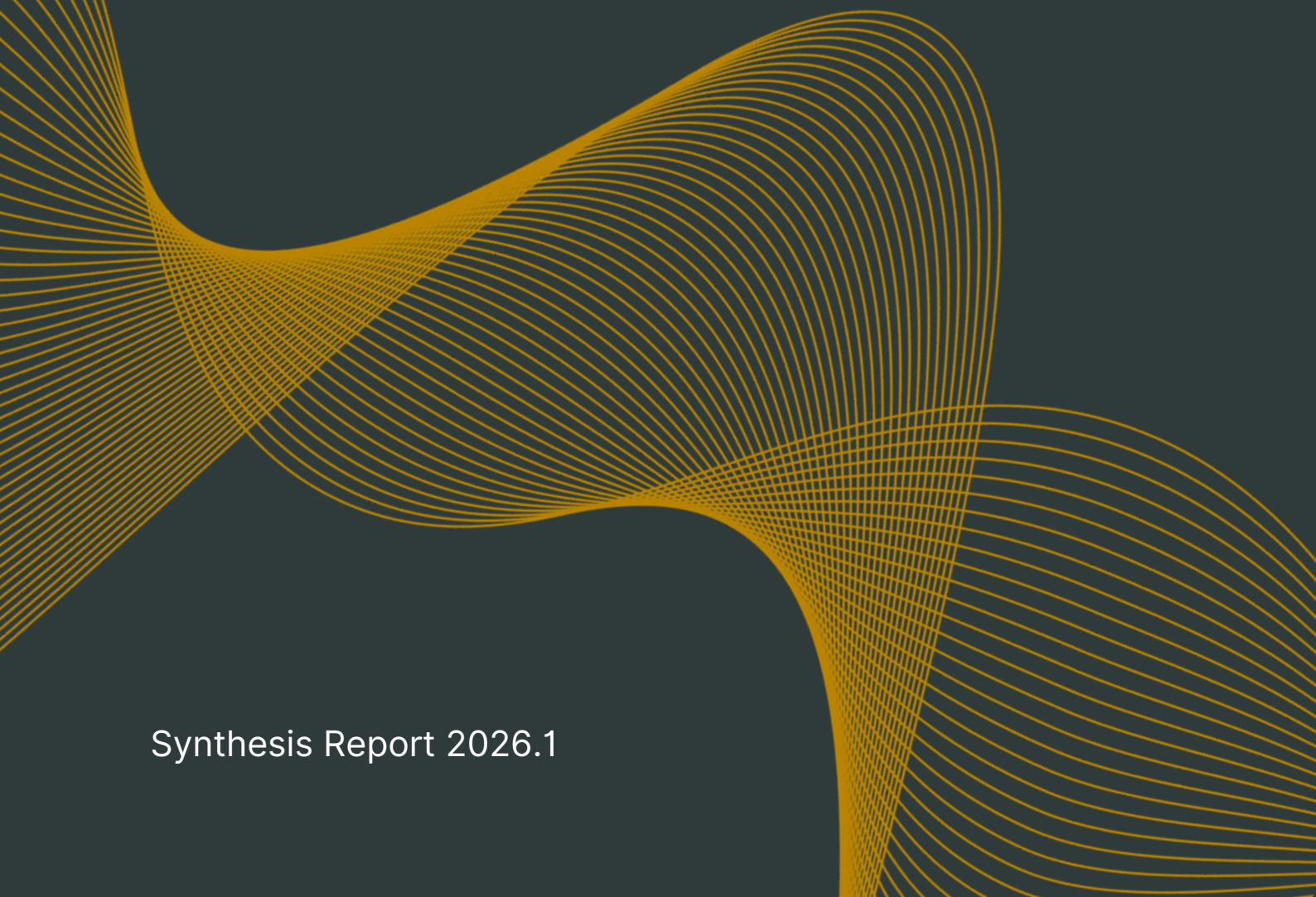
IPIE
International Panel on the Information Environment

Detecting, Deterring, Investigating, and Prosecuting Technology-Facilitated Child Sexual Exploitation and Sexual Abuse

A Systematic Review



Synthesis Report 2026.1

IPIE
International Panel on the Information Environment

Detecting, Deterring, Investigating, and Prosecuting Technology-Facilitated Child Sexual Exploitation and Sexual Abuse

A Systematic Review

Synthesis Report 2026.1

How to cite:
International Panel on the Information Environment [K. Pothong, S. Kaynak, D. Fry, S. Ghai, S. Livingstone, A. Phippen, C. R. Soriano, L. M. Given, P.N. Howard, S. Valenzuela (eds.)], *Detecting, Deterring, Investigating, and Prosecuting Technology-Facilitated Child Sexual Exploitation and Sexual Abuse: A Systematic Review*. Zurich, Switzerland: IPIE, 2026. Synthesis Report, SR2026.1, doi: 10.61452/UZUS7376.

SYNOPSIS

Technology-facilitated child sexual exploitation and sexual abuse (TF-CSEA) is an escalating global crisis. Digital platforms, social media, livestreaming services, and online payment systems enable sexual abuse of children at unprecedented scale and speed.

Reports of online grooming, financial sextortion, livestreamed abuse, and AI-generated child sexual abuse material continue to rise across regions. Existing interventions struggle to keep pace with technological change, allowing offenders to operate across borders with limited risk of detection or disruption.

This assessment synthesizes the evidence on detecting, deterring, investigating, and prosecuting TF-CSEA from over 100 high-quality studies published over the past decade. Following standard PRISMA and synthesis protocols, the review assesses technical, legal, policing, behavioral, and educational interventions and provides four key findings:

1. **Most interventions focus on detecting abuse after it occurs**. Far fewer disrupt the systems that enable TF-CSEA, including payment mechanisms, advertising and recruitment pathways, and judicial capacity.
2. **Technical tools reduce harm at scale but depend on legal authority, secure data access, safeguards, and effective enforcement**. Without these, automated and AI-assisted tools have limited impact.
3. **Behavioral and educational interventions reduce risk and increase awareness, but cannot replace platform accountability**. Evidence of sustained behavior change remains limited without regulatory and enforcement support.
4. **Financial systems are the most underused leverage point against TF-CSEA**. Few interventions disrupt payments financing abuse, focusing instead on tracing transactions after harm occurs.

This synthesis provides the most comprehensive assessment of TF-CSEA interventions to date. Evidence gaps remain, especially on payment disruption and long-term outcomes. Nonetheless, the findings establish clear consensus on the need for coordinated legal authority, scalable technical systems, sustained enforcement, and action to interrupt financial flows.

CONTENTS

SECTION 1. INTRODUCTION

Various international legal instruments outlaw child sexual exploitation and sexual abuse irrespective of where the offences take place, making states the primary duty-bearers to protect children against these crimes. In this document, a "child" refers to anyone under the age of 18, according to the United Nations Convention on the Rights of the Child (UNCRC) (1989) [1]. Examples of these international legal instruments include Article 34 of the UNCRC [1]; the International Labour Organization's (ILO) Worst Forms of Child Labour Convention, 1999 (Convention No. 182, Article 3(b)) [2]; the Lanzarote Convention [3]; and the UN Convention against Cybercrime, 2024 (Article 14) [4]. Increasingly, sexual offences against children are facilitated and exacerbated by advances in digital technologies, as is demonstrated by the growing diversity and volume of sexual offending against children being reported [6].

Technology-facilitated child sexual exploitation and sexual abuse (TF-CSEA) encompasses sexual offences against children "made possible with the help of technology" [6, p.82]. While these offences may be committed in both digital and physical environments, digital technologies directly enable sexual offences committed against children while they are online. Examples include "enticing/manipulating/threatening [children] to get them to perform sexual acts in front of a webcam"; child online grooming for sexual purposes and distribution; disseminating or "knowingly obtaining" access to child sexual exploitation and child sexual abuse materials (CSAM) online; and "live streaming of child sexual abuse" [6 pp. 84–85].

Digital technologies also facilitate child sexual offending in person. Examples include enabling perpetrators to identify and connect with child victims; coordinating sexual offending against the child; and capturing the sexual

encounters to archive and distribute these records [6]. This systematic review lays out the complexity of the TF-CSEA ecosystem, and maps out efforts to combat these crimes to inform future policies and interventions.

The Complex TF-CSEA Landscape and Offending Chain

As background to this systematic review, we first mapped TF-CSEA occurrences using variables and data pertaining to the use of technology by children, perpetrators, and others [7]. The aims of that initial research were to understand where the risks lie and which data sources might provide evidence of these risks. Based on this, the liability of various actors, including technology companies, in contributing to such risks could be better understood and attributed.

The variables and data pertaining to technology use by perpetrators and children are essential for the research required to inform policy, legislative, and regulatory decisions and interventions against TF-CSEA.

Using the "4Cs" (content, contact, conduct, and contract) of child online risks (see Endnote) to categorize technology uses for TF-CSEA [8], this initial research identified three key interplaying components that make TF-CSEA complex. The components are:

1. Technologies' evolving technical capabilities.
2. Users' evolving technical skills and use of new technologies.
3. The evolving contexts that shape and are reshaped by technology use.

This interplay suggests that technological advances afford new opportunities to perpetrators, children, and others that could expose children to technology-facilitated harms. Examples include livestreaming of child sexual abuse, artificial intelligence (AI)-generated CSAM, easier potential victim identification through algorithmic recommendation systems, and alternative ways to monetize, order, and pay for CSAM [7].

Figure 1. TF-CSEA Offending Chain.

Source: IPIE.

The diverse range of technology uses identified in this initial research indicates an expansive offending chain (see Figure 1). These activities can be grouped into four interwoven categories [7], and TF-CSEA can include one or a combination of the activities listed in Figure 1.

The complexity of the TF-CSEA landscape and offending chain, as well as the increased attention paid to this issue by civil society and governments, inevitably leads to a quest for potential interventions. Although there have been many attempts to address TF-CSEA in various jurisdictions [9], [10], [11], [12], [13], given the evolving nature of technologies, uses, and contexts, no single solution can mitigate the risks. Furthermore, although various solutions have been proposed or implemented, ranging from broad regulations to educational programs, there is no systematic repository of these approaches. In short, it would be worthwhile to map out the interventions that have been developed and implemented, along with any available assessments of their effectiveness and reports on their outcomes.

In response, this systematic review aimed to identify interventions addressing TF-CSEA along the offending chain. The resulting review provides a nuanced picture

of where scientific research has thus far focused, existing gaps in the research, effective intervention practices, and where further attention is required.

TF-CSEA Intervention Ecosystem

The ecosystem and pathways for interventions in TF-CSEA are also complex, involving diverse measures and multistakeholder collaboration across organizations and jurisdictions. On the policy front, UNICEF [13] and the WeProtect Global Alliance, for example, are driving the policy agenda for child online protection [14]. UNICEF is playing an important role by engaging the private sector, starting with the telecom sector, and more recently, the gaming industry [15].

Examples of such interventions include supporting child online protection by developing tools and guidance for companies to respect children's rights, in this case, to protection from sexual abuse (UNCRC, Article 34) [13], [16], [17], [18], [19]. The WeProtect Global Alliance introduced the Model National Response (MNR) to coordinate, monitor, and measure progress by organizations and national governments that commit to combating TF-CSEA [14]. MNR serves as an essential blueprint and operational framework for interventions in TF-CSEA at national levels, spanning policy and governance, criminal justice, victim support, societal awareness, industry engagement, and communication strategies [14].

