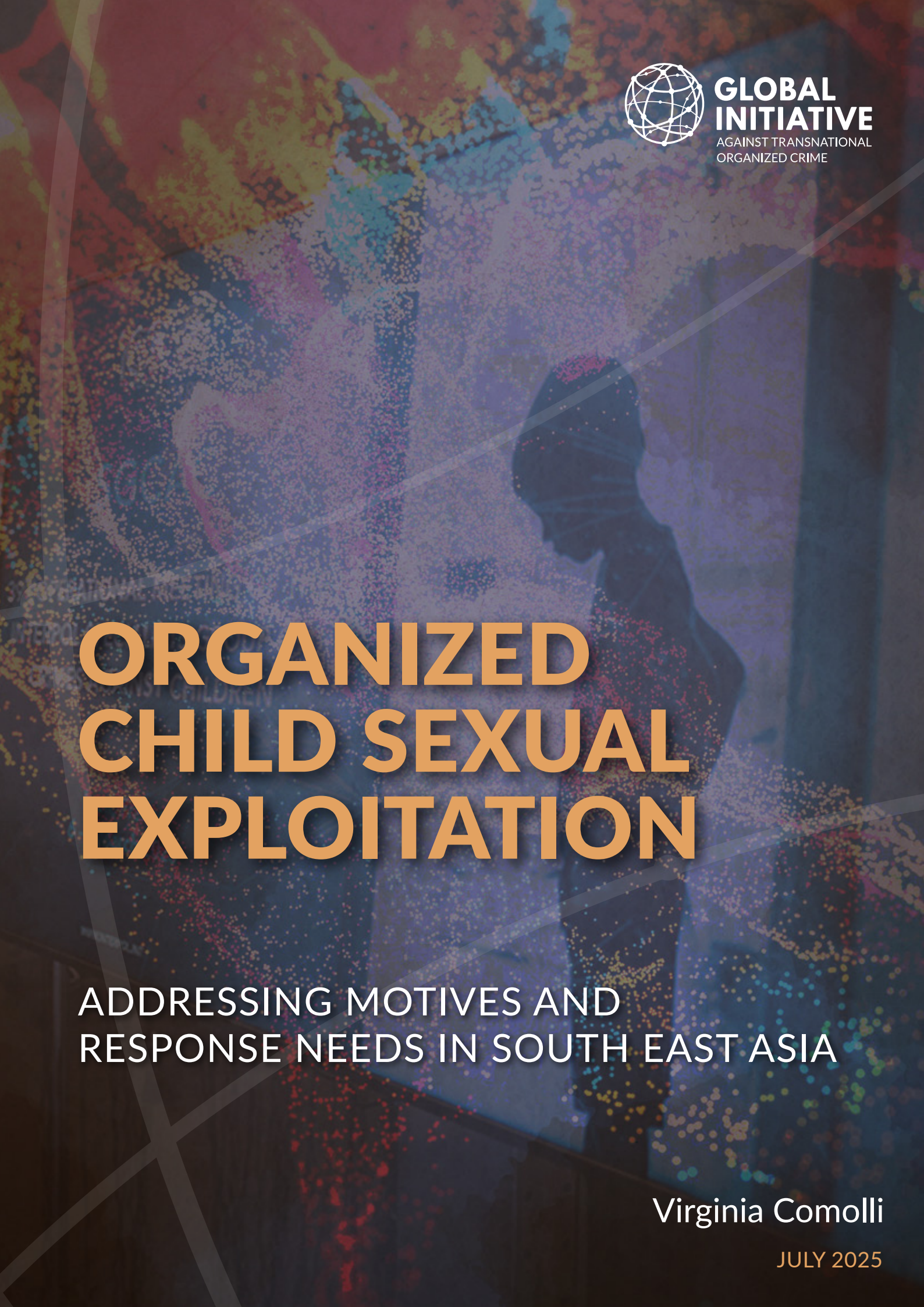


GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ORGANIZED CHILD SEXUAL EXPLOITATION

ADDRESSING MOTIVES AND RESPONSE NEEDS IN SOUTH EAST ASIA

Virginia Comolli

JULY 2025

ACKNOWLEDGEMENTS

The author wishes to thank the civil society actors consulted for this brief who generously shared their knowledge and experience in the areas of child safety and protection. These include, among others, ECPAT International, Crime Stoppers International, the International Centre for Missing & Exploited Children, Evident, ChildFund and the tech industry alliance Tech Coalition.

The author is also grateful to Louise Taylor at the Global Initiative Against Transnational Organized Crime (GI-TOC) for her feedback, and the GI-TOC Publications team.

A special thanks to Jarryd Dunbar, Australian Federal Police, and Smita Mitra, subject matter expert, for their role as external peer reviewers.

This publication has been funded by the Australian Government through the Department of Foreign Affairs and Trade. The views expressed in this publication are the author's alone and are not necessarily the views of the Australian Government.

ABOUT THE AUTHOR

Virginia Comolli is the head of the GI-TOC's Pacific Programme, a portfolio consisting of research, analysis and on-the-ground engagement with local and international stakeholders across Oceania. Previously, as senior expert in the GI-TOC's Asia Pacific Observatory, she conducted research on child sexual exploitation and abuse in Mekong countries. Before joining the GI-TOC, Virginia spent 14 years with the International Institute for Strategic Studies, most recently as senior fellow and head of the conflict, security and development programme.

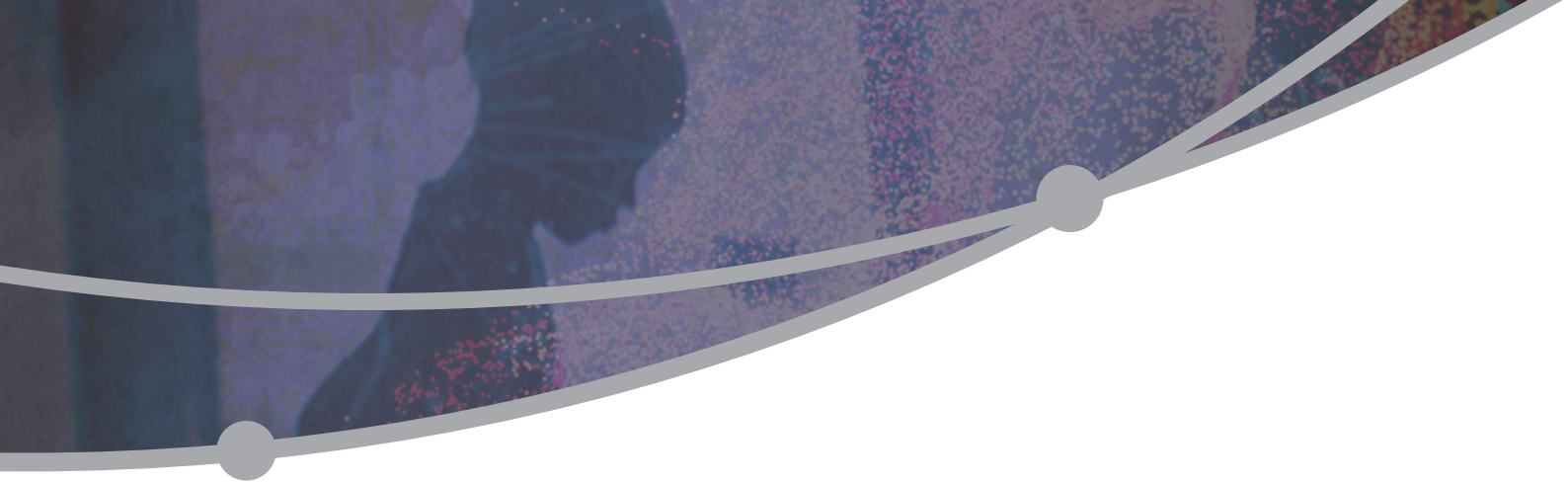
© 2025 Global Initiative Against Transnational Organized Crime.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Global Initiative.

