial outcomes.

This fragmentation is further compounded by the fact that many SOE behaviors, such as coercive self-harm,

Many SOE behaviors, such as coercive self-harm, suicide encouragement, non–ideologically motivated violence, or networked psychological abuse, do not consistently meet the thresholds required to trigger enforcement actions, despite representing high-certainty intelligence signals of SOE.

[40] 2026. Argentino, M.A., & Lindsay, A. Schrödinger's Terrorism: Is It or Is It Not in the Box?. *From the Depths.*

[41] 2026. UK House of Commons. Combatting new forms of extremism.

suicide encouragement, non–ideologically motivated violence, or networked psychological abuse, do not consistently meet the thresholds required to trigger enforcement actions, despite representing high-certainty intelligence signals of SOE. For example, platforms may observe network-specific language, iconography, and coercive self-harm content alongside strong indicators that exploitation is occurring in private channels or encrypted spaces. While the combined signals suggest high-certainty of abuse, there is no mechanism to report the collective pattern of risk indicators, especially if the violative/illegal content required for activation remains undetected. As a result, collectively meaningful intelligence remains unreported and unacted upon.

HURDLE 4

Operational coordination is not structurally embedded across the ecosystem

Institutional rigidity also contributes to a fourth hurdle: coordination and collaboration. While multiple actors are accountable for their individual contributions, no formal governance mechanisms exist to ensure these contributions are consistently integrated within SOE response.

Across sectors of response, including platforms, reporting mechanisms, law enforcement, victim services, civil society, and research institutions, each actor has a unique but partial intelligence vantage point. Platforms observe behavioral signals, account networks, and cross-platform dynamics; reporting systems capture structured disclosures tied to specific, mandated categories; law enforcement develops case-based intelligence linked to individuals, devices, and incidents; and victim services provide insight into harm trajectories and trauma-informed recovery pathways. While these contributions are deeply complementary, they are not, at present, structurally connected in ways that support effective and informed coordination of response.

This absence of a forcing function extends to prevention and long-term disruption. These functions do not sit as clear priorities within any mandate and are often treated as secondary priorities. Without governance structures to elevate and integrate them alongside reactive response, they will remain under-resourced and disconnected from the broader system.

Impact

Because coordination is not an embedded function of the system, it serves as a discretionary one that often breaks down without visibility or ownership, despite having significant impacts on the quality and integrity of response. Rather than a coordinated system, SOE response operates as a patchwork of episodic, fragile, and nontransferable institutional connections within and across sectors, where information and intelligence flow unevenly between voluntary actors depending on access, relationships, and individual initiative, rather than functional accountability. This introduces variability in response, limits scalability, and creates uneven access to coordinated intervention across jurisdictions and systems.

The cumulative effect is a response ecosystem that absorbs increasing coordination costs without developing the structural capacity to integrate them. As a result, response remains

segmented, limiting the ability to prevent escalation, disrupt SOE networks, or build long-term resilience. As SOE continues to evolve across domains, platforms, and jurisdictions, systems that lack supportive governance to coordinate across them will remain persistently outmatched.

HURDLE 5

Institutional incentives constrain system adaptation

The fifth challenge anchors response to institutional incentives. Across the ecosystem, institutional behavior is shaped by liability frameworks, funding mechanisms, and performance metrics that prioritize domain-specific outcomes over cross-system coordination. Institutions are evaluated and resourced based on their ability to perform within their own mandates, rather than their contributions to collective response.

This is perhaps best reflected in how success is measured within them. Platforms prioritize policy enforcement and user engagement; law enforcement prioritizes evidentiary thresholds and prosecutable cases; victim services prioritize stabilization and long-term recovery. Without shared metrics, owned and operationalized through defined governance mechanisms that prioritize collaboration to reflect collective impact, successful coordination lacks coherent measurement, and success in one domain does not translate into success in another. Across these actors, prevention and long-term disruption efforts, in particular, are reinforced as secondary priorities, as they do not produce immediate, measurable outcomes aligned with institutional performance frameworks.