At the legal and regulatory level, countries and regions worldwide have enacted laws and regulations to address TF-CSEA. For example, the Philippines introduced the Anti-Child Pornography Act in 2009 to criminalize the "luring" and "grooming" of a child to engage in sexual activities [20]. The Act, which was updated in 2022 [21], also imposes a reporting duty on internet service providers (ISPs), content hosts, credit card companies, banks, and other businesses with direct knowledge of CSAM to notify the Philippine National Police or the National Bureau of Investigation.

Similarly, the South African Cybercrimes Act criminalizes child grooming for in-person as well as online sexual exploitation and abuse [22]. At the European Union (EU) regional level, Directive 2011/93/EU [23] lays down minimum rules for member states concerning the definition of criminal offences and sanctions against child sexual exploitation and abuse. This includes the recruitment of a child for pornographic purposes and the solicitation of a child for sexual acts.

Law enforcement agencies such as INTERPOL and Europol play important roles in victim and criminal identification across borders, integrating technologies to support intelligence gathering [24, 25]. Non-profit organizations are also contributing to global efforts to combat TF-CSEA in different ways. The USA's National Center for Missing & Exploited Children (NCMEC) operates CyberTipline, a national centralized reporting system for public and electronic service providers to report suspected child sexual exploitation and abuse [26]. The UK's Internet Watch Foundation (IWF) operates a hotline that provides the public with a safe and anonymous channel through which they can report suspected online images and videos featuring child sexual abuse. The IWF has also developed cutting-edge technical tools to aid the identification and removal of online child sexual abuse images and videos [27], [28].

Some nongovernmental organizations (NGOs) also incorporate research components in their child protection work. For example, one of the longest standing NGOs, End Child Prostitution in Asian Tourism (ECPAT), was established in Thailand in 1990 [29]. ECPAT internationalized in 1997 and changed its name to End Child Prostitution, Child Pornography and Trafficking [30]. The organization now coordinates research and actions to combat child sexual exploitation and abuse in over 155 countries [30]. It has convened a multistakeholder working group to develop its Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse [6]. It also contributes to the research and

publication of the Disrupting Harm series [31], which documents TF-CSEA in 12 different countries.

Another international NGO, Safe Online, funds projects, programs, and research to develop evidence, solutions, and technologies to address TF-CSEA and other digital harms [32]. Similarly, the Childlight Global Child Safety Institute, hosted by the University of Edinburgh, produces data-driven, publicly accessible research reports. It offers a global index that provides a systematic estimate of the scale of TF-CSEA and reports on different dimensions of this problem.

Further research initiatives on a global scale would be extremely valuable. This systematic review builds on the work of these organizations to document the prevalence of TF-CSEA, focusing on existing and emerging interventions to address these harms.

SECTION 2. RESEARCH OBJECTIVES AND QUESTIONS

Despite national and international efforts to combat TF-CSEA, reports of such crimes are still on the rise. According to CyberTipline report, online enticement rose from 292,951 reports in 2024 to 518,720 in 2025, while financial sextortion cases rose from 13,842 in 2024 to 23,593 in 2025 [5]. An even steeper increase is TF-CSEA involving the use of generative artificial intelligence (GenAI), which rose from 6,835 cases in 2024 to 440,419 in 2025 [5].

TF-CSEA offending involves a complex ecosystem and multiple pathways in the offending chain. This makes it difficult to track and discern what measures are available to address offences, the state of the art of interventions, and how well they work. This complexity also makes it difficult to spot any gaps in efforts to detect, deter, investigate, and prosecute these crimes. TF-CSEA continues to evolve as new features are introduced by technologies like AI. It is therefore important to reflect on whether current interventions are adequate to curb existing and emerging offences, and to identify any gaps that need to be filled.

To this end, we conducted a systematic review of interventions that aim to deter and minimize the risks of TF-CSEA, asking:

> What interventions have been developed and deployed to combat TF-CSEA?
>
> Have any interventions been evaluated? And if so, how well does the intervention work?

This systematic review deliberately focuses on interventions aimed at detecting, deterring, investigating, and prosecuting TF-CSEA offending. We treat criminal and financial penalties as forms of deterrence. Please note that interventions aimed at rescuing victims and supporting survivors are beyond the scope of this review.

SECTION 3. METHODS

Systematic reviews are valuable for their rigorous approach to evidence synthesis in order to inform practices or policies [33]. They systematically set out the research questions and methods to rigorously assess the research literature on a topic of interest [33], [34], [35].

In the domain of TF-CSEA, systematic reviews of interventions are rare. When these are conducted, they tend to focus on a specific type of intervention, for example, a technical tool to prevent online child sexual abuse [36]. Most systematic reviews of TF-CSEA revolve around the occurrence of harms [37] and their effects [38]. This IPIE review aims to provide an overview of the breadth of the interventions and a narrative description of their reported outcomes.

The value of this systematic review lies in its in-depth examination of the peer-reviewed literature, with additional insights from the gray literature, including organizations' reports. The two types of literature complement one another. The peer-reviewed academic publications tended to focus on single or interconnected interventions, while the gray literature offered accounts of multiple interventions applied within national or regional contexts. This review documents the most studied types of TF-CSEA interventions and gaps, key stakeholders, and the implications of both on the TF-CSEA offending chain.

The resulting analysis underscores the potential of selected interventions in the detection, deterrence, investigation, and prosecution of these crimes and how they might be adapted and applied in other jurisdictions. The analysis also highlights the additional efforts required to protect children from this form of exploitation and abuse, as well as to secure justice for victims.

Sampling Procedures

This systematic review follows the PRISMA protocol [39] for study selection and review. The sampling procedure for study selection began with the development of the search strategy and identification of the databases. We drew on A Guidebook of Terminology to Use for Literature, Systematic and Scoping Reviews in the Research Area of Child Sexual Exploitation and Abuse [40], and other reports on TF-CSEA interventions, to identify relevant keywords to develop our search strategy.

Given the objective of this systematic review, our search strategy combined two key components: interventions (e.g., prevention, Domain Name System [DNS] blocking, hashing) and types of offending (e.g., CSAM, child sextortion, livestreaming of child sexual exploitation). Applying Boolean logic, our most successful search strategy contained the full list of keywords from the intervention component, and only the broad description of types of offending below:

(Intervention OR Prevention OR Countermeasure* OR “Technical solutions” OR Education OR Literacy OR “Industry mandatory reporting” OR “Behav* psychology intervention” OR Policing OR Detection OR Deter* OR “DNS blocking” OR PhotoDNA OR “Photo DNA” OR Hash* OR Filter*) AND (“Technology facilitated” OR Online OR Technology assisted) AND (“Child sexual exploitation and sexual abuse” OR “Child sexual exploitation” OR “Child sexual abuse”).

Our successful search strategy refers to the one that returned the most relevant results across all three databases:

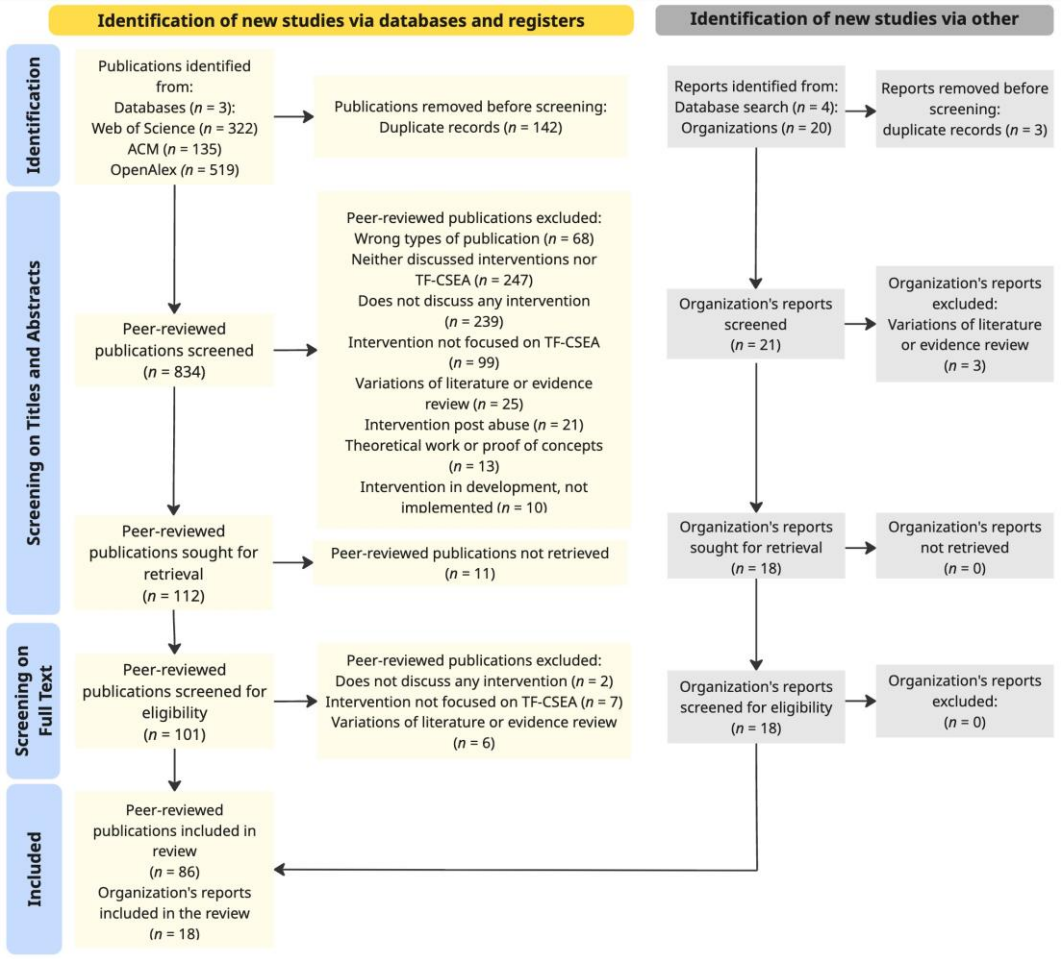
- Web of Science: www-webofscience-com.lse.idm.oclc.org/wos/woscc/smart-search
- Association for Computing Machinery (ACM) Digital Library: https://dl.acm.org

- OpenAlex: https://openalex.org

We chose a search range of over 10 years (January 2015 to July 2025) for currency of interventions, given the evolving nature of technologies. The databases were chosen because, together, they enable the identification of multidisciplinary research on a diverse range of interventions in TF-CSEA. Web of Science includes indexes for peer-reviewed publications across various social science fields, providing relevant research evidence on people's experiences with technologies. ACM indexes peer-reviewed journal publications and conference papers in computer science and human–computer interaction (HCI), offering rich grounds for research on technical interventions into TF-CSEA. OpenAlex is a multidisciplinary database that indexes both academic and gray literature and provides a useful source for some organizations' reports. By choosing these databases, our search did not include book chapters or other types of academic publications.

We also searched the websites of key organizations combating TF-CSEA to ensure the comprehensiveness of our search for gray literature. These included UNICEF, Safe Online, ECPAT, International Justice Mission, and the WeProtect Global Alliance. The rationale for the specific focus on these organizations' websites lies in their active roles in combating TF-CSEA. We ran our searches on 17th July 2025. The results of these searches are summarized in the PRISMA diagram (Figure 2).

Figure 2. PRISMA Flow Diagram of the Systematic Review Process.



Source: IPIE calculations based on data collected
Note: This flow of peer-reviewed publication and organization report selection is based on a standard design suggested by the PRISMA recommendation [39].

Collectively, 1,003 peer-reviewed academic publications and organization reports were uploaded to Rayyan, an AI-powered online platform for managing and conducting systematic literature reviews. A total of 145 duplicates were removed using the platform's duplicate detection function under author oversight. This left a total of 834 academic publications and 21 organizations' reports for title and abstract screening.