Cover: © *INTERPOL*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS



SUMMARY

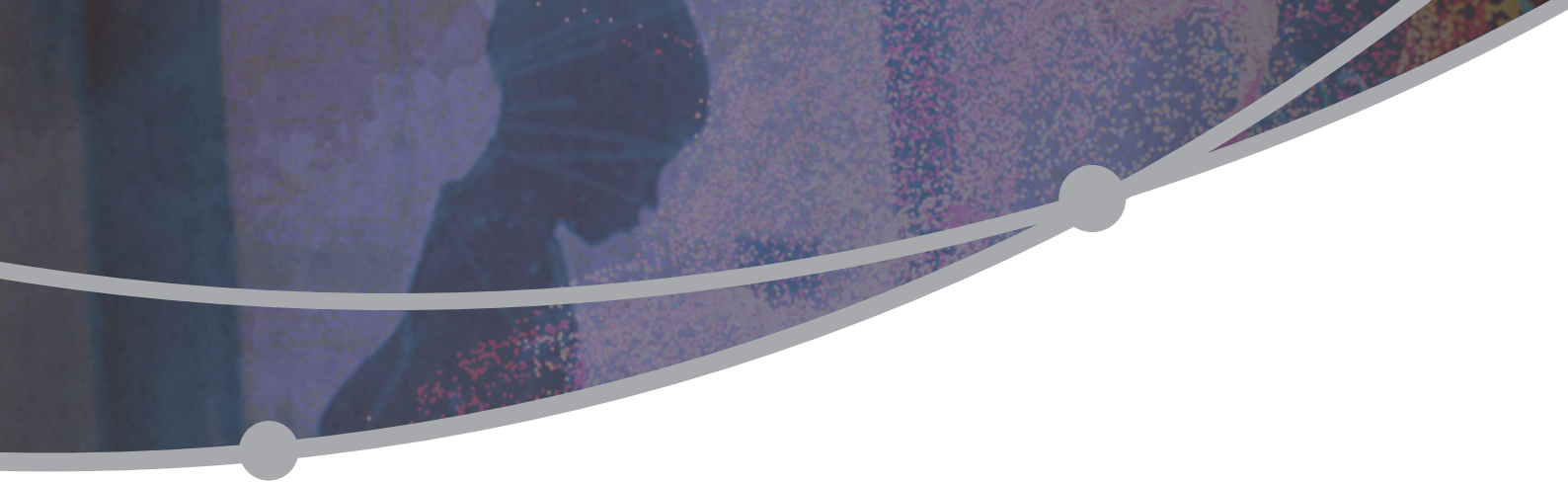
Child sexual exploitation and abuse (CSEA) and online CSEA (OCSEA) lurk in some of the darkest corners of the criminal universe. These labels encompass a variety of online and offline crimes targeting minors of all ages, regions and demographics who become victims of strangers, family members and peers, working alone or as part of international networks. The latter are the focus of this policy brief.

CSEA/OCSEA trends in South East Asia and many other regions of the world suggest that besides gratification-driven individual offenders, an ever growing number of organized criminals are sexually exploiting children for profit. This shift suggests that the way these crimes are understood and combated should be adapted accordingly. The proposed approach includes changing the focus from victim to offender identification, and placing greater onus on public–private partnerships, innovation and collaboration across crime-fighting areas.

In support of this argument, this brief discusses the evolution of some forms of CSEA/OCSEA into organized crime, considers current responses in South East Asia and proposes a set of recommendations.

Key points

- CSEA takes many forms, including in-person contact offending, abuse on demand, and the production and sale of child sexual abuse material (CSAM).
- Since the early 2000s, CSEA has undergone a significant transformation, largely driven by increased digital connectivity and technological advances such as encrypted communications, anonymous payment systems and cryptocurrencies.
- While South East Asia has long been affected by CSEA, crackdowns in the physical realm and in certain countries have led to the displacement of this activity to other regions and platforms, with further displacement likely.
- Offences have become increasingly organized and sophisticated, particularly in relation to the production and dissemination of CSAM.
- Organized criminal groups are increasingly involved in CSEA and OCSEA, motivated by financial gain. Their involvement has intensified the harm inflicted on children.
- The shift towards more sophisticated, networked and organized forms of exploitation underscores the need for an organized crime framework that emphasizes perpetrator identification and the dismantling of networks.



INTRODUCTION

Some countries in South East Asia have become hotspots for CSEA and, more specifically, sexual exploitation of children in situations of travel and tourism. This exploitation happens when offenders, usually but not exclusively from the West, travel to a more vulnerable setting. European, Australian and New Zealand offenders, among others, have found their way to the likes of Cambodia, Thailand and the Philippines.

The high prevalence of these crimes and greater awareness of them have prompted policy, law enforcement, private sector and civil society responses. These interventions, it can be argued, have made contact-offending and cross-border trafficking of minors more difficult. The case of Cambodia exemplifies this trend. Once infamous for the commercial sexual exploitation of children (CSEC) and other forms of child exploitation (linked to so-called volunteerism, for instance), the country saw a marked decline of CSEC prevalence from 15–30% in the early 2000s to just over 2% a decade later, with prevalence among children under 15 registering the most significant decline. A study by the International Justice Mission attributed this trend to the strengthening of anti-sex trafficking measures introduced by the government with the support of coalitions and civil society organizations.[1] Notably, the study – which relied on undercover data collectors – identified 'numerous individuals' linked to the commercial sex industry who feared arrest if they were found guilty of trafficking minors. Similarly, establishment owners had become afraid of anti-trafficking legislation and tried to distance themselves from CSEC.[2]

These developments are, of course, positive. When one market is disrupted, however, there is a risk of displacement to countries with less advanced legal provisions, enforcement and understanding of these crimes.[3] Related to this, and even though little data is available, anecdotal evidence points to cases of sexual exploitation of children in the broader Asia Pacific region, in particular in Pacific island countries such as Fiji or the Marshall Islands, linked to travel and tourism.[4]

A hotel sign prohibiting sex tourism in Phnom Penh, Cambodia. *Photo: GI-TOC*

Contact offending is only one type of CSEA. The Philippines is an internationally infamous hub for the livestreaming of child sexual abuse. Perpetrators from further afield pay facilitators and victims to view the sexual abuse of children, and the same offenders often direct the abuse in real time, requesting specific acts to be performed.[5]

The proliferation of social media platforms and their growing user bases have enabled further digital exploitation, often connected to the production and distribution of CSAM. At the time of writing, for instance, Thai media reported the case of five siblings, all under 18, rescued by the authorities as their family forced them to record 'pornographic videos'. Their eldest sister was acting as a 'recruiter', inviting potential buyers to purchase the videos on a Line chat group.[6]

The surge in 'sextortion'[7] is another case in point. Teenage boys are by far the largest target group for this category of OCSEA, in contrast to other forms of sexual exploitation where most victims are girls.[8] Sextortion trends also show that South East Asia is not only a place where victims are abused by local and foreign offenders; it is also the home of criminals who engage in sextortion activities elsewhere in the world, as the British National Crime Agency made clear when it launched a 2025 online campaign to raise awareness of sextortion among boys.[9]