These incentive pressures are further amplified by broader attention dynamics. Media coverage, public scrutiny, and political prioritization can influence which threats receive attention and resources, often reinforcing reactive responses to high-visibility incidents rather than sustained investment in prevention or the quiet work of meaningful coordination.

Impact

As a result, gaps in cross-system collaboration remain structurally preserved and reinforced. Efforts to coordinate across systems often require additional time, resources, and risk,[42] while offering limited institutional return.

In practice, institutional efforts to operate across these boundaries are often delayed, deprioritized, unsupported, or actively discouraged. Collectively, initial discretionary progress is often redirected back into legacy pathways, limiting the system's ability to adapt. Instead, response actors across sectors are incentivized to "stay in their lanes," defaulting to actions that are clearly authorized, measurable, and defensible within their own institutions, despite acknowledgment that they are insufficient in addressing the full scope of SOE. Ultimately, this yields the persistence of well-recognized gaps in coordination and response, even where awareness and capability exist.

[42] Cross-system collaboration often introduces complex navigation of legal and operational uncertainty.

Recommendations

Addressing SOE requires a shift from fragmented, reactive responses toward coordinated approaches that enable earlier identification, integrated assessment, and sustained intervention. To support this shift, the following recommendations are organized across three response horizons that reflect key areas of impact across the life cycle of threat disruption. These horizons distinguish between efforts focused on early identification, system-level coordination, and longer-term capacity-building.

Many of the necessary tools, capabilities, and areas of expertise already exist across the ecosystem. The primary challenge ahead is in intentional adaptation and coordination. In this way, these recommendations represent foundational steps toward longer-term structural evolution, rather than comprehensive redesign.

Horizon 1 — Enable earlier interruptions of SOE engagement by expanding risk identification upstream.

Anchor awareness efforts in observable behaviors vs. full threat comprehension.

Behavioral indicators of SOE are often visible but remain unrecognized or misinterpreted. Across the literature, and within interviews, risk recognition is persistently tied to points of crisis, despite many youth displaying observable behaviors that could have enabled earlier, lower-intensity interventions focused on prosocial redirection.

Awareness strategies should prioritize educating general audiences about observable behaviors associated with SOE that should serve as early prompts for closer attention. These include[43] but are not limited to:

- **Changes in digital behaviors**, including sudden secrecy around online activity; rapid or sustained increases in time spent online; references to multiple or new platforms, or interactions involving pressure, "tasks," or conditional belonging (e.g., referencing "doxxing[44]"); unexplained increases in gaming currencies or other digital currencies (e.g., crypto) and unexplained access to new devices.
- **Changes in physical appearance**, including declines in hygiene, eating, or sleeping habits; covering specific body parts; and unexplained wounds (e.g., cuts, bite marks, burns) or new scars (often appearing as symbols or patterns).[45]
- **Changes in emotional well-being**, including disproportionate anger, anxiety, or fear if digital devices are taken away; incorporation of extreme language and symbols; needing to

[43] 2026. FBI, Boston. Open Letter to Parents, Guardians, and Caregivers.

[44] "Doxxing is the action or practice of obtaining and/or publishing personally identifiable information on the internet, usually with criminal or malicious intent." *USA vs. Cayden Brock Newberry*, Criminal Complaint.

[45] Representative of "fansigning" or "cutsigning" which is "the act of writing, cutting, or carving specific numbers, letters, symbols, names, or insignia onto one's own body." *USA vs. Cayden Brock Newberry*, Criminal Complaint.

"consult" friends online for permission to do things; preoccupation with extreme content (e.g., gore, mass casualty attacks) and/or weaponry; and attempts to control others in their lives, like peers, siblings, or others they perceive as vulnerable.