Of these 855 publications and reports, 751 were excluded because they did not meet the inclusion criteria and could not be retrieved. The reasons for their exclusions are summarized in Figure 2. To be included for data extraction and analysis, the study design required that publications and reports meet the following criteria:

1. Publication dates: Published between January 2015 and July 2025.
2. Object of analysis:
    a. Interventions aimed at protecting children, anyone under 18 years of age.
    b. Any form of intervention aimed at detecting, deterring, investigating, and prosecuting TF-CSEA.
3. Features of publications and reports:
    a. Primary dataset: Peer-reviewed academic publications, reporting empirical research
    b. Secondary dataset: Gray literature (i.e., organizations' reports) to provide context around interventions
    c. All publications and reports must discuss TF-CSEA-focused interventions
    d. Intervention is fully developed, ready to deploy, or in deployment, at any scale of geographic community and/or digital space.

We independently screened the final set of 104 publications (86 academic and 18 organizational reports) and compared their inclusion decisions to ensure reliability. The result of this reliability test on screening criteria is reported in Section 3.

Analytical Procedures

In sum, 86 peer-reviewed academic publications and 18 organizations' reports met the inclusion criteria and were investigated for the review. We drafted the

initial coding frame for data extraction, based on the research questions, to consistently capture details for each included publication and report. Incorporating feedback from members of the International Panel on the Information Environment (IPIE) Scientific Panel, the variables were finalized (see Table 1 and the full list of coded variables in Appendix A).

Twelve items from the 86 peer-reviewed publications were randomly selected, using Rayyan. The inter-coder reliability between two coders reached 100% agreement on 54 variables, 91.7% on 14 variables, 83.3% on 8 variables, and 75% on 2 variables. Minor disagreements arose from coders' varying clarity regarding the scope and definitions of the variables, as well as how each coder interpreted the definitions and codes. Neither coder found conflicts in the coding structure or the variables.

Examples of variables that require clarification include "scale of the intervention implementation" and "intervention operation". Examples of code meanings that require clarification include "online (at a system level)" and "automated web crawler". With an aligned understanding of the definitions following additional discussions, we updated the definitions of these terms in the codebook (see Appendix A).

Table 1. Coding structure.

Structure of the coding frame	Coding criteria
Publication or report details	Publication or report title, publication year, author(s), publication type (academic or gray literature)
TF-CSEA intervention	Type and number of interventions reported, intervention development and implementation, funding, scale of implementation, subjects and contexts for the intervention, and objectives
TF-CSEA intervention evaluation	Whether the intervention has been evaluated, by whom, methods, findings, limitations, and results

These publications were coded for the systematic review. We then used the organizations' reports to provide context on the interventions. We registered our methods and protocol for this systematic review on the Open Science Framework (OSF). We have structured our reporting of the findings according to our research questions.

SECTION 4. FINDINGS

Both the contextual information gathered from the organizations' reports and the analysis of peer-reviewed academic publications show that TF-CSEA interventions involve diverse measures and stakeholders. Many interventions were multidimensional: they encompassed more than one type of intervention, served one or more objectives, and addressed various aspects of the TF-CSEA offending chain and intervention pathways. This reflects the complexity of the crimes and their evolving nature, due in part to the diverse affordances of emerging technologies. Therefore, interventions to detect, deter, investigate, and prosecute these crimes are necessarily multifaceted, involving diverse measures and stakeholders. There is no one-size-fits-all solution, nor a quick fix to combat TF-CSEA. However, in the primary dataset, we identified five types of interventions across diverse geographical, jurisdictional, and cultural boundaries that were the most commonly reported. These include technological tools and protocols, policing and investigation, behavioral interventions, legal and regulatory interventions, and education, literacy, or awareness-raising campaigns.

What Interventions Have Been Developed and Deployed to Combat TF-CSEA?

Our first research question aimed to identify the intervention categories, their domains of operation, their objectives, and the segments of the offending chain they address. The review also identified the stakeholders involved, including the developers, implementers, funders, and evaluators of the intervention.

TF-CSEA Intervention Categories

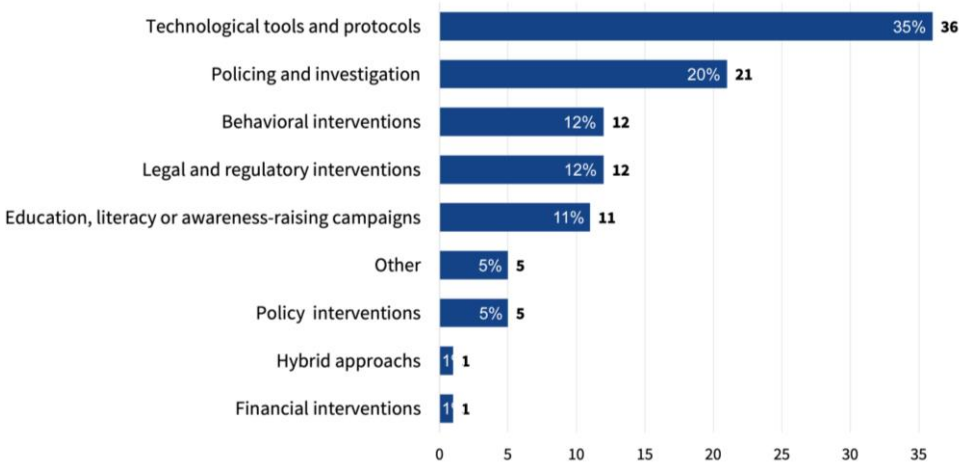
The interventions were categorized by their primary mechanisms of change. For example, an activity designed to increase awareness, or educating particular populations such as children, parents, or professionals working with children, would be coded as education, literacy, or awareness-raising campaigns. Similarly,

interventions involving law enforcement efforts to police, investigate, arrest, and prosecute those involved in TF-CSEA would be coded under policing and investigation. Technological tools and protocols focused on the use of digital applications, products, or services to detect, deter, and curb TF-CSEA. Examples included automated content (images and text-based conversations), transaction monitoring tools, and hashing and voice analysis. The full list of categories is given in Appendix A. If an intervention involved interlinked processes, such as the technological tools and protocols used in a policing investigation, we coded it under all applicable intervention types.

As depicted in Figure 3, our analysis of the peer-reviewed academic publications identified at least nine types of TF-CSEA interventions. Technological tools and protocols (n = 36) were the most frequently studied type of intervention across all the peer-reviewed academic publications, followed by policing and investigation (n = 21).

These two categories are often interrelated, reflecting the growing trend of integrating technologies into the policing and investigation of TF-CSEA. For example, Europol developed and deployed a crowdsourcing platform to collect public tips on the locations of victims and perpetrators [24]. Another example is a digital forensic solution for identifying CSAM uploaders and downloaders. This has been used in real-life policing and investigation, resulting in convictions of CSAM offenders in the USA [41]. Stathis and Marinakis's [42] discussion of the computer voice stress analyzer (CVSA) used by the USA's Internet Crimes Against Children (ICAC) is yet another example. This tool helps to obtain critical online child sexual offence information, resulting in the identification of previously undiscovered live victims.

Figure 3. Frequency of Intervention Types.



Source: Data based on manually coded articles collected on 17th July 2025 from databases.
Note: *n* = 104 (100%) intervention categories. The units of analysis here are occurrences of coded variables, not the number of publications coded. The Other category includes parent-child discussion, CSEA, and the sentencing process. See Appendix B for the coding frame and definitions of coded variables.

The next most common categories, both with 12 items, were behavioral interventions and legal and regulatory interventions. Most behavioral interventions were aimed at potential or ex-offenders [43], [44], [45], [46], [47], [48], [49]. Most used technological tools and protocols to deliver interventions. Many involved automated warning messages triggered by attempts to access illegal or "barely legal" sexual pornographic content [44], [45], [47], [48]. Technological tools and protocols can also display therapeutic and deterrent messages to internet users when they attempt to access "barely legal" pornography (e.g., Pornhub) [48, p. 3]. Behavioral interventions using an AI avatar have also been used to train law enforcement officers and improve their victim interviewing skills [50].

Legal and regulatory interventions focused on prescribing criminal sanctions against TF-CSEA [51], [52], [53]. They also examined the prescription of legal duties for relevant service providers used to facilitate TF-CSEA, such as digital platforms and financial institutions [54], [55], [56]. Some of these legal duties

require digital providers to deploy specific technological tools and protocols, such as content moderation systems [57]. Another specific example is the European Commission's proposed Regulation to Prevent and Combat Child Sexual Abuse (the CSA Regulation), which mandates that regulated service providers deploy a CSAM automated scanning and detection tool [58].

The delivery of behavioral interventions and legal requirements placed on regulated service providers discussed in this review highlight that technological tools and protocols tend to operate cross-functionally with other types of interventions. We also observed cross-functional interventions among other categories, for example, between legal or regulatory interventions and financial interventions. This includes an anti-money laundering (AML) law, which has been leveraged to impose a legal duty on financial institutions to report suspicious transactions that might relate to CSAM and other forms of sexual exploitation and abuse [55]. It also authorizes the disruption of suspected payments for these crimes [55].

This cross-functional operation between two types of intervention is also reported in actual TF-CSEA interventions featured in the organizations' reports. These confirm the existence of such laws and their operation. However, they show that the application of these laws extends only to reporting obligations and allows law enforcement agencies to track and trace TF-CSEA; the direct payment disruption to prevent the completion of such transactions remains an unmet objective [59].

In the same vein, Dushi [58] highlights a dialectical relationship between legal and regulatory interventions and technological tools and protocols. Dushi argued that the capabilities of an existing tool, in this case, Thorn, to "detect, review and report CSAM" at scale could inspire future legal and regulatory interventions that mandate the deployment of similar technological tools and protocols [58, p. 14]. This kind of mandate could generate further demand for this intervention [58],

which, if successful (as with Thorn), could, in turn, inspire or enable other technological developments [60].

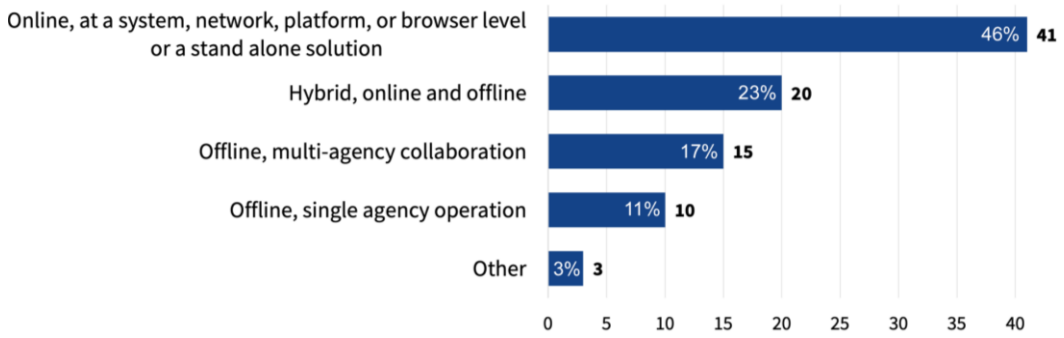
The interventions covered in all the publications reviewed were similar. Overall, peer-reviewed academic publications tended to focus on a specific type of intervention or a set of interventions. The organizations' reports took a different approach, typically emphasizing broad discussions of multisectoral collaboration and focusing specifically on *education and awareness-raising* programs [9], [10], [11], [12], [20], [22], [61], [62], [63], [64], [65], [66], [67].

TF-CSEA Intervention Operations

The interventions were coded by domain of operation. They could be an offline (e.g., in-person) single-agency or multi-agency operation, an online operation at a network, system, platform, or browser, or a standalone operation (see Appendix A). The online operations dominated the intervention landscape (see Figure 4).