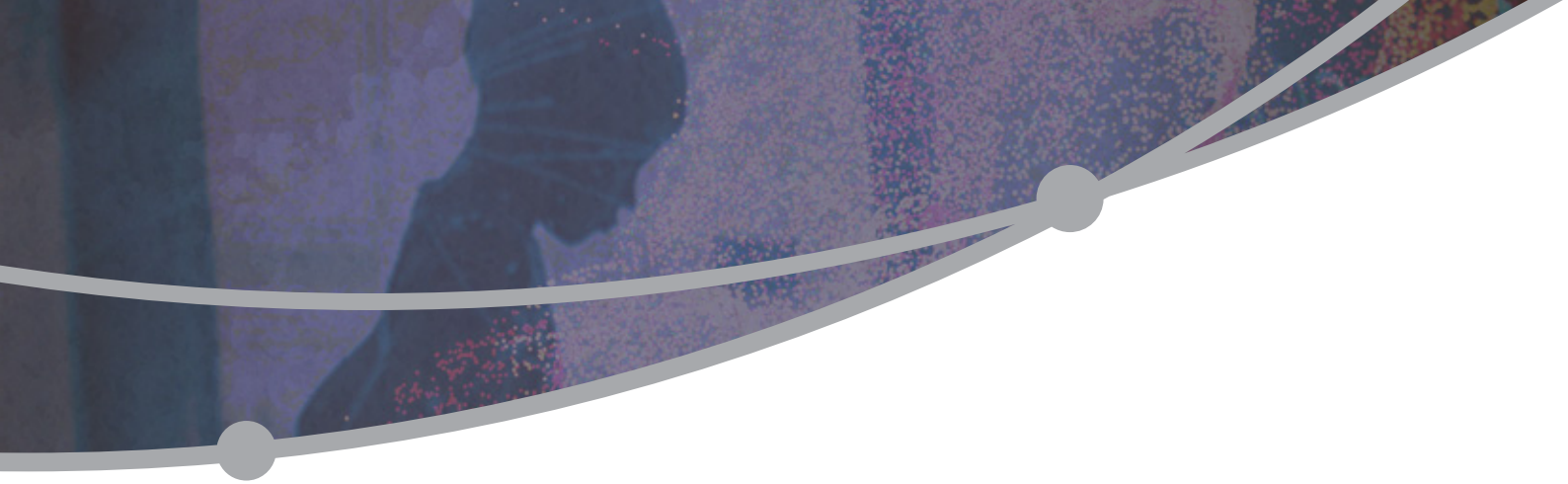
New motives

This digital dimension has affected the motivations behind CSEA, which brings us to the focus of this policy brief. At the Global Initiative Against Transnational Organized Crime we have been discussing whether CSEA/OCSEA is an organized crime. Experts and law enforcement are often divided on this question, and while there is no internationally agreed definition of organized crime, most would agree that it is driven by financial gain. Traditionally, sexual gratification rather than greed motivates CSEA offenders such as paedophile rings whose members trade CSAM. Now, though, organized crime groups or networks seeking to make money have become part of the equation, and may have no interest in the abuse or the abuse material. For instance, in 2022 an investigation by INTERPOL

and police in Singapore and Hong Kong uncovered and dismantled a transnational sextortion ring. The syndicate had extracted payments from victims by luring them into nude chats through a malicious app that also stole their phone's contacts. The criminals would then threaten to send the intimate images to victims' friends and relatives, blackmailing them for tens of thousands of dollars.[10]

Determining whether these crimes amount to 'organized crime' goes beyond a theoretical discussion on definitions. This brief argues that when certain parameters apply – perpetrators operating in a networked way and/or with financial gain as a motive, for example – adopting an organized crime approach would strengthen responses from law enforcement and private sector entities such as tech companies and the financial sector. This switch in approach requires a further important shift from victim identification to perpetrator identification.

Until now, the primary focus has been on victims and victim identification, as seen by available data and literature on CSEA/OCSEA, the awareness initiatives that have been launched and the work of NGOs. These efforts are valuable and much needed but less attention seems to be paid to identifying offenders. Consequently, offenders – and their tactics and motivations – are less well understood, enabling them to continue offending to the detriment of victims.



CSEA/OCSEA AS ORGANIZED CRIME

CSEA trends in South East Asia (and more widely) point to a shift towards organized criminal methods since the late 2000s. Before widespread internet access, exploitation was mostly localized (linked to the tourism and hospitality industry or brothels) and driven by individual abusers or small gangs. From around 2010, the combination of cheap digital technology, mobile internet and anonymizing tools empowered criminals. Extreme poverty in target Asian countries, increasing availability of high-speed internet and a large overseas customer base have provided new opportunities for organized crime groups to exploit children for financial gain.

By the mid-2010s, law enforcement and experts not only recognized that 'livestreaming of child sexual abuse … [was] a significant and emerging threat' but also that 'children [were] made to engage in sexual activity in exchange for payment to the family or to an organized crime group'.[11] In practice, many exploitation rings are structured like criminal syndicates: they are cross-border operations with hierarchies, roles (recruiters, facilitators, payment handlers) and profit motives.[12] In this respect, Operation Endeavour – run by Australian, UK and US law enforcement (2012–2014) – uncovered an organized crime group in the Philippines that livestreamed child sexual abuse to paying foreign customers. Facilitators (sometimes relatives of the children) arranged the abuse on demand in exchange for cash. The investigation spanned 14 jurisdictions, including Hong Kong, Taiwan, Australia, the US and several European countries.[13]

The emergence of cryptocurrencies (including pseudonymous cryptocurrencies such as Bitcoin and privacy coins such as Monero)[14] also prompted a step change: criminals could collect payments virtually untraceably. From the mid-2010s, the increased commercial sale of CSAM on the dark web went hand in hand with a significant expansion of cryptocurrency use on these platforms, which almost exclusively accept this form of payment. The appeal of cryptocurrency derives from the perception of untraceability and therefore the expectation of avoiding detection (although this is not necessarily the case).[15]

Importantly, all the above has seen a spike since the early 2020s. In fact, the COVID-19 pandemic further accelerated online (as well as offline) abuse.[16] Lockdowns increased children's online presence and travel restrictions encouraged travelling offenders to transition to online platforms,[17] while scammers further pivoted to livestreaming for profit.[18]

The joint international Operation Endeavour uncovered an organized crime group in the Philippines that livestreamed child sexual abuse content. *Photo: ICE*

Amid these rapid transformations, law enforcement and governance mechanisms have struggled to keep up and are still lagging on high-tech tools to pre-empt, prevent and respond to OCSEA. One such area is the classification of artificial intelligence (AI)-generated CSAM, laws to address this, and law enforcement capabilities to prevent such content proliferating and disrupt the cycle of harm.[19]

Factors that point to CSEA/OCSEA as a form of organized crime

The most organized forms of CSEA/OCSEA crimes in South East Asia are linked to the production and distribution of CSAM. Generating and circulating CSAM is not a complex endeavour, especially for self-generated material that minors create on their smartphones and share with their peers. The emergence of so-called 'nudification' apps that use AI to generate sexual images of children (and adults) further simplifies the job of anyone wishing to produce CSAM. This became apparent, to mention one case, when in 2024 police started investigating deep fake nude pictures of pupils of Singapore Sports School that had been generated and circulated by fellow students.[20]

Profiting from CSAM also does not necessarily require technical know-how of sophisticated payment systems. Payments linked to CSAM can be made with traditional bank transfers, gift cards and preloaded Visa cards, as is the case for sextortion, where victims (usually teenage boys) are not likely to use cryptocurrencies.[21]

When it comes to large-scale activities, however, there are factors that point to greater organization and sophistication of methods, as well as new motives. These suggest that although the networks involved may not be part of an established organized crime group in the same way as a drug cartel, members engage in transnational organized criminal activities, most likely for profit, and they should be countered accordingly.

Level of organization

A key factor differentiating gratification-motivated individual offenders from large-scale networks generating and circulating CSAM is the higher level of organization exhibited by the latter actors. A recent case provides a useful illustration.

Kidflix was one of the largest paedophile platforms in the world, with 1.8 million users and 91 000 CSAM videos. It was shut down in April 2025 as part of Operation Stream, led by Europol and involving 35 countries, including Australia and New Zealand.[22] The operation resulted in 79 arrests and almost 1 400 suspect identifications. Unlike traditional file-sharing, Kidflix's creator had built a rich community site and allowed streaming (not just downloading) of CSAM incorporating user contributions. Users would pay in cryptocurrency and earn tokens for uploading new abuse material.[23] Though Kidflix operated globally, it illustrates methods probably mirrored in smaller regional networks: gamified forums, token economies and vast libraries. It is also an example of platform innovation.