- **Changes within the home environment**, including the delivery of unexplained gifts or packages for the child; increase in "pranks" that target the home, child, or siblings (e.g., randomly delivered pizzas, prank phone calls); unexplained harm to siblings or family pets; changes in family pet responses to the child (e.g., avoidance, fear); strange smells associated with the child's room or bathrooms (e.g., urine, vomit, burning smells); and unexplained police response to the home (e.g., "SWATTing" or "FEDing"[46]).

Importantly, these behaviors do not independently confirm SOE and do not need to co-occur as risk is further mediated by both static (e.g., gender, age) and dynamic (e.g., life experiences, behavioral frequency) factors. In this way, the value of increasing recognition of observable behaviors often associated with SOE lies in triggering earlier protective forms of proportionate engagement and intervention with the child displaying them.

Establish media sensitivity guidelines.

Broader information ecosystems also shape how risk is recognized. Overly detailed media coverage or sensational reporting focused on harm severity can reinforce SOE notoriety and status-seeking dynamics, while unclear or insufficient coverage that neglects observable behavioral indicators can delay recognition of risk. Establishing media sensitivity guidelines can support more consistent, contextualized reporting on SOE while avoiding amplification of SOE escalation dynamics.[47]

Deploy targeted deterrence and disruption strategies in high-risk environments.

Current SOE disruption efforts underutilize gateway communities as places to disrupt recruitment. Many of these online spaces are not inherently harmful but are actively targeted by SOE actors as tactical recruitment vehicles. Embedding early points of friction and redirection into the user experience that signal certain behaviors for young users to be cautious about could reinforce opportunities for more organic risk recognition. These efforts could also include in-platform reporting flows for when a user does recognize such behavior, so the gateway platform can better understand its functional role within the SOE ecosystem and develop supportive detection models (e.g., language-based scripts related to platform migration).

Build "linkage literacy" across common system entry points.

Across key frontline professions, including healthcare, social services, mental health, education, and law enforcement, uneven

[46] "Swatting is the action or practice of making false emergency calls to police, or other emergency services, to bring about the dispatch of armed police officers (i.e., SWAT teams) to a particular location." 2025. *USA vs. Cayden Brock Newberry*, Criminal Complaint. "FEDing" involves the specific activation of federal law enforcement response in this context.

[47] 2017. Miendl, J., Mass Shootings: The Role of Media in Promoting Generalized Imitation. *American Journal of Public Health*. 2015. Towers, S., et al. Contagion in Mass Killings and School Shootings. *PLoS One*.

awareness of technology-facilitated harms, including SOE, results in the inconsistent inclusion of online dimensions within initial evaluations. This yields partial assessments and variability in treatment as youth presenting with different dimensions of SOE harms are screened for risk differently depending on where they first enter the system.

Professional training across these sectors should be updated to include digital drivers of youth experiences, including networked exploitation. Updating intake protocols, expanding screening questions, and training staff to account for digital risk factors in evaluations would broaden early recognition and better tailor treatment options. These improvements would yield benefits not only for SOE but also for the broader field of technology-facilitated harms.

These updates should also include establishing clear referral pathways to specialized units that are better positioned to interpret and assess more nuanced variables, including cross-platform activity, network dynamics, and escalation risk. Referral pathways should further incorporate clinicians with relevant specialties to address co-occurring conditions (e.g., ASD, BPD, ODD) and other psychological dynamics (e.g., diathesis-stress models) that may heighten vulnerability and shape risk and treatment needs, particularly for young people.

Horizon 2 — Unify concurrent response efforts to reduce operational friction.

Equip specialized responders with SOE-specific assessment guidance.

Once SOE has been identified and routed to specialized responders, the horizontal nature of the threat must be addressed. Developing integrated, cross-domain threat assessment and risk-progression frameworks that reflect the nuance of SOE is critical. Doing so will enable greater standardization in specialized assessment and initial case formulation and result in higher-quality interventions alongside alignment in applicable expertise. Defaulting to the parallel application of competing frameworks should not remain an option.