Online interventions were most frequently mentioned in the reviewed documents, followed by hybrid (online and offline) interventions. These two categories highlight the prominence of digital technologies in tackling TF-CSEA. Qualitative analysis highlights a growing trend towards technological tools and protocols built on AI, including machine learning (ML) techniques, with 25 out of the 36 technological tools and protocols (Figure 3) coded using AI. Many of these technological tools and protocols are automated screening and detection tools for CSAM [50], [60], [68], [69] or predatory conversations indicating grooming or sexual harassment activities [70], [71], [72], [73]. ML techniques, such as model-agnostic editing, have been leveraged to develop a technical governance mechanism that prevents model-generated sexually explicit content even when prompted, using text-to-image GenAI tools [74].

Figure 4. Frequency of Intervention Operations.



Source: Data based on manually coded articles collected on 17th July 2025 from databases.
Note: *n* = 89 (100%) intervention operations. The units of analysis here are occurrences of coded variables, not the number of publications coded. See Appendix B for the coding frame and definitions of coded variables.

However, the effectiveness and reliability of these ML-driven technological tools and protocols depend on the quality and representativeness of data for model training. Several studies, when discussing the development and assessment of these AI-driven solutions, cited restricted access to real CSAM for model training as a limitation [73], [75], [76], [77]. Collaboration between law enforcement agencies and (often) academic developers offered the necessary data infrastructure for developing these ML solutions [60], [73], [78], [79].

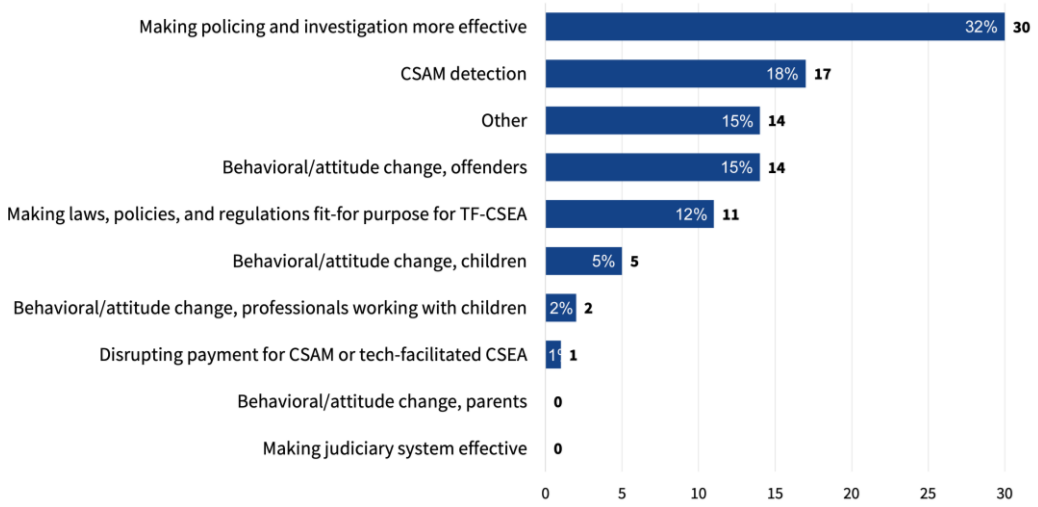
Reflecting the prominent intersection of technical interventions with policing and investigation, hybrid approaches, such as online and in-person interventions, were the second most common operations reported. The least discussed interventions were offline single-agency and offline multi-agency operations. Offline single-agency operations focus on the organization's policy reviews, capacity building, and classification of child sexual exploitation and children's ages. Offline multi-agency operations include TF-CSEA investigations, prosecutions, settlements, implementation of legal requirements, and research.

TF-CSEA Intervention Objectives

The interventions were coded according to their primary objective, such as the detection of CSAM, behavior or attitude change among different actors (such as

children, professionals, or offenders), or improvements to the policing system. As shown in Figure 5, most interventions were geared towards making policing and investigation more effective, followed by CSAM detection. The next most common categories were behavioral/attitude change for offenders and Other. Intervention objectives in the Other category were not predefined in the coding frame. These include, for example, integrating child online safety measures, improving technical safety boundary-setting for GenAI, and behavioral/attitudinal change among third-party observers. Within these subcategories, the integration of child online safety measures was mentioned six times across the coded peer-reviewed publications. This attention to integrating child online safety measures, including content moderation systems, highlights a growing interest in embedded, safety-oriented technological tools, primarily as part of policy interventions. The long tail of other sub-categories demonstrates the diversity and complexity of TF-CSEA interventions.

Figure 5. Frequency of Intervention Objectives.



Source: Data based on manually coded articles collected on 17th July 2025 from databases.
Note: *n* = 94 (100%) intervention objectives. The units of analysis here are occurrences of coded variables, not the number of publications coded. See Appendix B for the coding frame and definitions of coded variables.

Strikingly, none of the interventions studied improved the judiciary's effectiveness in handling TF-CSEA. Nor do existing and available interventions serve the objective of behavioral or attitudinal change among parents. There was only one example of a technological tool having an ancillary effect by disrupting revenue streams from CSAM exchanges [80].

By comparing two coded variables of intervention types and intervention objectives across all the peer-reviewed academic publications, we found that an intervention can serve many intervention objectives. As they are cross-functional with various other types of interventions, technical interventions serve the most diverse range of objectives, from making policing and investigation more effective [41], [70], [72], [77], to CSAM detection and analysis [28], [68], [69], [76], [81], [81], [83], to behavioral or attitude changes among offenders or potential offenders [45]. Notably, technical interventions predominantly serve the objectives of CSAM detection and analysis and improving the effectiveness of policing and investigation.

One unique case involved deploying web crawling and scanning across the open and dark webs to detect illegal content, including CSAM, as an intelligence-gathering tool for policing and investigation. This led to the identification of a collection of online image boards used to host and share CSAM, known as Trichan [80]. The by-product of the Trichan takedown arguably disrupted the financial gains from CSAM exchanges facilitated by this collection of online image boards, which, in turn, disrupted CSAM payments. Another interesting example is a technological tool developed for and by children and young people. It engages young people in its development and serves objectives, such as better-targeted online safety mechanisms and youth empowerment [84].

Other types of interventions serve more specific objectives. For example, policing and investigation-related interventions involve improving the effectiveness of

policing and investigation [85], [86], [87], and detecting CSAM [88]. Behavioral interventions primarily support behavioral change [43], [44], [47], [89], most of which focus almost exclusively on offenders or potential offenders [43], [44], [47], [89]. One unique case in behavioral interventions aims to train personnel involved in policing and investigation to improve their effectiveness [50].

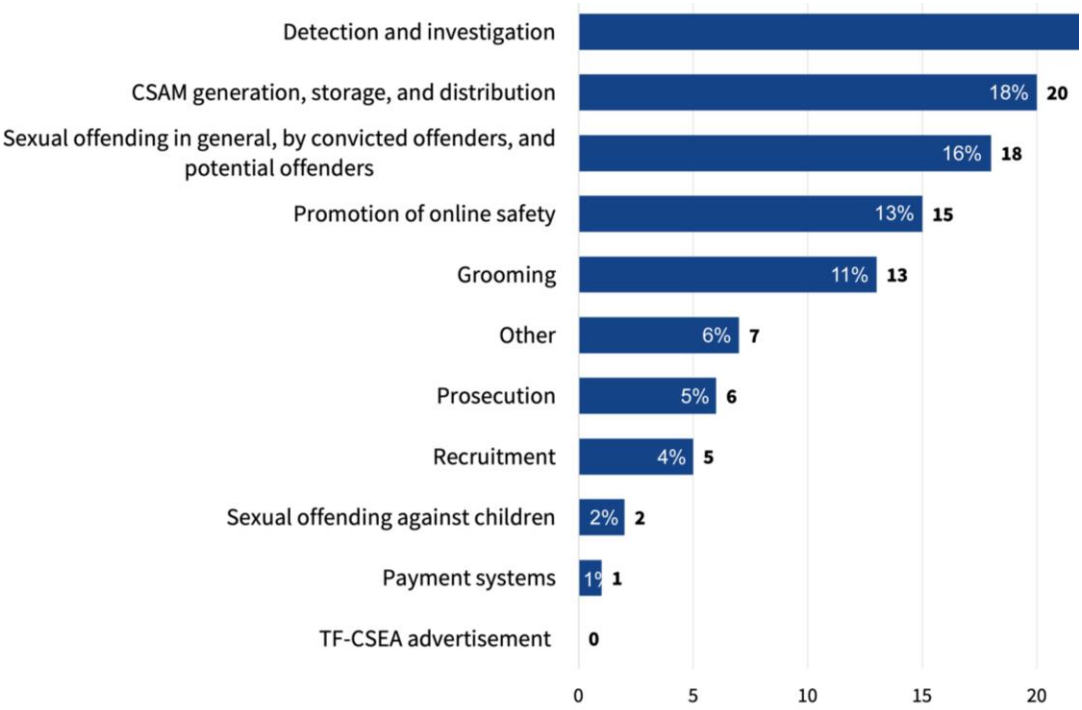
The objective of behavioral or attitude change addressing children is predominantly achieved through education or awareness-raising campaigns [90], [91]. Behavioral or attitude change among professionals working with children has been achieved through both behavioral interventions [92] and education or awareness-raising campaigns [93]. Legal or regulatory interventions naturally serve the objective of making laws and regulations fit-for-purpose for TF-CSEA [51], [53], [54], [57].

Locus of the Intervention within the TF-CSEA Ecosystem

The locus of the intervention refers to the activities that an intervention addresses. These include both the activities within the TF-CSEA offending chain and TF-CSEA prevention and response. See Appendix A for the full list.

The majority of the publications reporting on TF-CSEA interventions addressed detection and investigation (n = 28) (see Figure 6). The next most commonly reported categories were: CSAM generation, storage, and distribution (n = 20); sexual offending (n = 18); promotion of online safety (n = 15); and grooming (n = 13). Additionally, several points in the TF-CSEA offending chain and prevention and response pathways addressed in the intervention did not fit our predefined categories. These intervention loci were each mentioned only once or twice across the peer-reviewed publications and organizations' reports. Examples of these categories include promoting (law enforcement) officers' wellbeing; platform accountability and transparency; victim support; and research on CSAM.

Figure 6. Frequency of Intervention Locus Within the TF-CSEA Ecosystem.



Source: Data based on manually coded articles collected on 17th July 2025 from databases.
Note: *n* = 114 (100%) intervention mechanisms and their impacts on the intervention chain. The units of analysis here are occurrences of coded variables, not the number of publications coded. See Appendix B for the coding frame and definitions of coded variables.

Four predefined elements within the TF-CSEA ecosystem were discussed only six or fewer times across the coded peer-reviewed publications. These categories were prosecution, recruitment, sexual offending against children (in general), and payment systems. There was a fifth category, TF-CSEA advertisement, that did not appear in any of the publications.

Within this long tail of less frequently discussed items, the fewest publications (n = 1) reported interventions designed to address digital payment systems used to purchase CSAM. The Trichan takedown is the only evidence demonstrating the desirable ancillary effect of disrupting revenue streams from CSAM exchanges [80]. Thus, we coded this as an effect on payment systems that fuel the commercialization of CSAM and other TF-CSEA offending. Evidence from the organizations' reports [9], [20], [59], [63], and other background research [94],

suggests a distinct lack of direct interventions into specific digital payment systems to stop or prevent payments.