A further case speaks to the level of organization, financial sophistication and encryption of these criminal activities. In March 2025, a joint Thai–US operation led to the arrest of a Thai-based German national running two subscription CSAM websites. He operated them using WampServer software (which generates login credentials, shielding users' identities) with the Tor control panel.[24] The sites had about 5 000 videos and 10 000 paying members. Their owner, 'Steffen', required cryptocurrency payments (Bitcoin and Monero, with Monero offering near total anonymity) and relied on encrypted infrastructure to evade law enforcement.[25] Investigators traced the crypto transactions through layers of digital wallets to the point where funds were converted to cash (Thai baht). The sites also sold spyware through the dark web.[26]

Another characteristic pointing to offenders' high levels of organization is the development of formal structured hierarchies and defined roles and responsibilities by CSAM traders operating on the dark web. This applies to those motivated by the desire to harm children and those seeking financial gain.[27]

Changing motivations

In recent years, financial profit has become the driver of large-scale CSAM production and circulation, with criminals capitalizing on the vulnerabilities (or, for them, opportunities) of Asian countries in an era of high connectivity and widely accessible technology. Paedophiles and sexual predators have been joined in the OCSEA world by opportunistic criminals who derive no gratification from the digital material that has been produced but who instead see CSAM as just another lucrative business opportunity.

Supporting this point, INTERPOL's Operation Narsil (2021–2023) was one of the first to target individuals profiting from advertising revenues on CSAM websites. Twenty-seven countries, ranging from Argentina to Belarus and including Thailand and Singapore, were involved. In Thailand, the investigation led to the arrest of a local man for the possession and distribution of CSAM. A large CSAM catalogue and records of financial transactions related to the sale of the material were found at his home.[28] INTERPOL's 'worst of' list of domains distributing the most extreme CSAM was at the core of the investigation. This suggests that, in the name of financial profit, the offenders had no qualms about producing and circulating videos and images depicting extreme and severe abuse of young children (under 13).[29] This observation aligns with suggestions by child safety NGOs consulted for this brief that the more severe the abuse captured on camera, the higher the profits for criminal groups. This reality drives ever harsher and more pernicious levels of child abuse.

INTERPOL's Operation Narsil targeted individuals profiting from revenue generated by online child sexual abuse material. *Photo: INTERPOL*

While not yet widespread in South East Asia, globally CSAM is used as a gatekeeping device by criminals such as drug cartels or ideologically motivated groups. In order to be added to private groups – on Telegram, for instance – prospective members are required to download CSAM on their devices as proof of their commitment.[30] This is another example of CSEA/OCSEA-organized crime convergence, with motivations potentially unrelated to sexual gratification.

Domestic and transnational networks

It is worth considering the geographical nature of these networks, both domestic and transnational. Across South East Asia, both types are involved.

In many cases, local networks recruit and exploit children. In the Philippines and Cambodia, there have been reports of community-based rings (some linked to trafficking) that produce CSAM or coordinate livestreams. A UN Children's Fund (Unicef)/ECPAT International study in the Philippines highlighted how local abusers and facilitators – including children's caregivers – organized live abuse sessions at the request of paying foreigners.[31] In Thailand's hospitality and entertainment sectors, operators of bars or massage parlours (now more clandestine) have historically supplied children to sex offenders; after law enforcement pressure on brothels, networks shifted towards street-based and online solicitation.[32]

The transnational dimension is where greater organization can be observed. Demand often comes from abroad. Wealthy offenders in North America, Europe, Australia or elsewhere pay to order abuse or access large CSAM libraries. Investigations such as the one in the Philippines discussed earlier reveal sophisticated transnational chains with members in different countries all playing a role. In many cases, on-site facilitators remained in the victim's country while customers and financial flows crossed borders.[33] The extent of cross-border cooperation among offenders became clear during a five-week operation in which police from Singapore, Hong Kong, Japan, South Korea, Malaysia and Thailand arrested 435 individuals in February–March 2025. Many electronic devices and examples of AI-generated CSAM were also recovered.[34]

Common operating methods employed by criminals include grooming on social media, setting up hidden chat rooms on apps such as Telegram or WeChat and using encrypted cloud storage. Some offenders form closed groups on mainstream platforms to share links to hidden sites. Organized

rings also run offline recruitment through deceptive job or modelling offers, then coerce victims into online performances. Payment is often requested in cryptocurrency or funnelled through international banking networks (hawala, money mules) to cover tracks. Yet, the ever-growing sextortion trend does not require advanced payment systems.

Invite child abuse pyramid sites

Since 2022, the UK-based Internet Watch Foundation (IWF) has uncovered a disturbing new method of distributing CSAM online. Invite child abuse pyramid (ICAP) sites mimic viral marketing schemes, incentivizing individuals to share links to abusive content. Those who spread the links widely are 'rewarded' with access to increasingly severe material, creating a self-perpetuating cycle of abuse distribution. This model transforms users into unwitting participants in a criminal network, amplifying the websites' reach.

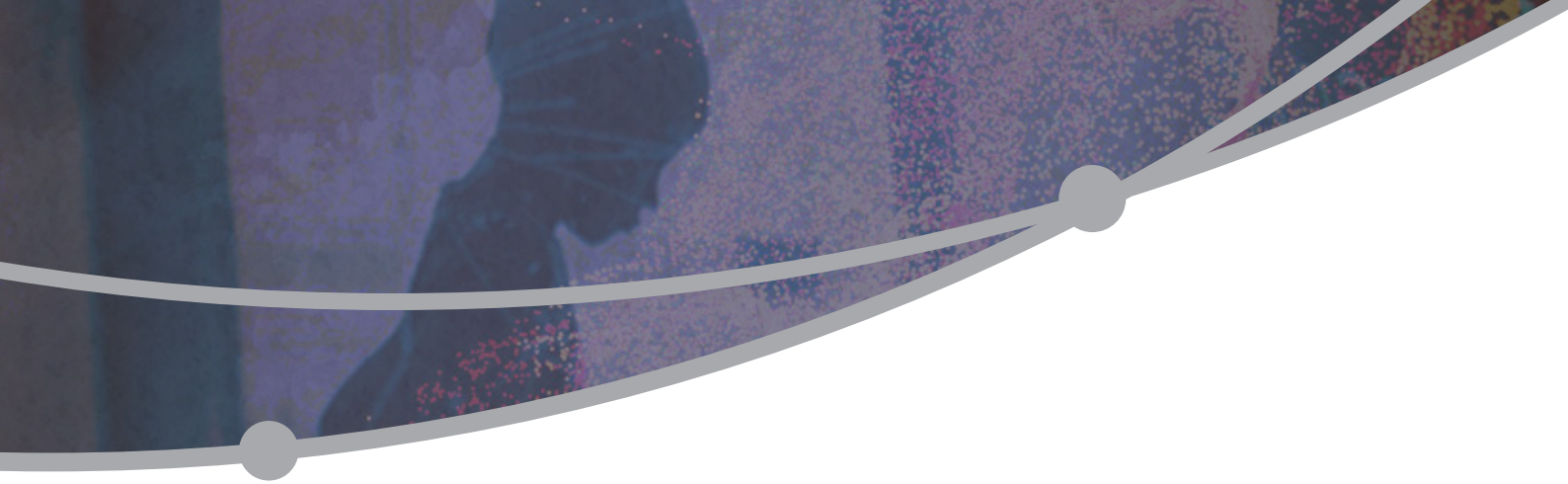
ICAP sites are commercial in nature and require payment for full access, but they rely heavily on non-commercial platforms – such as social media, blogs, chat rooms, forums and video channels – for recruitment and distribution. The links they share often appear in spaces where users expect to connect and communicate, not encounter illegal content. The links frequently vanish soon after being posted but their spread is rapid and difficult to control. A single link might appear many times on the same page and in various places, broadening its reach to unsuspecting users.

The content hosted on these sites is among the most extreme classified under UK law. It includes 'category A' material involving the sexual abuse and torture of babies and toddlers (as well as older children and animals). The sites often lure viewers with preview videos then urge them to register and share more links in return for access to further content, effectively commodifying the abuse of children in a pyramid-style incentive system.

Throughout 2023, the IWF observed a growing number of these links in general-purpose, non-commercial online spaces. This is particularly concerning because it exposes members of the public to deeply disturbing material. In fact, nearly all reports of ICAP sites received by the IWF came from people who stumbled across them.[35]

While there is no evidence of ICAP sites being linked to CSAM distribution in South East Asia, there have been reports of videos showing animal cruelty for entertainment involving the killing of primate species in the region.[36]

The IWF's broader data indicates that Hong Kong and Singapore are among the top 10 countries for the hosting of CSAM. In 2023, Hong Kong accounted for 9% of total reports, a four-percentage-point increase from the previous year, while Singapore accounted for 3%, a two-point increase.[37] ■



THE CURRENT APPROACH

To varying degrees, and in partnership with authorities from outside the region, governments and police forces in South East Asia have responded with new laws, specialized units and international cooperation. These activities are complemented by private sector and civil society efforts. However, there is a tendency to address CSEA/OCSEA through more traditional approaches that investigate cases in isolation while failing to acknowledge the organized crime nature of the offences. In parallel, the focus is often disproportionately on victims, and apart from newsworthy cases little is known about perpetrators and their networks.