Such efforts will require intentional collaboration across mental health professionals, forensic specialists, and law enforcement in the development and application of shared assessment protocols, including the development of measures to identify, interview, and intervene. Embedding this multidisciplinary input into framework design will strengthen consistency, defensibility, and usability across contexts.

Specialized responders must also be equipped to assess and address the complexity of role ambiguity and fluidity within their cases. Developing stage-based assessment models, specialized and bespoke interview techniques, and guidance for managing overlapping victimization and perpetration behaviors will support more holistic and proportionate intervention approaches.

Expand platform detection to act on patterns, not just incidents.

SOE groups have distinctive digital nomenclatures, aesthetics, and behavioral patterns; clear indicators include group branding, iconography, structure, and language used. While some platforms have begun to develop network- and pattern-based detection models, these approaches remain limited in scope, confined to specialized teams, or are not embedded into enforcement workflows due to a lack of corresponding policy mechanisms.

To address this, platforms should establish and operationalize policy mechanisms for cross-signal analysis, behavioral modeling, and pattern-based detection to enable more effective identification and enforcement against these networks. These policies can also include enforcement against the common targeting patterns through which SOE networks identify victims and normalize harm prior to direct exploitation. Additionally, they should be paired with policies that address related problematic content and behaviors, which may not be independently violative but function as enabling infrastructure for abuse.

SOE groups often involve hundreds to thousands of users. For this reason, platforms should also pre-position support pathways within pattern-based enforcement actions. While users associated with the groups represent misuse of the platform, not all users involved represent the same engagement and risk level. Strict enforcement without paired integration of support options leaves a critical gap to connect some users with help and/or opportunities for redirection.

At the same time, pattern-based enforcement policies should complement, not replace, content-level detection and enforcement against violative material within identified or suspected SOE communities. This is essential given the diversity of users within these groups, including victims experiencing severe harm. Without this, pattern-based enforcement at the group level will eliminate critical opportunities to surface, detect, and act on abuse occurring within these communities.

This recommendation is particularly important given that a significant portion of industry detection remains reliant on user reporting. In SOE contexts, the users most likely to observe reportable activity are participants within the networks themselves, where social dynamics suppress good-faith reporting. Where reporting does occur, it is often strategically co-opted by one group attempting to dominate another. As a result, signals generated through user reporting tend to overrepresent moments of intergroup conflict rather than the underlying prevalence of harm. This reality reinforces the need for platform detection approaches that operate at the level of patterns and networks rather than isolated incidents.

Decouple threat intelligence from evidentiary thresholds.

Current response challenges highlight how investigative approaches that are focused solely on prosecutable offenses within individual cases constrain visibility into and action in response to the coordinated nature of SOE. Shifting to more intelligence-driven approaches will enable investigative response to act on aggregated signals, resulting in faster and more effective network disruption. This includes developing policies and systems that support adapted investigative frameworks, integration of device-based data across cases, and training practitioners to better interpret and leverage nonevidentiary signals.

Build and fund coordinated, hybrid response structures.

The current structuring of institutional response breaks down unified SOE threat intelligence at the point of intake. This fractures interconnected signals, critically separating them from their fuller investigative context. Coordinated, hybrid response structures responsible for integrating intelligence and aligning collective response are needed to counteract this fragmentation. Importantly, this does not require building entirely new systems from scratch; both child safety and counterextremism domains have established coordination models; however, these models largely operate in parallel. The opportunity ahead is to adapt and extend these existing practices to reflect a level of integration required for an effective SOE response.

This includes formalized and accountable intelligence-sharing pathways, such as dedicated joint task forces[48] or fusion centers, as well as unified intake and triage mechanisms to foster shared entry points capable of ingesting interconnected and cross-domain intelligence signals.[49,50] At minimum, this can be supported through dedicated, cross-trained liaison roles.

These efforts must also be complemented by the development of enabling and scalable technical infrastructure, including pattern-recognition tooling, shared signal databases, and cross-device analytic capabilities.