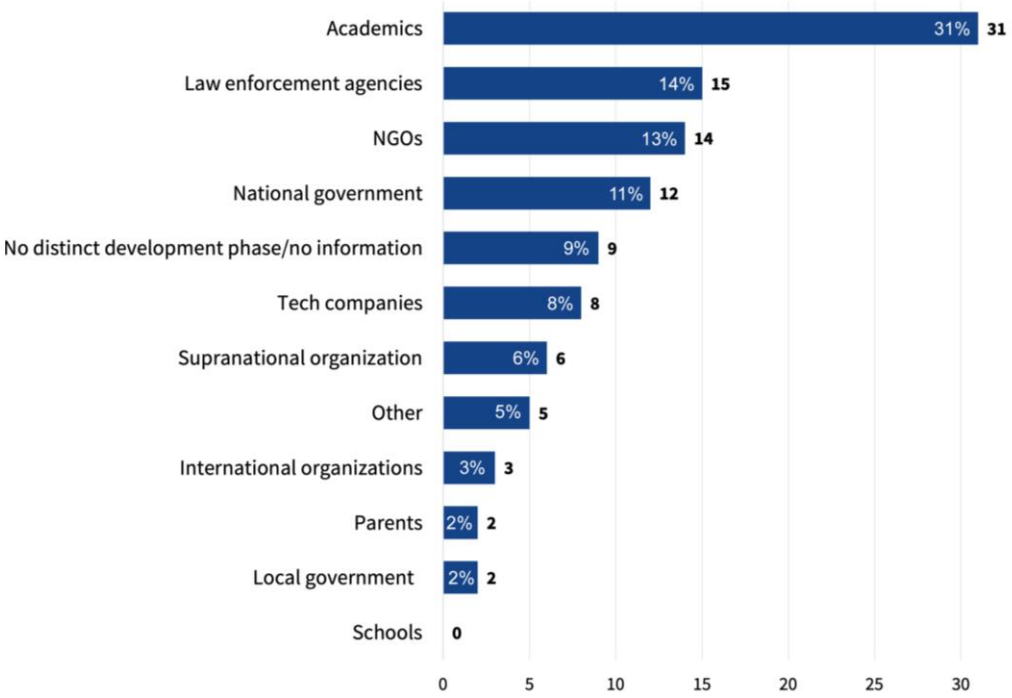
There are existing financial interventions involving collaboration between financial institutions and digital payment service providers worldwide. However, these only provide evidence of transactions involving CSAM or other TF-CSEA, so that law enforcement agencies can trace them back to perpetrators ex post facto [9], [20], [59], [63]. No publication reported on advertisement of self-exploitation or self-generated CSAM; our mapping exercise of TF-CSEA occurrences and relevant variables and data points identified these as emerging practices [7].

Stakeholders Driving TF-CSEA Intervention Development, Implementation, and Research

Stakeholders coded in each article included developers, implementers, and assessors of interventions (if assessments were done), and funders for interventions and/or assessments. Our analysis of the coded variables, comparing developers with implementers, and the types of interventions reported, presents a diverse overview of the stakeholders and the roles each plays.

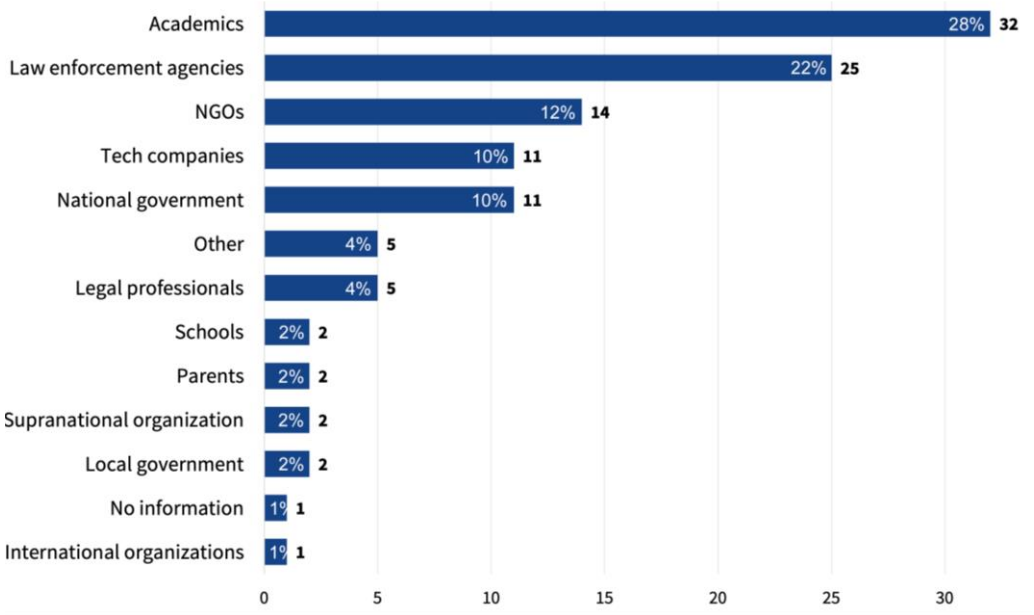
Details about these stakeholders were identified from the peer-reviewed academic publications (see Figures 7 and 8). These include supranational organizations (such as the EU), parents, schools, and academics. However, most publications reported on academics as both developers and implementers, focusing predominantly on the technological tools and protocols, sometimes in collaboration with law enforcement agencies [60], [73], [75], [78], [79]. Academics were also reported to have developed and/or implemented behavioral interventions [43], [55], as well as education, literacy, and awareness-raising campaigns [95], [96].

Figure 7. TF-CSEA Intervention Developers.



Source: Data based on manually coded articles collected on 17th July 2025 from databases.
Note: *n* = 107 (100%) intervention developers. The units of analysis here are occurrences of coded variables, not the number of publications coded. See Appendix B for the coding frame and definitions of coded variables.

Figure 8. TF-CSEA Intervention Implementers.



Source: Data based on manually coded articles collected on 17th July 2025 from databases.
Note: *n* = 113 (100%) intervention implementers. The units of analysis here are occurrences of coded variables, not the number of publications coded. See Appendix B for the coding frame and definitions of coded variables.

The next most reported categories about developers and/or implementers of TF-CSEA interventions were law enforcement agencies, NGOs, and national governments (see Figures 7 and 8). Peer-reviewed academic publications reported that law enforcement agencies primarily engaged in policing and investigation. These agencies are leading the way in devising investigative techniques and are increasingly leveraging technologies to improve the effectiveness and efficiency of their investigations [24], [42], [50], [87].

The peer-reviewed publications also documented the diverse roles that NGOs play in TF-CSEA interventions, spanning technological tools and protocols [80], policy interventions [97], education, literacy, and awareness-raising campaigns [98], [99], behavioral interventions [100], and policing and investigation [101]. Publications rarely reported on interventions developed and/or implemented by supranational organizations, schools, or parents.

Peer-reviewed academic publications also reported that national governments play diverse roles. These include developing and implementing mainly policy interventions [102], [103], law and regulatory interventions [51], [52], [55], and policing and investigation efforts [103], [104], [105]. In one case, for example, a government agency worked with academics to develop and implement perceptual hashing using a pretrained vision transformer as a technological tool to identify known illegal content, including CSAM [69].

The work of international organizations did not feature as prominently in peer-reviewed academic publications as in their reports. This difference is likely the result of a genre bias, given the different intended audiences and writing styles between academic publications and the reports. Our comparison across the three coded variables of intervention development, implementation, and intervention types shows that international organizations are mainly leading the development of policy and regulatory frameworks [53], [102]. These organizations also provide

technological tools and protocols, as well as support, particularly in policing and investigation [103]. Technology companies are second only to academics in the frequency with which they drive the development and/or implementation of technological tools and protocols [68], [82], [106].

We note that the TF-CSEA intervention ecosystem is complex. There are other types of stakeholders operating their own programs of activities to combat TF-CSEA that were not mentioned in any of the reviewed documents. Examples include industry alliances, such as the Global System for Mobile Communications Association (GSMA) and the Asia-Pacific Financial Coalition Against Child Sexual Exploitation (APFC).

Our qualitative analysis of the authors' funding statements in their publications (while not exhaustive of all relationships) identified another influential stakeholder group: funders. Of the 86 peer-reviewed academic publications, 31 did not provide any funding information, and 4 reported receiving no funding. Of the 51 publications that received funding, our analysis identified a diverse group of funders. We list examples of these funders to reflect their institutional and geographical diversity:

- Government agencies and research councils, for example, UK Research and Innovation (UKRI) [107], Economic and Social Research Council (ESRC) [108], Dutch Research Council (Nederlandse Organisatie voor Wetenschappelijk Onderzoek, NWO) [54], and São Paulo Research Foundation (Fundação de Amparo à Pesquisa do Estado de São Paulo, FAPESP) [75], [78], [79]
- Universities, research centers, and research institutions, such as the Leverhulme Centre for the Future of Intelligence [71], Australian Institute of Criminology [109], Forensic Psychology Research Institute [110], and New York University Shanghai [50]

- Foundations and not-for-profit organizations, for example, Hayao Nakayama Foundation for Science & Technology and Culture [50]
- International organizations and supranational unions, such as the European Union's Horizon 2020 [24]
- Commercial companies, such as Google LARA 2021 [79] and Meta [111].

By comparing the two coded variables, funding and intervention types, we found that most funding reported in peer-reviewed academic publications was devoted to research on technological tools and protocols, followed by policing and investigation. Funding for technological tools and protocols accounted for 24 of the 51 peer-reviewed academic publications that received funding. Eleven peer-reviewed academic publications examined policing and investigation. The third-most-funded research area was behavioral intervention.

Interestingly, the organizations' reports listed a broader range of funders, including major funding organizations in the field. These include Safe Online and the International Justice Mission's Centre to End Online Sexual Exploitation of Children. The diversity of interventions discussed in these reports makes it difficult to identify patterns among funding, funders, and the specific types of interventions financed.

The organizations' reports also show that intergovernmental organizations (a category not mentioned in the peer-reviewed publications) play a key role in combating TF-CSEA. These organizations developed and coordinated policy frameworks for implementing national TF-CSEA interventions and provided technical support and training [9], [10], [11], [13], [20], [63]. These efforts are particularly dominant in developing countries.

National governments and government agencies, as the primary duty-bearers for children's rights, are also reported as playing roles in both the development and implementation of various types of interventions. These primarily include policy

and budget coordination, responses to TF-CSEA cases, and the development and implementation of education and awareness-raising campaigns [10], [11], [65], [66]. Law enforcement agencies, especially the specialized units, are critical for policing and investigating these crimes. They are increasingly collaborating with technology companies, particularly those operating digital payment systems, including cryptocurrencies [10], [12], [20], [63], [64].

Although beyond this review's scope, our background reading of the organizations' reports shows that NGOs are providing mainly victim support services, including crisis response, and hotlines or helplines for suspected TF-CSAM, thus filling the service gap left by government agencies [9], [64], [65], [66]. Examples of these services include Childline Kenya, Action Pour Les Enfants (APLE) Cambodia, C-Sema in Tanzania, and Protect and Save the Children in Malaysia. The organizations' reports depict two private sectors: technology companies, such as Apple, Facebook, Google, and Microsoft, and financial or digital payment service providers, such as Wings [9] and Western Union [20], as key contributors to TF-CSEA interventions. However, these are mainly related to detecting and reporting CSAM and suspicious financial transactions [10], [13], [66], [67]. There were few reports of technology companies driving the development of technological tools and protocols to curb TF-CSEA.

In summary, international organizations, academics, law enforcement agencies, NGOs, and national governments play important yet diverse roles in developing and implementing TF-CSEA interventions. Another key stakeholder group with the financial power to direct research, development, and assessment of TF-CSEA interventions includes various types of funders, ranging from government agencies and research councils to universities, not-for-profit organizations, and commercial companies.