Further underscoring the strong focus on victim identification, prosecutions in many CSEA cases – especially those involving physical contact – depend heavily on the victim's disclosure and subsequent testimony. This stems from the fact that physical or medical evidence is often minimal or absent.[38] Yet, the process of disclosure can be complex and influenced by factors including the child's age, relationship to the perpetrator and fear of not being believed. Alarmingly, Unicef's Disrupting Harm data shows that over 30% of OCSEA victims do not disclose their experience to anyone. Friends (40%) and siblings (24%) are the two most common choices for children who decide to disclose. Even in those cases, the abuse is often not further disclosed to adults, let alone a helpline or the police.[39]

With the rise of technology-facilitated abuse, digital evidence has become increasingly pivotal in prosecuting abuse cases. This includes photographs, videos, chat logs and metadata that can corroborate a victim's account or, in some instances, serve as standalone evidence of abuse. For example, in cases involving the production and distribution of CSAM, digital footprints can be instrumental in identifying perpetrators and substantiating charges without requiring the victim's in-court testimony. Moreover, the use of digital evidence aligns with evolving legal strategies aimed at reducing the trauma victims may experience during legal proceedings.

In addition to these obvious benefits, this investigative approach – if taken further and with the awareness of factors that point to OCSEA as an organized crime – makes it possible to gain detailed insights into the organized crime networks responsible for CSAM-related offences, identifying their structures and methods. In turn, pursuing and eventually prosecuting these organized criminals would help protect a larger number of potential future victims.

Notwithstanding this call for a more organized crime-oriented approach, it is important to acknowledge the wide range of responses that have been deployed in the region, not least as they offer lessons for other countries that may be vulnerable to the displacement of CSEA/OCSEA and/or may display more nascent markets for some of these offences.

Existing responses

Despite remaining legislative gaps, all South East Asian countries explicitly criminalize production, distribution and possession of CSAM, and many have updated laws to cover online grooming and livestreaming.[40] For example, Malaysia's 2017 Sexual Offences Against Children Act penalizes a wide range of CSAM activities;[41] the Philippines' Cybercrime Prevention Act (2012)[42] and Anti-Child Pornography Act (2009)[43] are used to charge online offenders; and Cambodia's laws against trafficking and pornography include child-specific provisions.[44] However, many gaps remain.

None of the Mekong countries and only two out of 10 Association of South East Asian Nations (ASEAN) countries require internet service providers to report suspected CSAM to law enforcement or any other agency. Statutes in Laos and Indonesia do not include a definition of CSAM (Vietnam's legislation doesn't either, but the definition of 'pornographic performance' includes actions involving individuals under 16). Furthermore, Vietnam and Myanmar do not criminalize simple possession of CSAM, regardless of the intent to distribute the material.[45]

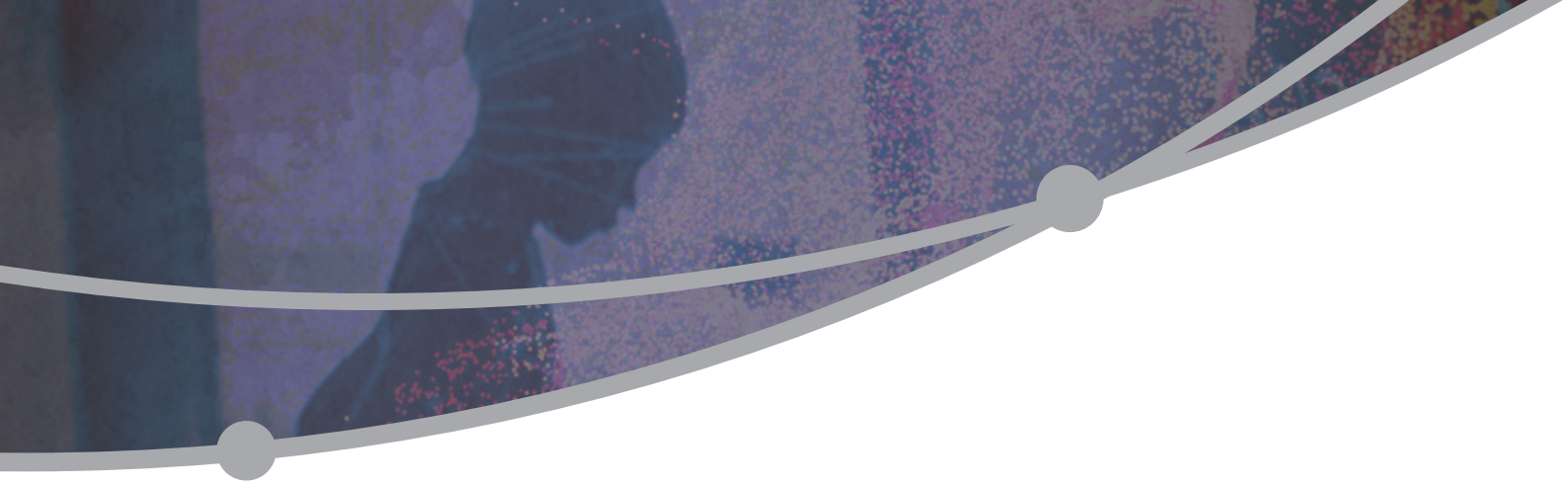
Many countries have dedicated cybercrime or child protection police units. In the Philippines, the Inter-Agency Council Against Child Pornography, the National Coordination Center against Online Sexual Abuse or Exploitation of Children and Child Sexual Abuse or Exploitation Materials under the Department of Justice and the Anti-Cybercrime Group of the national police focus on OCSEA. Thailand's Technology Crime Suppression Division leads OCSEA cases. International assistance has bolstered these units: for example, in July 2024, Philippine investigators received INTERPOL training and direct access to INTERPOL's global child exploitation image database.[46] Joint operations are common: law enforcement in the Philippines, Australia, UK and US have collaborated on dozens of cases. In one Philippine prosecution, evidence came from an Australian arrest of an offender who had been viewing Philippine-produced livestreams.[47] Information sharing with the US has also allowed Vietnamese authorities to stop several CSAM rings. [48] These examples underscore cross-border modus operandi and the use of foreign tip-offs to prosecute local facilitators.

Looking at regional and international frameworks, ASEAN has acknowledged OCSEA as a priority. The 2019 ASEAN declaration on the protection of children from all forms of online exploitation and abuse and its accompanying action plan urge member states to share information and harmonize laws.[49] The UN (UN Office on Drugs and Crime, Unicef) and INTERPOL regularly conduct workshops and investigations in the region.

Financial regulators such as the Asia/Pacific Group on Money Laundering have begun including OCSEA in anti-money laundering guidance, prompting banks in Asia to monitor suspicious cryptocurrency flows tied to child exploitation.[50] While regulatory frameworks for virtual assets are still developing, many Asia–Pacific governments encourage banks and exchanges to flag suspicious activity. Crypto analytics companies (as in Thailand's Steffen case) work with law enforcement to trace transactions. Several exchanges have compliance checks to prevent known offenders from cashing out. On the traditional finance side, anti-money laundering units are urged to consider child exploitation as a predicate offence. For example, after large CSEA stings, some countries issued advisories to banks to look for patterns (e.g. many small Bitcoin deposits followed by large withdrawals).[51] Payment networks (credit cards, digital wallets) generally prohibit use for any CSAM purchase and freeze accounts if flagged. However, some analysts note that more robust financial action is needed across the region: for instance, formal reporting protocols between tech companies, banks and police are still being established in many countries.

