



September Brown Bag

The rise of sadistic online exploitation: What frontline professionals need to know



Thursday, 17 September 2026



September Brown Bag

Sadistic online exploitation (SOE) is an emerging form of online harm that thrives within networked communities where exploitation, humiliation and violence can become pathways to belonging and status. Unlike traditional models of online abuse, SOE often blurs the lines between victimisation and participation, creating significant challenges for prevention and response efforts.

In our September Brown Bag, Amanda Goharian unpacked the latest research on SOE, explored how these environments operate, examined the impact on young people, and discussed opportunities to improve early intervention, detection and cross-sector collaboration to better protect children and young people online.



Amanda Goharian
Director of Research & Insights, Thorn

Audience Q&A

Following a robust session, not all audience questions were able to be addressed during the webinar. Amanda has kindly provided us with her answers to those questions, and ICMEC Australia has included the questions and answers below as written by the author.

Q1: Protective capabilities and resources vary between and even within law enforcement agencies with most policing being reactive/responsive to crime reports, intelligence and other inputs. What proactive measures can police take with SOE, when the reporting data may not reflect a need for police reaction/response?

A: I think one of the biggest opportunities is shifting from thinking exclusively about case response to threat visibility. A challenge with SOE is that many of the earlier signals we see, things like coercive self-harm, suicide encouragement, psychological abuse, or concerning online relationships, may not independently meet a threshold for enforcement. Yet, in the context of SOE these represent meaningful intelligence signals. Proactively, I think there is an opportunity to better connect signals across cases, accounts, devices, and jurisdictions; build stronger relationships with platform

threat teams and adjacent investigative units; and make sure frontline officers know when something that looks like an isolated incident may actually warrant a broader look. E.g., if an officer is responding to a call involving a suicidal teen — does the process provide the space to ask about online influences or contexts or does it ask additional questions to the caregivers about possible changes in the teen's behaviour or home environment? In Thorn's report, we explore the idea of decoupling threat intelligence from evidentiary thresholds. The point isn't to lower the threshold for enforcement. It's to avoid making "can I prosecute this right now?" the threshold for whether information has intelligence value.

Q2: What account behaviours and financial transaction patterns are commonly associated with individuals potentially involved in SOE-related activity?

A: I think there are two slightly different questions here. On account behaviours, our research provided a clearer picture. SOE activity is highly networked and cross-platform, so I would be looking less for a single account behaviour and more for patterns across accounts and environments. That can include movement across multiple platforms or into more private channels, connections to known SOE accounts or communities, use of group-specific language or iconography, very high levels of online activity, and participation in coordinated behaviours like recruitment, coercive "tasks," harassment, doxxing, or circulation of harmful content. Thorn's research also identified unexplained access to new accounts/devices or increases in gaming or digital currencies as potential behavioural indicators. Importantly, none of these independently indicate SOE; their value comes from how they cluster and connect to a broader pattern of activity.

On financial transactions specifically, Thorn's evidence is less developed. Our research surfaced the use of gaming currencies and crypto, overlap with cybercrime and crypto-scam communities, and emerging examples of youth monetizing harmful but lawful content. I anticipate researchers focused on SOE from more of the cybercrime domain have a clearer context of consistent SOE-specific financial signatures, such as particular transaction values, frequencies, or payment methods.

Q3: Are there any keywords that are associated with SOE-related communications between participants? And any trends with monetary values/frequency?

A: There is recognisable SOE-specific language, slang, group branding, handles, iconography and lore, and some communities use systems of points, badges or other

status markers. Thorn's research identified that some platforms are already using network- and pattern-based approaches because SOE groups can have distinctive nomenclature, aesthetics and behavioural signatures. There are also industry working groups specifically oriented around developing, sharing, and maintaining these kinds of threat signals as they evolve. This is particularly important because the indicators are not static, however a limitation is that much of this coordination remains voluntary and dependent on participating companies participating & contributing what they are seeing. So, yes, the capability to identify and maintain these signals does exist, but much of that intelligence is necessarily sensitive and not publicly available.

One example is the Tech Coalition's Project Lantern, a voluntary cross-platform signal-sharing program for online child sexual exploitation and abuse. Lantern allows participating companies to share signals such as usernames, account identifiers, URLs, keywords or codewords, and behavioural indicators so that another company can investigate whether related activity is occurring on its own service. Lantern also includes financial institutions (e.g., Cash App, PayPal, Western Union). That said, financial institutions currently participate in Project Lantern on a receive-only basis rather than contributing their own signals back into Lantern.

For law enforcement, access often depends on participating in the relevant information-sharing mechanisms and working groups, and maintaining relationships with industry partners who are seeing these signals evolve in real time. A publicly available list of keywords or indicators is unlikely to provide the same value, both because the indicators change quickly and because broad disclosure could undermine their usefulness for detection.

Q4: What do you think are the key areas to improve training in SOE for law enforcement?

A: Based on Thorn's work, there are four areas identified to improve law enforcement (LE) training related to SOE:

- First, linkage literacy: disseminating information and knowledge that allows LE across different threat domains to recognise that a case presenting as self-harm, cybercrime, sexual exploitation, extremism, animal cruelty or harassment may be one part of a connected online environment. This could also include updating professional training and intake protocols so digital risk factors and networked exploitation are incorporated into initial assessment.