How Well Does the Intervention Work?

Our second research question concerned the effectiveness of the reported intervention. The analysis in this section is based on the reported scale of the intervention, information on its assessment, and some examples of promising interventions.

We interpret the scale of the intervention based on its likely reach. For example, legal and regulatory interventions likely mean that the legal protection or provisions will apply nationwide. Or, in the case of the USA, federal laws would likely benefit the population nationwide, while state laws would only benefit the population within the relevant states. A technological tool or protocol is likely applicable across geographical borders.

Our findings show a diverse scale of intervention operations, with the majority having the potential to be applied across geographical and jurisdictional borders due to their technical components [72], [81], [82], [106], [112]. Legal and regulatory interventions can also be applied across jurisdictions, at least in principle, with the power of their extra-territorial scope, as in the case of the Digital Services Act (DSA) [54], [56], [114]. Financial interventions as a TF-CSAM intervention likely require cross-border and multistakeholder collaboration to track and trace transactions, with the impact potentially spanning multiple jurisdictions depending on the locations of victims and perpetrators [10], [55], [59].

However, the evidence from operational financial interventions suggests that their effects only extend to tracking and tracing transactions that fuel TF-CSEA offending. They are not yet disrupting or blocking payment [59], [94]. Other types of intervention, such as policing and investigation [85], [87], [108], education, literacy, and awareness-raising campaigns [90], [93], and behavioral interventions, tend to be situation- and jurisdiction-bound [43], [46], [89]. That

said, learning what works increases the likelihood that interventions will be transferable across jurisdictions.

We systematically coded peer-reviewed academic publications according to whether they included any form of intervention appraisal and whether that appraisal was conducted by the same entity that developed or implemented the intervention. Among the 86 peer-reviewed academic publications, 75 included some form of appraisal. Of these 75, 47 were appraised by independent parties, meaning parties that had not developed the intervention.

The assessments tended to focus on describing the interventions perceived to be working well, the conditions under which they worked, and the challenges that constrained the success of the particular intervention. We report on what worked and the challenges encountered in these intervention implementations, grouped by the types of interventions most frequently examined. As the TF-CSEA ecosystem is complex, the core value of evidence synthesis lies in reporting insights that represent the diversity of both the offending and the mechanisms to prevent and respond to these crimes.

Successful and/or Promising Interventions

Our mapping of the interventions and their assessments identified four key types that have the potential to be applied or transferred across geographical and jurisdictional boundaries. These include: technological tools and protocols, legal and regulatory interventions, policing and investigation, and behavioral interventions.

Technological Tools and Protocols

Most technological tools and protocols that are in operation and received positive appraisal from the organizations' reports and peer-reviewed academic publications predominantly focused on detecting or filtering CSAM, as well as automated content scanning [113]. Examples include PhotoDNA, as originally

developed by Microsoft [10], [82], Thorn's Safer Predict [115], IWF's URL and Hash list [28], and child sexual abuse images (CSAI) [10], [28], [80], [82], [113], [115]. The measurement of success of these technological tools and protocols was based on their actual application and their effectiveness in accurately detecting CSAM and CSAI, as well as user surveys at scale. Only one of the tools, automated content scan, integrated machine learning (ML) models [112].

We identified two additional technological tools and protocols from peer-reviewed academic publications that were deployed in actual investigations. One was a technological tool used to investigate request traffic within Freenet. This identified CSAM downloaders and uploaders using a Bayesian hypothesis test, a mathematical model, to aid law enforcement investigations [41]. The effectiveness of this technological tool is demonstrable through its deployment in investigation and prosecution processes in the USA, resulting in convictions on charges involving engagement in child sex tourism, and the production, possession, receipt, and distribution of CSAM [41, p. 1506].

The other technological tool featured the use of a customized web crawler developed and deployed by the Canadian Centre for Child Protection (C3P) to search the open and dark webs for CSAM and check these images against a database of known abuse materials. This provided the necessary evidence to shift law enforcement's focus from negotiation to applying commercial pressure on the foundational internet infrastructure providers, resulting in the eventual closure of Trichan sites [80].

Other promising technological tools and protocols exist. Many leverage AI techniques, including ML, to detect either CSAM [60], [116], or predatory or sexually unsafe exchanges online, especially on social media platforms [70], [73], [117]. One promising AI-driven solution achieved statistically significant reliability in governing the technical capabilities of GenAI, preventing the governed AI

models from generating sexually explicit content involving children [74]. Another promising technological tool leveraged a customized automated web crawler to execute various cyberattacks against the child exploitation networks of website domains to disrupt their operations [112]. These were developed and appraised as effective primarily to aid CSAM and grooming detection and investigation, and to enhance policing and investigation. However, they were only tested for accuracy and effectiveness in lab settings, rather than deployed in actual interventions.

Despite these promising results, these data-driven technological tools and protocols are only as good as their training data. Challenges related to the scale and volume of the training data, which shape the effectiveness of these interventions, remain unresolved. We discuss these in more detail in the sub-section concerning challenges to successful TF-CSEA interventions.

Legal and Regulatory Interventions

As the technology-enabled element of TF-CSEA offending makes the crime borderless, legal and regulatory interventions need to be globally aligned, at least in principle, or have extraterritorial scope for them to stand a chance of being effective. Our qualitative analysis of the organizations' reports and peer-reviewed academic publications identified two examples of legal instruments that have cross-border influence in and beyond Europe, and one promising legal and regulatory intervention.

The first example is the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) [3], setting out criminal offences for a broad spectrum of TF-CSEA, including child grooming for sexual purposes, and obliging signatories to criminalize these activities. The Lanzarote Committee further recommended that state parties extend the definition of child grooming for sexual purposes to include sexual abuse committed solely online [9], [10], [22]. As a legal instrument, the Lanzarote

Convention has resulted in the introduction or amendment of existing national laws to criminalize child grooming and other TF-CSEA in Italy [52], the Philippines [20], Malaysia [65], Cambodia [9], Ethiopia [67], South Africa [22], and Ghana [13].

The second example shows that criminal sanctions against CSEA, as set out, for example, in the EU's Directive 2011/93/EU [23] in demand-side countries, have the desired cascading effect on disrupting TF-CSEA in supply-side countries like the Philippines [59].

Other promising legal instruments at national and regional levels include mandating transparency mechanisms for regulated technology companies. This would hold these companies accountable for their facilitation of TF-CSEA, and help detect and protect children from these crimes. Examples of these legal instruments include the Australian Online Safety Act 2021 and UK Online Safety Act 2023 [114], and the EU Digital Services Act 2022 [54], [56], [57]. These national and regional laws have extraterritorial scope [118], [119], [120]. They all mandate transparency mechanisms, requiring technology companies to moderate content generated and exchanged using their services. They also require reports on the prevalence of illegal and harmful content and their content moderation decisions, including measures taken to tackle the availability of such content [118], [119], [120]. However, these laws face enforcement challenges and difficulties in aligning their reporting metrics.

Policing and Investigation

Various policing and investigative techniques identified in the organizations' reports and the peer-reviewed academic literature tend to be applied within their respective national borders. However, technologies used to enhance policing and investigation can be transferable across geographical borders and jurisdictions. Several organizations' reports highlighted the importance and positive outcomes of digital intelligence gathering and investigative tools, such as INTERPOL's

International Child Sexual Exploitation (ICSE) database, in aiding international policing and investigations. The use of such technology has resulted, for example, in victim rescue through an ICSE referral in the Philippines [120], and a tip from INTERPOL about a Thai offender who was later charged with online human trafficking and sentenced to 146 years in prison [63]. Similar technology use has also resulted in the arrest and prosecution of child sex offenders in multiple countries, including Thailand, Australia, and the USA, as part of Operation Blackwrist [63].

Similar to what has been identified from the organizations' reports, information technologies, such as a child protection system (GridCop®), have been used to identify local peer-to-peer network traders of child sexual abuse images and videos [103]. A broader range of technologies for policing and investigation has been identified from peer-reviewed academic publications. These include online undercover child abuse investigations [121] and the use of voice analysis technology, such as a computer voice stress analyzer (CVSA) in an investigation, to obtain important, secure, critical offence information [122]. Walker et al. [101] also reported positive outcomes from engaging non-offending partners and affected family members, leading to enhanced evidence and disclosures about offending behaviors and bail breaches.

Behavioral Interventions

The transferable learning from the successful deployment of behavioral interventions centers on having a message, content, or approach that helps service users overcome their fears, for example, of judgment and shaming. Many behavioral interventions aimed at preventing and deterring prospective or actual offenders from accessing or viewing CSAM use warnings [45] and therapeutic messages [48]. Prichard et al. [48] found that deterrent and therapeutic referral messages had a significant positive impact on reducing click-through rates to

such illegal content. Similarly, the use of digital media campaigns to encourage the target audience (those with pedophilic inclinations) to seek help to avoid committing child sexual abuse or consuming CSAM. These were considered a success, having directed 15–20 individuals a month to seek help from the Berlin research office [43]. The success of this intervention lies in its non-judgmental communication approach, which led the German Parliament to pass legislation to fund specialized, anonymous treatment services for self-referred individuals through the health insurance system [43]. This approach also informed the design of advertisements placed on search engine results pages in response to individuals' entry of keywords when searching for child sexual exploitation materials, a behavioral intervention explored in New Zealand [47].

Stop It Now!, a UK and Ireland project operated by the Lucy Faithfull Foundation, operates an anonymous and confidential helpline service using the telephone, online chat, and/or email for anyone concerned about their own or others' sexual behavior. This includes convicted sex offenders and those at risk of sexual offending [98]. A survey of self-reported behavioral change showed that 80% of survey respondents reported they had stopped viewing child sexual abuse images, while 60% reported changing their behavior to avoid potentially risky situations [98].

Another noteworthy behavioral intervention is an internet-based eight-week cognitive behavioral therapy (CBT) course with therapist support and psychotherapist feedback. This targets participants' thoughts and emotions related to problematic behaviors or exposure to high-risk situations, leading to CSAM viewing [123]. A randomized controlled trial (RCT) on participants recruited from the dark net showed a significantly larger drop in CSAM viewing time among program participants than among those in the psychological placebo control groups from pre- to post-treatment to follow-up [123]. The key to this

intervention's success, according to the researchers, lay in the CBT methods and content, which targeted high-risk situations, thoughts, and emotions leading to CSAM consumption [123].

Education, Literacy, and Awareness-Raising Campaigns

When it comes to education, literacy and awareness-raising campaigns, the approach taken to children's knowledge and skill development, designed to keep them safe from TF-CSEA, is a key successful intervention. Using a game-based format, which appeals to children's playful nature, can be another factor that makes such campaigns applicable across jurisdictions and cultural contexts.

An outstanding example of such an educational campaign is the End Violence Against Children (EVAC) game developed by ECPAT International and UNICEF. EVAC is a digital educational game using inquiry-based learning, which is focused on issues of child sexual exploitation and grooming to help children, primarily in Thailand and Cambodia, develop knowledge and awareness of internet safety and child online grooming [91]. The initial evaluation of the game's effectiveness involved observations of professionals who used the precursor simulations and users' feedback on the game. Feedback from educators shows that 94% perceived their students as having developed greater knowledge and awareness of internet safety and online grooming [91]. Among users, 87% found the game extremely effective at prompting discussion and illustrating grooming situations [91]. However, there is no record of these gains in knowledge or awareness resulting in behavioral changes, possibly due to the lack of longitudinal studies on the impact of this type of intervention.