The exploitation of internet and social media platforms for CSEA/OCSEA means they face high expectations to counter these criminal activities, including the removal of child abuse content and cooperation with law enforcement. All major social media and chat services used in the region participate in global child safety initiatives. In the Philippines, the private-sector consortium SaferKidsPH was formed in 2019, funded by donors,[52] and companies such as Facebook, Google and local telecoms (PLDT/Smart, Globe) were consulted on policy and have supported awareness campaigns.[53] Tech firms also supply scanning tools: Google and Microsoft provide PhotoDNA hash filtering to detect known CSAM.[54] Internet service providers in many countries agree to block web addresses on government blacklists (e.g. IP blocklists of known CSAM servers). Regional partnerships (often supported by Unicef/ECPAT) run children's helplines and allow public reporting of CSAM websites to industry hotlines as part of the International Association of Internet Hotlines network.[55]

A host of domestic and international NGOs in the region are active in the child protection arena. Many are linked to the ECPAT network, which aims to eliminate the sexual exploitation of children.[56] An important actor is the International Centre for Missing & Exploited Children,[57] which works with governments to strengthen laws. These organizations also bridge public–private efforts: for example, they organize multi-stakeholder workshops where tech companies meet police and child protection agencies to design joint solutions. The US National Center for Missing & Exploited Children has long had a cyber tipline to receive information on suspected OCSEA.[58]



CONCLUSION AND RECOMMENDATIONS

In South East Asia, CSEA – especially in its online forms – has taken on many hallmarks of organized crime. Criminal groups have extended into cyberspace and new criminal enterprises have sprung up purely online. Cases from the Philippines, Thailand and elsewhere show that offenders use sophisticated dark web platforms, encryption, global communication networks and cryptocurrency payments to facilitate large-scale abuse for profit. These organized operations have global customers and often collaborate across borders.

Part of developing effective responses is accepting that over the past 20 years CSEA/OCSEA in South East Asia and many other parts of the world has transitioned from fragmented abusers into networked enterprises, driven by profit and enabled by digital technology. This is not to suggest that gratification is no longer a driver for many offenders but that a larger proportion of offenders are motivated by financial gain. Also, the two motivations can coexist within the same network. A greater understanding of this can be achieved by recalibrating the approach and putting greater emphasis on offender identification.

By exploring the links between CSEA/OCSEA and organized crime it would be possible to draw in more resources to combat these activities. For instance, law enforcement investigations could rely on anti-money laundering teams around the world who could feed into international investigations with the aim of cutting off criminals' revenue streams. This work, which effectively would combine financial crime and the existing victim-centred approach, requires further expansion of existing private–public partnerships.

Law enforcement interviewed for this brief suggested that an effective path to achieve this objective would be through industry champions that take the lead in encouraging cooperation between industry and police. Some financial service providers, such as Western Union, are well placed to do so. Furthermore, money remitters such as Wise that hold considerable data could assist by sharing information in an easily digestible format with law enforcement.

In this respect, as criminals adapt and import methods from other regions and markets, there is value in observing and possibly trialling new approaches that have been developed elsewhere in the world. One such example is Canada's 2020 launch of a public–private initiative, Project Shadow, co-led by Scotiabank and the Canadian Centre for Child Protection, with support from the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the country's financial intelligence unit.

Project Shadow supports the identification and reporting of money laundering associated with proceeds from OCSEA.[59] Central to this initiative are customized money laundering indicators developed by FINTRAC. These indicators are designed to monitor suspicious transactions related to child trafficking and sexual exploitation, including flagging suspicious activity associated with consumers, facilitators and producers of CSAM, as well as with luring activities. They serve as a critical reference for financial institutions and other reporting entities when submitting suspicious transaction reports.[60] Notably in the context of this brief, the Philippines and Thailand were the top two jurisdictions receiving money transfers from Canada linked to OCSAE.[61]

Building on this experience, in 2023, ECPAT International and its member Capital Humano y Social Alternativo piloted a transaction alert detection system in Scotiabank's Peru branches. As a result, Peru became the first country in Latin America to adopt an alert on child trafficking and sexual exploitation of children through its financial intelligence unit, UIF-Peru. A key takeaway from the pilot was the necessity of adapting money laundering indicators to the Peruvian context, rather than directly transplanting those developed in Canada. While challenges remain, particularly in scaling the approach and ensuring prosecutorial buy-in, the ability to trace transactions and pinpoint offenders offers a powerful tool for uncovering patterns. These insights can, in turn, support the identification of other offenders employing similar financial methods and transaction behaviours.[62]

An international operation led to the arrest of 58 people in the Philippines for their involvement in a global internet sextortion network. *© Ted Aljibe/AFP via Getty Images*

This 'follow the money' approach, when combined with a network-oriented investigative mindset, offers significant added value. By tracing payments for CSAM and livestreamed abuse, then analysing subsequent transactions linked to the recipients of funds, it becomes possible to uncover additional offenders within the broader criminal network. [63] This method not only aids in identifying individual perpetrators but also in mapping the structure and reach of exploitation networks. However, the success of this approach hinges on strong collaboration between the public and private sectors, underpinned by effective mechanisms for timely and secure data sharing.

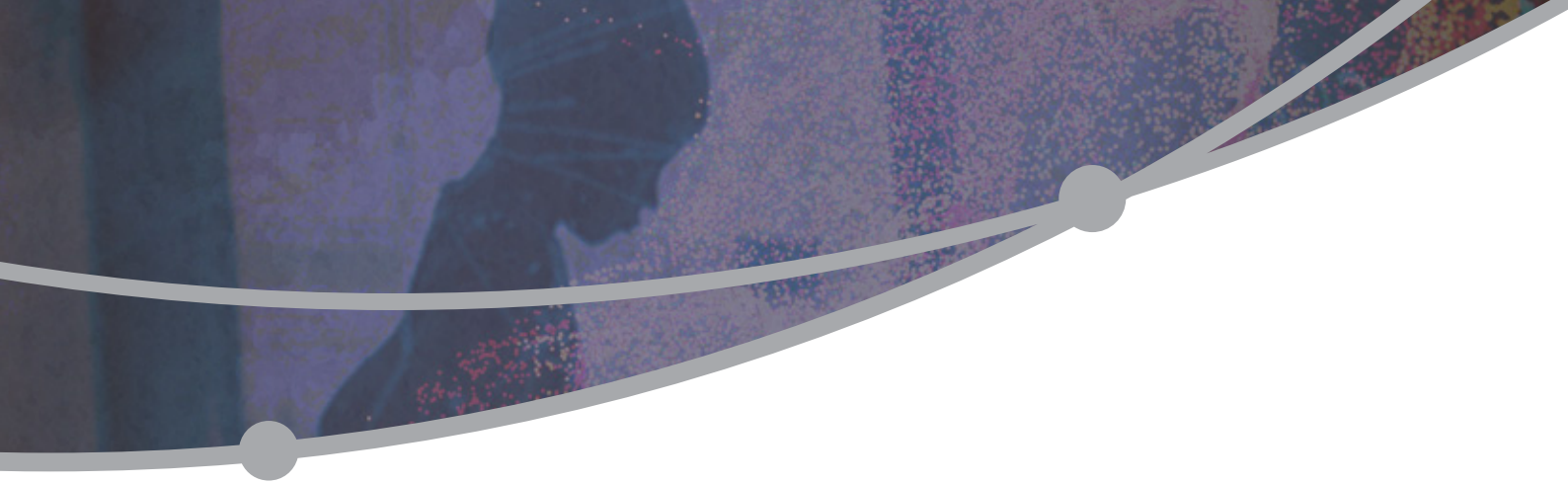
As well as learning from other regions, there is great value in learning from other crime areas. For instance, officers who have long worked on CSEA cases would benefit from exposure to colleagues with backgrounds in organized crime investigations. Specifically, knowledge transfer on how networks operate (online and offline) or money laundering techniques would help identify the factors that point to CSEA/OCSEA as an organized crime.

The shared learning would also help identify new areas of vulnerability. For instance, interviews for this brief indicated a convergence between OCSEA and ideologically driven groups such as the US-based 764 network promoting satanist and neo-Nazi beliefs. The network, which is at the centre of a major FBI investigation,[64] operates in many countries (including Australia),[65] engaging in sextortion and encouraging young people to self-harm. While there is no evidence of this occurring in South East Asia, it is an example of potential permutations of the OCSEA phenomenon.