- Second, role fluidity: officers need to be prepared for young people who may simultaneously be victims, active participants and people who have harmed others. Existing victim/offender distinctions can produce very different responses depending on which behaviour is encountered first and whether it is the only aspect investigated/explored.
- Third, disengagement and exit strategies: LE should understand that removing access to a network or disrupting an account may interrupt the immediate harm without addressing what is sustaining a young person's participation within SOE group(s). Training should include how to assess those underlying drivers, particularly belonging, identity, status, and acceptance, and how to connect young people with credible exit pathways and prosocial alternatives that reduce the likelihood of re-engagement.
- And fourth, cross-domain escalation and referral (e.g., coordinated task forces/fusion centres): knowing when to bring in crimes-against-children investigators, cyber specialists, counter-extremism teams, behavioural-health professionals or other partners rather than trying to force the case into one investigative frame. The underlying problem is that SOE often requires integration & coordination of response across multiple domains.

Q5: You mentioned that recruitment has occurred through platforms such as Discord. Are the SOE communities themselves located on the clear or dark web, or both?

A: Based on Thorn's research, SOE activity is not primarily concentrated on the dark web. We identified activity across mainstream platforms and services including Discord, Instagram, Snapchat, Roblox, Telegram, TikTok, Facebook, and others (e.g., Spotify, YouTube, PlayStation, Gmail). Recruitment into SOE groups often begins in pretty ordinary online environments, including gaming spaces or communities organized around mental health, identity, or other vulnerabilities. Activity can then move into more private or closed spaces. This doesn't mean SOE activity does not occur on the dark web, but one of the important features of this threat is that a significant amount of recruitment, engagement, and harmful activity can occur through mainstream online environments. This differs somewhat from historical patterns of networked child sexual exploitation, where offender communities have been more closely associated with dark-web environments. That said, dark web SOE activity does exist, particularly as it relates to the cybercrime elements (e.g. PII exploits, etc.).

Q6: What are the rates of victims of SOE becoming perpetrators? Do we have this data?

A: At present, I am not aware of any data/evidence that examines the rates of victims of SOE becoming perpetrators. We have enough evidence to say that victim-to-victimizer pathways occur, but we don't yet know how often that occurs, and we don't yet have a strong evidence base identifying which factors make that transition more or less likely. This is specifically one of the research gaps Thorn identified in our report and I am hopeful that in the near future, more evidence will be dedicated to better understanding this.

Q7: Although Satanism, and other anti-social occult/esoteric belief systems form only one part of the problem (and vary in impact), it is very poorly understood. What research is being done to address this knowledge gap?

A: This wasn't something Thorn's research examined as a discrete area, so I'd be cautious about overstating what I can say about the broader research base. What did come through in our work is that ideology, symbols, and belief systems can serve different functions within these communities. In some cases, extreme or transgressive imagery may reflect genuine ideological belief. In others, it may be performative, a mechanism for group identity, boundary-pushing, status, or simply demonstrating willingness to transgress norms. That ambiguity is actually one of the things that makes these cases difficult to interpret through traditional extremism frameworks. For me, the important research question isn't only what is someone claiming to believe or referencing. It's also what function is that belief system, imagery, or symbolism serving within the community? Our research suggests that belonging, status, and participation in harm are often central organizing dynamics, regardless of the specific ideology being elevated. Marc-André Argentino's and Angus Lindsay's relevant work digs into this more in-depth: [Remotely Coerced Violence: 764, The Com Network, and the Hybridization of Threats & Nihilism and Terror: How M.K.Y. Is Redefining Terrorism, Recruitment, and Mass Violence.](#)

Q8: Are there any known online platforms that may host SOE or have high SOE engagement?

A: See response to question 5 - Question 5 & 8 are similar so I answered them collectively.

Q9: From a law enforcement perspective, I am curious as to whether others view current data collection (for suicide and serious self harm) as adequate. If not, how are others encouraging improved data collection, and what agencies are involved? I.e. law enforcement agencies, health sector, Coronial records.

A: This is an area where I'd want to distinguish what Thorn's research directly examined from what I think it points to. We didn't specifically evaluate the adequacy of suicide or self-harm data collection systems, although in our research these systems were frequently identified as current gaps/future opportunities. This was particularly pronounced among platform Trust & Safety teams and LE analysts who described the challenge of not having a formal reporting mechanism for submitting/triaging cases that had high indicators of SOE activity, but the only available content was self-harm or suicide related. An important question for improved data collection is whether subsequent systems for these are able to consistently capture things like online encouragement or coercion, whether other people were directing or witnessing the behaviour, whether it was live-streamed or recorded, what accounts or platforms were involved, and whether there was a broader pattern of activity. To the heart of the question, this points toward a multidisciplinary data problem rather than something law enforcement can solve alone. Health, mental health, law enforcement, child protection, coronial/medical examiner systems, and platforms may all hold relevant information. Thorn's report argues for more formalized intelligence-sharing, shared intake and triage, cross-trained liaison roles, and systems capable of connecting signals across cases.

ICMEC Australia would like to thank Amanda for presenting Thorn's research on the webinar, as well as for taking the time to answer all of the questions provided.