Challenges to Successful TF-CSEA Interventions

Despite demonstrable capabilities and success across diverse interventions, challenges remain in combating TF-CSEA. First, legal and regulatory interventions often fall short in implementation and enforcement. Where robust legal and

regulatory interventions exist in principle, some legal requirements still lack consistency on reporting metrics, and as a result, the data submitted are incoherent [54], [56], [114]. Examples include transparency requirements prescribed under the UK and Australian Online Safety Acts and the EU Digital Services Act.

In addition, the technological component of CSEA offending and the complex internet ecosystems make CSEA offending a moving target, often leaving laws and regulations lagging behind emerging ways of offending, and creating gaps in child protection against these crimes [124], [125]. For example, online sexual extortion and the livestreaming of child sexual abuse are not covered by relevant Cambodian law (such as the Law on Suppression of Human Trafficking and Sexual Exploitation, or the Criminal Code) [9]. Similarly, in Indonesia, neither the Penal Code, nor the Law on Pornography, nor the Law on Information and Electronic Transactions criminalize the livestreaming of child sexual abuse or online grooming [10]. This is also the case with the Thai Penal Code and other laws [63]. The case of the Trichan takedown highlighted the failure of a regulatory light-touch approach to internet governance to protect children against tech-facilitated CSAM distribution and commercialization [80].

Second, although technological tools and protocols are advancing at a pace consistent with TF-CSEA, their effectiveness is constrained by the quantity, diversity, and quality of data available for training models [68], [75], as well as by privacy concerns [110], [126]. While access to verified CSAM for training, developing, and testing technological tools and protocols may improve the accuracy and reliability of the tools, access to or use of CSAM beyond law enforcement purposes is never straightforward. It is riddled with ethical and legal issues, not least concerning victim consent and researchers' wellbeing.

Other constraints on the effectiveness of technological tools and protocols include scalability [127], platform functionalities [115], and quality control due to reliance on third-party freeware [116]. Importantly, although most technological tools and protocols examined in this review involved accuracy testing, none discussed the gravity of a false positive result on an individual in an actual situation. Nor did they discuss channels through which a false positive could be challenged and remedied. Given these limitations, care is needed when examining the findings on technical advances to discern whether they are steps that contribute, for example, only as a proxy task [75], or create a viable solution.

Another challenge is that while some technological tools and protocols are effective, for example, in detecting CSAM and sending removal notices to companies hosting such materials, the organizations deploying these technologies lack legal authority or enforcement powers [80], rendering the solution ineffective.

Third, technical tools are playing an increasingly important role in aiding policing and investigation. However, more training is needed for law enforcement officers and forensic personnel, so that technological tools and protocols can be effectively integrated into policing and investigation [105], [128]. More technical tools are also needed to support law enforcement agencies in combating increasingly complex and elusive TF-CSEA [109].

Finally, educators and other professionals working with children may lack knowledge of TF-CSEA [92], [93]. This underscores the importance of education, literacy, and awareness-raising campaigns as TF-CSEA interventions, not only for children but also for adults.

SECTION 5. CONCLUSION AND RECOMMENDATIONS

The multidisciplinary approach underpinning our systematic review has yielded the desired result of identifying diverse types of TF-CSEA interventions and appraisals. Drawing on computer science and computational forensics, we identified various technological tools and protocols [50], [60], [68], [69], [70] and their cross-functional application with other types of interventions, such as policing and investigation [42], [104], behavioral interventions [48], and regulatory interventions [58]. Literature from criminology and criminal justice [80], [129], [130], and digital humanities [130], [131] was a valuable source on the state of the art in policing and investigation. Naturally, literature from legal and policy studies and from social science disciplines tends to highlight policy and regulatory gaps [51], [56], [114], [125]. Likewise, psychology and public health studies offer rich insights on key ingredients for successful behavioral interventions, although these predominantly covered procedures directed at potential or convicted sex offenders to prevent TF-CSEA offences and recidivism [43], [46], [47], [98], [100], [123].

The breadth of interventions identified in this systematic literature review suggests a strong foundation for tackling this multifaceted crime. However, there is a clear requirement for continuous international and multi-agency collaboration to stay abreast of the technological components and advances that make this crime a moving target.

> **Recommendation 1**: International organizations, intergovernmental organizations, and/or research institutes should be funded to conduct research on TF-CSEA interventions and develop repositories of evidence-based practice to facilitate the further development and improvement of existing tools.

Based on the current state of the art of TF-CSEA interventions, emerging technologies are not only exacerbating the problem; they are also propelling *technological tools and protocols* to combat the problem, mainly towards the areas of CSAM or CSAI detection [10], [28], [80], [82], [113], [115]. There is a growing number of *technological tools and protocols* leveraging AI techniques to detect CSAM [60], [116]. However, CSAM is already in the public domain and thus incorporated into the training data. For example, an image-based dataset, LAION-5B, was used to train an open-source deep learning model, Stable Diffusion [132]. Such CSAM contamination exacerbates the risks and harms of CSAM production, distribution, and commercialization, resulting in both revictimization of CSAM subjects and enabling AI tools to generate similar content. At the same time, commercial developers and academics are bound by legal and ethical constraints on their access to verified CSAM for training and testing the performance of their AI-driven tools [68], [75].

> **Recommendation 2**: Policymakers, law enforcement agencies (LEAs), and other organizations that hold CSAM data should foster closer collaboration with authorized academics and commercial developers to produce safe, secure, and privacy-respecting methods of leveraging CSAM data to improve the reliability of technological tools and protocols. Priority should be given to approaches that do not enable researchers or commercial developers to have direct access to CSAM, and without these sensitive data leaving agencies' secure storage. For example, access to these data could be through remote execution, or execution by LEA partners to validate a model's reliability [75], [78], [79], or secure data sandboxes for algorithm or model testing.

This systematic literature review has also demonstrated the increasingly important role that technologies play in raising the effectiveness of policing and

investigation. However, not every country has direct access to use, or the technical capacity to develop, its own technical tools for policing and investigating TF-CSEA [9], [64], [65], [66], [104], [109], [125]. In many countries, especially in developing countries, the lack of stable, dedicated, and secure internet connections remains a basic obstacle to policing and investigation. Law enforcement officers and forensic personnel also require periodic training to stay abreast of technological advances in order to effectively police and investigate TF-CSEA crimes, and to integrate available technologies into their work [10], [11], [85], [103], [108]. While international collaboration, for example, led by INTERPOL, has played an important role in bridging this divide through intelligence sharing [12], [53], [63], [66], [103], [133], there is room for more such cooperation.

> **Recommendation 3**: National governments should allocate more funding to capacity building for law enforcement officers and forensic personnel, equipping them with the knowledge, skills, technological infrastructure (such as stable internet), and tools to detect and investigate TF-CSEA, with support from international experts.

Our review also identified effective measures within international law to align the scope and framework for criminalizing and sanctioning TF-CSEA across multiple jurisdictions [9], [13], [20], [22], [52], [65], [67]. National and regional laws with extraterritorial scope also indicate potential to work across geographic borders and jurisdictions to hold technology companies accountable for facilitating CSEA [54], [56], [57], [114]. There is more room for international and national efforts to leverage legal instruments to harmonize the criminalization of, and sanctions against, evolving TF-CSEA, including measures to hold technology companies accountable for facilitating these crimes. This could include devising legal requirements for digital payment services to disrupt suspected transactions related to CSEA [10], [11], [59], [64].

Recommendation 4: International organizations and national governments should work together to harmonize criminal sections for TF-CSEA, promote extraterritorial scope in relevant national and regional laws, and identify measures to consistently enforce this provision across jurisdictions.

Recommendation 5: Legislators should update relevant laws and regulations, including extending the duty to report suspicious financial transactions to digital payment and gift exchange platforms, to bridge the gap in financial interventions to combat TF-CSEA. Where appropriate, legislators should also introduce legal requirements for financial institutions, digital payment, and gift exchange platforms known for their frequent use of financing TF-CSEA to disrupt flagged CSEA-related transactions.

Our review also showed that user-centric design of behavioral interventions, education, literacy, and awareness-raising campaigns has borne positive results, for example, in lowering CSAM consumption [48], [98] and increasing awareness of online safety and grooming [91]. This approach to behavioral interventions, education, literacy, and awareness-raising campaigns could be more widely encouraged, given its positive impact on preventing TF-CSEA.

Funding inevitably plays an important role in enabling research on, and the development, implementation, and maintenance of, interventions. Our systematic review shows that funding for research and intervention development is currently concentrated on technical interventions alone. As TF-CSEA is complex and multifaceted, funding to detect, deter, investigate, and prosecute these crimes could be distributed more evenly across different types of interventions.

Recommendation 6: Funding organizations should recalibrate their priorities and distribute funding resources more evenly across different

types of interventions. Priority should be given to behavioral research, including longitudinal research, to determine which interventions translate to behavioral changes given the evidence gap in this area.

GLOSSARY

Artificial intelligence (AI)	A suite of computing techniques that enable machines to complete tasks that traditionally require human intelligence [134].
Avatar	A computer-generated character or persona that represents an individual in a digital environment, often in digital games, simulations, and virtual environments [50].
Child(ren)	Individuals aged 18 or under [1].
Child sexual abuse images (CSAI)	Images depicting and/or documenting sexually abusive or exploitative acts involving a child [6].
Child sexual abuse materials (CSAM)	Materials depicting and/or documenting sexually abusive or exploitative acts involving a child [6].
Child sexual exploitation and sexual abuse (CSEA)	The involvement of children in sexual activities in exchange for something from third parties and/or perpetrators, and the subjection of children to engage in sexual activities, with or without children's awareness [6].
CSAM downloaders	Receiving points for materials depicting and/or documenting sexually abusive or exploitative acts involving a child from the internet [41].
CSAM uploaders	Distribution points for materials depicting and/or documenting sexually abusing or exploitative acts involving a child onto the internet for others to access [41].
Click through rate	The rate at which internet users click on or respond to the actions called for after seeing the content (e.g., an advertisement or message) compared to the number of times it was shown [45], [48].
Computerized voice stress analysis (CVSA)	Computer software designed to detect changes in voice patterns resulting from stress to infer deceptive responses; a form of truth verification [122].
Dark web	An unindexed and hidden part of the internet that requires special software, such as the Tor browser, to access; often used for anonymous communications and illegal marketplaces [135].
Deep learning model	A type of machine learning model using multiple processing layers, similar to a human

	brain, to learn patterns and make decisions without explicit human instructions [136].
Freeware	Software, often proprietary, made available to the general public at no monetary cost.
Harm	Immediate or latent occurrences of adverse impacts on a person's physical and mental wellbeing.
Law	Mandatory conduct, or prohibition thereof, resulting from a legislative process.
Machine learning (ML)	A type of AI that learns to recognize patterns of training data and make inferences about new data, and based on the inferences, make decisions and predictions without explicit instructions from humans [137].
Open/surface website	The open internet is the unhidden internet as we know it.
Peer-to-peer network traders	Participants who directly exchange digital goods or services on an equal footing with another peer, using a computer network where computers act as equal points of exchange [131].
Regulation	Measures for implementing principles established by law.
Risk	Possibility or probability of adverse outcomes or actual harms.
Text-agnostic model (more commonly model-agnostic)	An approach or framework that can work with any type of machine learning, irrespective of how the model was built [74].
Text-to-image generative AI	A type of AI capable of generating images from written descriptions.
Web crawler	A computer program designed to read or view content on the internet and collect relevant information from the internet.
Website domain	A website address, the internet version of a physical address.