Vitally, the success of hybrid response structures depends on sufficient funding and resource allocation. Without investment in the expansion — if additional responsibilities are merely layered onto existing systems that are already overextended and resource constrained — they are unlikely to deliver meaningful results. Doing so may even create longer-term challenges by flooding current existing systems that are already struggling to keep pace with intake, triage, and investigation volumes associated with their mandates beyond SOE.

[48] This is being advanced at some national levels — e.g., in October 2025, the Australian Federal Police announced Taskforce POMPILID.
[49] The multidisciplinary team structures within Children's Advocacy Centers in the US and MITRE's ATT&CK knowledge base represent some models.
[50] This is being advanced at some national levels — e.g., the UK's National Crime Agency's Child Sexual Abuse Industry Partnerships Team — and by some NGOs, e.g., Tech Coalition's Lantern Program and the Global Internet Forum to Counter Terrorism's Hash-Sharing Database. However, all current efforts remain dependent on voluntary and discretionary contributions.

Horizon 3 — Expand the scope of interventions to support long-term response capacity and resilience.

Develop and scale "exit capacity" as a core component of response infrastructure.

SOE-involved youth span a continuum of potential engagement levels, and, for many, participation fulfills sociodevelopmental needs related to identity, belonging, and acceptance. This complicates disruption efforts, as simply removing immediate access does not effectively address the underlying drivers of participation.

Effective interventions must therefore be built to incorporate prosocial alternatives and credible exit pathways that can compete with the social and psychological functions these environments provide. Central to these programmatic interventions should be the deliberate integration of protective factors (e.g., stable relationships, prosocial goal-setting) to reduce risk and sustain resilience. Without this, disruption efforts are likely to remain episodic for some youth, with high rates of recidivism.

These efforts must begin with strengthening the evidence base for SOE-specific treatment and recovery approaches capable of redirecting, disengaging, and diverting youth. This includes investment in targeted research and embedding measurement and evaluation into implementation to support early calibration.[51]

Establishing what works across varying levels of vulnerability, engagement, and harm is foundational to improving individual outcomes and enabling scalable interventions that address all outcomes. These efforts must also expand the evidence base related to key factors and variables that influence the transition, for some, from victim to victimizer.

Create tailored support mechanisms for secondary victims.

SOE impacts extend beyond directly affected youth, creating secondary victims, including families and caretakers of involved youth and responders whose duties require exposure. Expanding the suite of available resources to be inclusive of supporting their recovery needs, including addressing secondary trauma, is essential.

For impacted families and caretakers, resources must be inclusive of SOE's role-ambiguity dynamics, oriented to supporting families of youth who have been victimized and families of youth who have harmed others. Such resources must be well tailored to SOE, as the severity and taboo nature of its harms compound shame, shock, and horror. Developing these support resources is critical to reinforcing a youth's immediate stabilizing environment and sustaining recovery over time.[52]

[51] 2025. Rousseau et al.

[52] Some resources developed for addressing problematic sexual behavior among youth, including sibling-on-sibling child sexual abuse, likely offer strong conceptual starting points for this. These include those developed by the National Center for Sexual Behavior of Youth, the Association for the Treatment & Prevention of Sexual Abuse, and the Office of Juvenile Justice and Deliquency Prevention.

For impacted responders, including law enforcement, content moderators, and treating clinicians, tailored resources oriented to fostering responder well-being are necessary to lessen secondary trauma exposure, avoid burnout, and increase professional resilience. This requires embedding support structures that limit harmful exposure, including specialized training and technical tooling, such as presuppositioning mental health resources for responders during their review, inbound content detection and tagging that flags severity features, voice distress detection, and others.

Invest in upstream prevention.

SOE emerges within broader risk environments shaped by systemic factors such as problematic internet use, early exposure to harmful content, and the normalization of exploitative or transgressive attitudes[53] and behavior.[54] Focusing solely on downstream response overlooks these upstream conditions that increase vulnerability and enable recruitment.