South East Asian actors possess extensive experience of tackling CSEA/OCSEA cases. Neighbouring countries with more nascent experience, particularly the Pacific Island nations, would benefit from lessons from South East Asia. Data is limited but trends mirror Asia. Connectivity and smartphone access have risen sharply in recent years, exposing Pacific children to online risks. A 2024 regional scan noted that as the Pacific becomes more connected, it is at greater risk of commodified, organized online child abuse. Local child protection workers report rising exposure of children to pornography and cyberbullying.[66] There is little evidence of large-scale darknet syndicates based in Pacific nations, but transnational criminals may exploit lax enforcement, legislative loopholes and limited law enforcement capacity. In many respects these factors make the islands convenient alternatives to South East Asia, where there is a significant focus on combating CSEA/OCSEA.

From the perspective of social media platforms, adopting an organized crime approach would mean not stopping at closing an individual social media account that has engaged in grooming or posting CSAM. From a counter-organized crime perspective, this would entail considering and investigating (through public–private joint efforts) whether the account is connected to a wider network of offenders who may be involved in other illicit activities. Taking down the network, rather than a sole offender, would represent a better result and reduce risks for a larger number of children – which is the goal of everyone working on CSEA/OCSEA-related issues, regardless of their sector.

Governments and industry are increasingly collaborating: stronger laws, specialized police units and international databases are being deployed, while tech and financial firms develop new tools to detect and disrupt networks. The region's challenge is to keep pace with the evolving tactics of CSEA/OCSEA rings, ensuring that every technological advantage criminals have is met by equally advanced legal, technical and financial countermeasures.



NOTES

1 International Justice Mission (IJM), New study finds significant decrease in children in Cambodia's commercial sex industry, June 2015, https://www.ijm.org/news/new-study-finds-significant-decrease-in-children-in-cambodias-commercial-sex-industry.

2 IJM, Commercial sexual exploitation of children in Cambodia, 2013, https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/CSEC-Prevalence-Cambodia-FINAL-12-Sept-2013-1_2021-02-05-070150.pdf.

3 Child Exploitation and Online Protection Centre, Threat assessment of child sexual exploitation and abuse, June 2013, p 13, https://www.tiverton-coventry.org.uk/wp-content/uploads/2019/11/CEOP_TACSEA2013_240613-FINAL.pdf.

4 ECPAT International, Offenders on the move: Global study on sexual exploitation of children in travel and tourism, 2016, https://www.ecpat.org.uk/offenders-on-the-move-global-study-on-sexual-exploitation-of-children-in-travel-and-tourism-2016.

5 Sarah Napier, Coen Teunissen and Hayley Boxall, Live streaming of child sexual abuse: An analysis of offender chat logs, *Trends & Issues In Crime and Criminal Justice*, 639, October 2021, https://www.aic.gov.au/sites/default/files/2021-10/ti639_live_streaming_of_child_sexual_abuse.pdf.

6 *Bangkok Post*, Children rescued from alleged exploitation in porn videos, 14 May 2025, https://www.bangkokpost.com/thailand/general/3025540/children-rescued-from-alleged-exploitation-in-porn-videos.

7 Sextortion is a form of blackmail using sexual images to force a child into further abuse by providing more images or making payments.

8 NCA, National Crime Agency launches online campaign to tackle 'sextortion' among young teenage boys, 20 March 2025, https://www.nationalcrimeagency.gov.uk/news/national-crime-agency-launches-online-campaign-to-tackle-sextortion-among-young-teenage-boys.

9 Ibid.

10 INTERPOL, Asia: Sextortion ring dismantled by police, 5 September 2022, https://www.interpol.int/en/News-and-Events/News/2022/Asia-Sextortion-ring-dismantled-by-police; Sergiu Gatlan, Interpol dismantles sextortion ring, warns of increased attacks, Bleeping Computer, 5 September 2022, https://www.bleepingcomputer.com/news/security/interpol-dismantles-sextortion-ring-warns-of-increased-attacks/.

11 Child Exploitation and Online Protection Centre, Threat assessment of child sexual exploitation and abuse, June 2013, p 8, https://www.tiverton-coventry.org.uk/wp-content/uploads/2019/11/CEOP_TACSEA2013_240613-FINAL.pdf.

12 UNODC, Protecting the future: Improving the response to child sex offending in South East Asia, August 2014, https://www.unodc.org/roseap/uploads/archive/documents/Publications/2015/childhood/2014.08.28.Protecting_the_Future-Responding_to_CSO.pdf.

13 US Immigration and Customs Enforcement, 29 arrested in international case involving live online webcam child abuse, 15 January 2014, https://www.ice.gov/news/releases/29-arrested-international-case-involving-live-online-webcam-child-abuse, BBC, Philippines web abuse ring smashed in UK-led operation, 16 January 2014, https://www.bbc.co.uk/news/uk-25749326.

14 International Centre for Missing & Exploited Children (ICMEC), Cryptocurrency and the trade of online child sexual abuse material, February 2021, https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf.

15 Ibid; Chainalysis, Making cryptocurrency part of the solution to human trafficking, 21 April 2020, https://www.chainalysis.com/blog/cryptocurrency-human-trafficking-2020/.

16 Plan International and Save the Children, Because we matter: Addressing COVID-19 and violence against girls in Asia-Pacific, 2020, https://resourcecentre.savethechildren.net/pdf/pi_stc_becausewematterpolicybrief-final.pdf.

17 INTERPOL, Child sexual exploitation and abuse: Covid-19 impact, Threats and trends, September 2020, https://www.interpol.int/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf.

18 Samson Inocencio Jr, Unsafe in lockdown: Double threats to children during COVID-19 crisis, IJM, accessed 22 May 2025, https://www.ijm.org/vawc/blog/unsafe-in-lockdown-double-threats-to-children-during-covid-19-crisis.

19 Chew Han Ei, Sun Sun Lim and Carol Soon, Commentary: The AI-fuelled child exploitation crisis is global – so must be our response, Institute of Policy Studies, 15 April 2025, https://lkyspp.nus.edu.sg/ips/publications/details/commentary--the-ai-fuelled-child-exploitation-crisis-is-global---so-must-be-our-response.

20 Chew Han Ei, Deepfake nude apps are ruining lives and have no place in app stores, *Straits Times*, 20 January 2025, https://nus.edu.sg/newshub/news/2025/2025-01/2025-01-20/DEEPFAKE-st-20jan-pB3.pdf.

21 Australian Transaction Reports and Analysis Centre et al, Combating the sexual exploitation of children for financial gain: Financial crime guide, December 2022, https://www.austrac.gov.au/sites/default/files/2023-05/AUSTRAC_2022_FCG_Combating_the_sexual_exploitation_of_children_web_0.pdf.

22 Cornelia Riehle, Pedophile platform 'Kidflix' shut down, Eucrim, 15 May 2025, https://eucrim.eu/news/pedophile-platform-kidflix-shut-down/.

23 Europol, Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users, 2 April 2025, https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users.

24 James Morris and Son Nguyen, German dark web porn and spymaster arrested in Chonburi. Police and US Homeland Security operation, *Thai Examiner*, 11 March 2025, https://www.thaiexaminer.com/thai-news-foreigners/2025/03/11/german-dark-web-porn-and-spymaster-arrested-in-chonburi-police-and-us-homeland-security-operation/.

25 *The Nation*, German retiree arrested for selling child pornography on dark web, 11 March 2025, https://www.nationthailand.com/news/general/40047276.

26 Khaosod English, Thai-US sting operation nets dark web German operator, 11 March 2025, https://www.khaosodenglish.com/featured/2025/03/11/thai-us-sting-operation-nets-dark-web-german-operator/.

27 Madeleine van der Bruggen and Arjan Blokland, Profiling darkweb child sexual exploitation material forum members using longitudinal posting history data, *Social Science Computer Review*, 40 (4) 2021, pp 865–891, https://doi.org/10.1177/0894439321994894.