Addressing these drivers is essential to reducing the overall pool of youth with elevated risk for engaging in SOE and limiting the conditions that enable SOE networks. This requires population-level approaches aimed at strengthening digital resilience, promoting healthy online engagement, and reducing exposure to high-risk environments for youth. This level of approach will enable prevention to be treated as a core system function rather than an auxiliary responsibility placed on caregivers or individual sectors. To be effective, prevention efforts must be cross-sectoral, integrating public health, social services, education, platform design, and policy approaches.

[53] Including online communities that promote unhealthy aspects of identity, such as involuntary celibate ("incel"), manosphere, and edgesphere communities.
[54] 2025. Rousseau et al.

Additional Considerations

Several practitioner insights that surfaced in the course of this research fell outside the immediate scope of this report. While not exhaustively explored here, these insights highlight dynamics that may shape future risk and response requirements.

- **Video content dominates:** SOE victimization is heavily captured through live-streaming and other video-based features, and practitioners describe how innovation in video-based detection continues to lag behind image-based capabilities. This impacts victim identification efforts and places a significant burden on law enforcement for manual review of long and distressing footage.
- **Language expansion of networks:** SOE threat activity is currently heavily concentrated in English-language environments. Some practitioners forecasted expansion of them into additional languages. This will increase the global reach of SOE threat environments and add complexity to detection, investigations, and intervention.
- **Continued evolution in role dynamics:** Some practitioners described seeing cases that increasingly involve younger females in "enforcer" or "recruiter" roles. This indicates that participation dynamics and recruitment strategies continue to evolve, reinforcing the need for deconfliction of role ambiguity within cases.
- **Commercialization of harmful but lawful content among youth:** Some practitioners described cases that involve youth in SOE networks who are producing and monetizing harmful but legal content, including self-harm material. This introduces new incentive structures that may further entrench participation while complicating detection and intervention thresholds.
- **Convergence with other child exploitation offenses:** Some practitioners mentioned other offender types involved in crimes against children are leveraging SOE networks as access points to victims and content. This includes older offenders with sexual and/or sadistic interests who exploit these environments to identify and groom victims or to access new CSAM.
- **Potential nation-state interaction:** Some practitioners, particularly aligned with extremism domains, referenced the identification of indicators that point heavily to foreign nation-state actors interacting with or enabling aspects of SOE networks. This introduces a new class of adversary into the child safety landscape and raises important implications for operational security, practitioner safety, and response protocols.

Looking Ahead

SOE within networked youth environments marks a fundamental shift in how harm manifests online for young people, introducing a new threat structure that blends exploitation dynamics in ways that challenge traditional categories and response strategies. Despite currently representing a comparatively smaller overall volume of exploitation experiences among youth, the voracity of its hybrid dynamics is likely to persist as a consistent and complicating factor in the broader ecosystem.

Importantly, the findings in this report do not reflect apathy, inaction, or indifference by institutions. They reflect the opposite: systems actively straining to adapt to a threat they were not designed to anticipate or address. Across interviews, practitioners at every level described sustained effort, creativity, and deep commitment to child safety. Their insights also reveal professionals working within real structural constraints, often compensating for systemic gaps through personal dedication and informal coordination. While these efforts are necessary and commendable, reliance on improvisation and individual commitment is not a sustainable substitute for institutional alignment and built-in, cross-system capacity.

Addressing current gaps will strengthen the response to SOE while also improving coordination across systems facing a threat landscape that is increasingly diffuse, hybrid, and fast-moving. Technology-facilitated threats are now not only unfolding across platforms, but incorporating additional dimensions that blend categories of harm and operationalize digital connectivity for acceleration.

What remains clear is the depth of commitment across the response ecosystem. Child safety professionals, extremism experts, platform teams, investigators, policymakers, and advocates share a common goal: protecting young people in environments changing faster than the systems built to safeguard them. The challenge ahead is not whether actors are willing to respond, but whether the response ecosystem can, collectively, evolve at the pace required.

THORN

thorn.org | info@thorn.org