28 INTERPOL, Operation Narsil disrupts network of child abuse websites designed to generate profits from advertising, 3 August 2023, https://www.interpol.int/en/News-and-Events/News/2023/Operation-Narsil-disrupts-network-of-child-abuse-websites-designed-to-generate-profits-from-advertising.

29 Erika Di Benedetto, INTERPOL operation dismantles global child abuse networks, Organized Crime and Corruption Reporting Project, 7 August 2023, https://www.occrp.org/en/news/interpol-operation-dismantles-global-child-abuse-networks.

30 Interview with Tech Coalition, 17 April 2025.

31 ECPAT, INTERPOL and Unicef, Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse, Global Partnership to End Violence Against Children, 2022, https://www.unicef.org/philippines/media/7396/file/Disrupting%20Harm%20in%20the%20Philippines.pdf.

32 UNODC, Protecting the future: Improving the response to child sex offending in South East Asia, 2014, https://www.unodc.org/roseap/uploads/archive/documents/download/2014.08.28.Protecting_the_Future-Responding_to_CSO.pdf.

33 BBC, Philippines web abuse ring smashed in UK-led operation, 16 January 2014, https://www.bbc.co.uk/news/uk-25749326.

34 Firdaus Hamzah, Asian police forces nab more than 400 suspects in joint operation targeting online child abuse, Channel News Asia, 4 April 2025, https://www.channelnewsasia.com/singapore/online-child-abuse-porn-arrests-cross-border-operation-5044101.

35 IWF, Case study: Viral marketing sites, IWF Annual Report, 2023, https://www.iwf.org.uk/annual-report-2023/case-studies/viral-marketing-sites/.

36 Stefan Krempl, Child abuse: Internet hotline warns of dangerous dissemination scheme, Heise, 13 May 2025, https://www.heise.de/en/news/Child-abuse-Internet-hotline-warns-of-dangerous-dissemination-scheme-10381514.html.

37 IWF, Geographical hosting: URLs, IWF Annual Report, 2023, https://www.iwf.org.uk/annual-report-2023/trends-and-data/geographical-hosting-urls/.

38 Stephanie D Block and Linda M Williams, The prosecution of child sexual abuse: A partnership to improve outcomes, Office of Justice Programs, National Criminal Justice Reference Service, March 2019, https://www.ojp.gov/pdffiles1/nij/grants/252768.pdf.

39 ECPAT, INTERPOL and Unicef, Children's disclosures of online sexual exploitation and abuse, Disrupting Harm's Data Insight 2, 2023, https://safeonline.global/wp-content/uploads/2023/12/DH-data-insight-2_FinalB.pdf.

40 ICMEC, Child sexual abuse material: Model legislation & global review (10th edition), 2023, https://cdn.icmec.org/wp-content/uploads/2023/10/CSAM-Model-Legislation_10th-Ed-Oct-2023.pdf; ICMEC and Freshfields Bruckhaus Deringer, Protecting children against sexual offences in Association of South East Asian Nations (ASEAN) member states, 2 February 2023, https://cdn.icmec.org/wp-content/uploads/2023/02/February-2023-ICMEC-Report-Protecting-children-against-sexual-offences-in-ASEAN-Member-States.pdf.

41 Laws of Malaysia, Act 792, Sexual Offences Against Children Act 2017, https://www.foongchengleong.com/downloads/Sexual%20Offences%20Against%20Children%20Act%202017.pdf.
42 Republic of the Philippines, Republic Act No 10175, Cybercrime Prevention Act of 2012, https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/.
43 Republic of the Philippines, Republic Act No 9775, Anti-Child Pornography Act of 2009, https://www.officialgazette.gov.ph/2009/11/17/republic-act-no-9775-s-2009/.
44 Royal Kram NS/RKM/0208/005 on the Suppression of Human Trafficking and Sexual Exploitation, 20 December 2007, https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=93355&cs=1CgryPEdWUaps3yk4ZHJo0CuCSj9Y64-eTK5AzTRdyyr2EXKnrotvxv3n0S8lb4fhE061XNqbXF4efDx5_ryD6A.
45 ICMEC, Child sexual abuse material: Model legislation & global review (10th edition), 2023, https://cdn.icmec.org/wp-content/uploads/2023/10/CSAM-Model-Legislation_10th-Ed-Oct-2023.pdf.
46 Council of Europe, GLACY-e: Philippines becomes the 70th country to connect to INTERPOL's international child sexual exploitation database, 8 July 2024, https://www.coe.int/en/web/cybercrime/-/glacy-e-philippines-becomes-the-70th-country-to-connect-to-interpol-s-international-child-sexual-exploitation-database.
47 IJM, Philippines: Woman receives life sentence for online sexual exploitation of children, August 2024, https://www.ijm.org/vawc/blog/philippines-woman-receives-life-sentence-for-online-sexual-exploitation-of-children.
48 Asia News Network, Growing public alarm over child pornography in Vietnam, *Phnom Penh Post*, 14 January 2020, https://www.phnompenhpost.com/international/growing-public-alarm-over-child-pornography-vietnam.
49 ASEAN, Declaration on the protection of children from all forms of online exploitation and abuse in ASEAN, November 2019, https://asean.org/wp-content/uploads/2019/11/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf.
50 Financial Action Task Force/Organisation for Economic Cooperation and Development, Detecting, disrupting and investigating online child sexual exploitation: Using financial intelligence to protect children from harm, 2025, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Online%20Child%20Sexual%20Exploitation%20Report.pdf.coredownload.inline.pdf.
51 Ergul Celiksoy et al, Payment methods and investigation of financial transactions in online sexual exploitation of children cases, University of Nottingham Rights Lab, 2023, https://www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/payment-methods-and-investigation-of-financial-transactions-in-online-sexual-exploitation-of-children-cases.pdf.
52 SaferKidsPH home page, accessed 20 May 2025, https://www.saferkidsph.org/.
53 Unicef, Ending online child sexual exploitation and abuse, December 2021, www.unicef.org/media/113731/file/Ending-Online-Sexual-Exploitation-and-Abuse.pdf.
54 Tech Coalition, The Tech Coalition empowers industry to combat online child sexual abuse with expanded PhotoDNA licensing, 27 January 2025, https://www.technologycoalition.org/newsroom/the-tech-coalition-empowers-industry-to-combat-online-child-sexual-abuse-with-expanded-photodna-licensing.
55 International Association of Internet Hotlines home page, accessed 20 May 2025, https://www.inhope.org/EN.
56 ECPAT, Membership with ECPAT International, accessed 20 May 2025, https://ecpat.org/membership-with-ecpat/.
57 ICMEC home page, accessed 20 May 2025, https://www.icmec.org/.
58 CyberTipline, National Center for Missing & Exploited Children, accessed 20 May 2025, https://www.missingkids.org/gethelpnow/cybertipline.
59 Project Shadow, WeProtect Global Alliance, accessed 22 May 2025, https://www.weprotect.org/resources/case-study/project-shadow/.
60 FINTRAC, Laundering of proceeds from online child sexual exploitation, Operational alert, December 2020, https://fintrac-canafe.canada.ca/intel/operation/exploitation-eng.pdf.
61 Ibid.
62 Interview with Guillaume Landry, executive director, ECPAT International, 22 May 2025.
63 World Childhood Foundation, Follow the money: Payments for livestreaming of child sexual abuse in the Philippines, 2025, https://childhood.se/wp-content/uploads/2025/03/child004-rapport-follow-the-money-digital-110325-2.pdf.
64 *The Guardian*, FBI opens inquiry into 764, online group that sexually exploits and encourages minors to self-harm, 11 May 2025, https://www.theguardian.com/us-news/2025/may/11/fbi-investigation-764-online-group.
65 Joel Erickson, Aussie teen targeted by horrific online 'paedophile cult', Kidspot, 4 March 2024, https://www.kidspot.com.au/news/aussie-teen-targeted-by-horrific-online-paedophile-cult/news-story/42be4ef4061dd9fb948cf75e4e84f43d.
66 Australian National Office for Child Safety, Pacific environmental scan report 2024, 2024, https://www.childsafety.gov.au/resources/pacific-environmental-scan-report-2024.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net