REFERENCES

[1] UN (United Nations) Committee on the Rights of the Child, *Convention on the Rights of the Child*. UNICEF, 1989. [Online]. Available: www.unicef.org/child-rights-convention/convention-text

[2] ILO (International Labour Organization), *Convention (No. 182) concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour*. 1999. Accessed: Jan. 28, 2026. [Online]. Available: https://treaties.un.org/Pages/showDetails.aspx?objid=080000028008ccbd&clang=_en

[3] Council of Europe, *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201) (Lanzarote Convention)*. 2010. Accessed: Jan. 28, 2026. [Online]. Available: www.coe.int/en/web/conventions/full-list

[4] UN (United Nations) Office on Drugs and Crime, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*. 2024. Accessed: Jan. 28, 2026. [Online]. Available: www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

[5] P. Davis, "Spike in online crimes against children a "wake-up call'," National Center for Missing & Exploited Children Blog, April 9, 2025. Accessed: Oct. 27, 2025. [Online]. Available: www.missingkids.org/content/ncmec/en/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call.html

[6] ECPAT International, *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Second Edition*, 2025. Accessed: May 10, 2025. [Online]. Available: https://ecpat.org/wp-content/uploads/2025/04/Second-Edition-Terminology-Guidelines-final.pdf

[7] K. Pothong, "The roles of technologies in facilitating child sexual exploitation and abuse: A mapping exercise," IPIE (International Panel on the Information Environment), Unpublished, 2025.

[8] S. Livingstone and M. Stoilova, *The 4Cs: Classifying Online Risk to Children*. Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI), CO:RE—Children Online: Research and Evidence, 2021. [Online]. Available: https://doi.org/10.21241/ssoar.71817

[9] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Cambodia: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4136/file/DH-Cambodia-Report-2022.pdf

[10] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Indonesia: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence Against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4141/file/DH-Indonesia-Report-2022.pdf

[11] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Mozambique: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence Against

Children, 2022. [Online]. Available: https://safeonline.global/wp-content/uploads/2023/12/2027-DH-MOZAMBIQUE-REPORT-ENGLISH-VERSION.pdf

[12] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Namibia: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence Against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4176/file/DH-Namibia-Report-2022.pdf

[13] UNICEF, *Ending Online Child Sexual Exploitation and Abuse: Lessons Learned and Promising Practices in Low- and Middle-Income Countries*. New York, 2021. [Online]. Available: www.unicef.org/media/113731/file/Ending%20Online%20Sexual%20Exploitation%20and%20Abuse.pdf

[14] WeProtect Global Alliance, *Framing the Future: How the Model National Response Framework Is Supporting National Efforts to End Child Sexual Exploitation and Abuse Online*, 2022. [Online]. Available: www.unicef.org/media/121066/file/Framing%20the%20Future.pdf

[15] UNICEF, *Recommendations for the Online Gaming Industry on Assessing Impact on Children*. 2020. Accessed: Jan. 23, 2026. [Online]. Available: www.unicef.org/childrightsandbusiness/media/1511/file/Recommendations-for-Online-Gaming-Industry.pdf

[16] UNICEF, *MO-CRIA: Child Rights Impact Self-Assessment Tool for Mobile Operators*, May 2021. Accessed: Jan. 28, 2025. [Online]. Available: www.unicef.org/reports/mo-cria-child-rights-impact-self-assessment-tool-mobile-operators

[17] UNICEF, *Guide to Using the Child Online Safety Assessment Tool: Empowering Technology Companies to Promote a Safe Online Environment for Children*. 2016. [Online]. Available: https://www.yumpu.com/en/document/read/56404479/guide-to-using-the-child-online-safety-assessment-tool/7

[18] UNICEF, "Tools and resources." Accessed: Dec. 03, 2024. [Online]. Available: www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/tools-and-resources

[19] UNICEF, "RITEC Design Toolbox." Accessed: Jan. 23, 2026. [Online]. Available: www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/online-gaming/ritec-design-toolbox

[20] 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. [Online]. Available: www.unicef.org/innocenti/media/4186/file/DH-Philippines-Report-2022.pdf

[21] Republic of the Philippines, *Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act*. 2022. [Online]. Available: https://lawphil.net/statutes/repacts/ra2022/ra_11930_2022.html

[22] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in South Africa: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence Against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4156/file/DH-South-Africa-Report-2022.pdf

[23] European Union, *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of*

children and child pornography, and replacing Council Framework Decision 2004/68/JHA, vol. 335, 2011. Accessed: Nov. 02, 2025. [Online]. Available: http://data.europa.eu/eli/dir/2011/93/oj

[24] E. Ilbiz and C. Kaunert, "Crowdsourcing to tackle online child sexual exploitation: Europol's 'Stop Child Abuse—Trace an Object' platform," *Policing: A Journal of Policy and Practice*, vol. 17, 2023.

[25] INTERPOL, "International Child Sexual Exploitation database." Accessed: Nov. 02, 2025. [Online]. Available: www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

[26] National Center for Missing & Exploited Children, *CyberTipline Report*. 2024. Accessed: Nov. 02, 2025. [Online]. Available: www.missingkids.org/content/ncmec/en/gethelpnow/cybertipline/cybertiplinedata.html

[27] Internet Watch Foundation, "About us." Accessed: Nov. 02, 2025. [Online]. Available: www.iwf.org.uk/about-us

[28] E. Martelozzo and J. DeMarco, "Exploring the removal of online child sexual abuse material in the UK: Processes and practice," *Crime Prevention & Community Safety*, vol. 22, no. 4, pp. 331–350, 2020. [Online]. Available: https://doi.org/10.1057/s41300-020-00099-2

[29] ECPAT, "About us." Accessed: Jan. 23, 2026. [Online]. Available: https://ecpat.org/about-us

[30] ECPAT, "Our history." Accessed: Nov. 02, 2025. [Online]. Available: https://ecpat.org/our-history

[31] ECPAT, *Disrupting Harm*. Accessed: Nov. 02, 2025. [Online]. Available: https://ecpat.org/disrupting-harm

[32] Safe Online, "Who we are." Accessed: Nov. 02, 2025. [Online]. Available: https://safeonline.global/about-us

[33] S. Acosta, T. Garza, H.-Y. Hsu, and P. Goodson, "Assessing quality in systematic literature reviews: A study of novice rater training," *SAGE Open*, vol. 10, no. 3, p. 2158244020939530, July 2020. doi: 10.1177/2158244020939530.

[34] M. J. Grant and A. Booth, "A typology of reviews: an analysis of 14 review types and associated methodologies," *Health Information and Libraries Journal*, vol. 26, no. 2, pp. 91–108, June 2009. doi: 10.1111/j.1471-1842.2009.00848.x.

[35] D. Pollock *et al*., "Recommendations for the extraction, analysis, and presentation of results in scoping reviews," *JBI Evidence Synthesis*, vol. 21, no. 3, pp. 520–532, March 2023. doi: 10.11124/JBIES-22-00123.

[36] S. Singh and V. Nambiar, "Role of artificial intelligence in the prevention of online child sexual abuse: A systematic review of literature," *Journal of Applied Security Research*, vol. 19, no. 4, pp. 586–627, October 2024. doi: 10.1080/19361610.2024.2331885.

[37] S. Page *et al*., "Psychological and emotional harms of online child sexual exploitation and abuse in children under the age of 18: A systematic review of the evidence," *Child Abuse Review*, vol. 34, no. 4, p. e70048, 2025. doi: 10.1002/car.70048.

[38] H. Gholamrezaei, M. R. Falsafinejad, and A. Khodabakhshi-Koolaee, "Exploring the dimensions of online child sexual abuse: A qualitative meta-synthesis study,"

Practice in Clinical Psychology, vol. 12, no. 3, pp. 217–230, July 2024. doi: 10.32598/jpcp.12.3.758.4.

[39] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, March 2021. doi: 10.1136/bmj.n71.

[40] Childlight Global Child Safety Institute, *Search Term Guidance: A Guidebook of Terminology to Use for Literature, Systematic and Scoping Reviews in the Research Area of Child Sexual Exploitation and Abuse*. 2024. [Online]. Available: https://childlight.org

[41] B. N. Levine, M. Liberatore, B. Lynn, and M. Wright, "A forensically sound method of identifying downloaders and uploaders in Freenet," *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, Association for Computing Machinery, New York, USA, pp. 1497–1512, 2020. [Online]. Available: https://doi.org/10.1145/3372297.3417876

[42] M. J. Stathis and M. M. Marinakis, "Shadows into light: The investigative utility of voice analysis with two types of online child-sex predators," *Journal of Child Sexual Abuse*, vol. 31, no. 1, pp. 51–72, 2022. doi: 10.1080/10538712.2019.1697780.

[43] K. Beier, "Preventing child sexual abuse and the use of child abuse images: The Prevention Project *Dunkelfeld* as an international perspective," *The International Journal of Forensic Psychotherapy*, vol. 1, no. 1. pp. 61–66, 2019.

[44] C. Hunn *et al*., "How to implement online warnings to prevent the use of child sexual abuse material," *Trends & Issues in Crime and Criminal Justice*, no. 669, pp. 1–14, 2023. [Online]. Available: https://doi.org/10.52922/ti78894

[45] J. Prichard, R. Wortley, P. Watters, C. Spiranovic, C. Hunn, and T. Krone, "Effects of automated messages on internet users attempting to access 'barely legal' pornography," *Sexual Abuse*, vol. 34, no. 1, pp. 106–124, 2021. [Online]. Available: https://doi.org/10.1177/10790632211013809

[46] P. Fromberger *et al.*, "@myTabu—A placebo controlled randomized trial of a guided web-based intervention for individuals who sexually abused children and individuals who consumed child sexual exploitation material: A clinical study protocol," *Frontiers in Psychiatry*, vol. 11, 2021. [Online]. Available: https://doi.org/10.3389/fpsyt.2020.575464

[47] C. Henry, "Designing effective digital advertisements to prevent online consumption of child sexual exploitation material," *Journal of Child Sexual Abuse*, vol. 29, no. 8, pp. 877–899, 2020. doi: 10.1080/10538712.2020.1841354.

[48] J. Prichard, R. Wortley, P. Watters, C. Spiranovic, and J. Scanlan, "The effect of therapeutic and deterrent messages on internet users attempting to access 'barely legal' pornography," *Child Abuse & Neglect*, vol. 155, pp. 106955–106955, 2024. [Online]. Available: https://doi.org/10.1016/j.chiabu.2024.106955

[49] J. R. Rimer, "Discipline as prevention: Psychoeducational strategies in internet sexual offending group programs," *International Journal of Offender Therapy and Comparative Criminology*, vol. 65, no. 15, pp. 1607–1628, 2021. https://doi.org/10.1177/0306624X20952389

[50] S. Haginoya, T. Ibe, S. Yamamoto, N. Yoshimoto, H. Mizushi, and P. Santtila, "AI avatar tells you what happened: The first test of using AI-operated children in simulated interviews to train investigative interviewers," *Frontiers in Psychology*, vol. 14, 2023. [Online]. Available: https://doi.org/10.3389/fpsyg.2023.1133621

[51] D. Wilkinson, E. Hanley, and B. P. Knijnenburg, "A comparative analysis of legislative protections for online safety in the Global South: A case study of the Caribbean," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. 362, pp. 1–29, 2024. [Online]. Available: https://doi.org/10.1145/3686901

[52] C. Bernasconi, "I rischi insiti nell'utilizzo del Web come possibile strumento di sfruttamento sessuale dei minori: l'attuazione in Italia della Convenzione di Lanzarote e il potenziamento degli strumenti repressive" ["The risks inherent in using the Web as a potential tool for the sexual exploitation of minors: The implementation of the Lanzarote Convention in Italy and the strengthening of repressive instruments"], *Annali online della Didattica e della Formazione Docente*, vol. 9, no. 13, pp. 59–71, 2017.

[53] B. Netkova and A. Q. Mustafa, "International legal standards in combating child online sexual abuse and exploitation," *Journal of Liberty and International Affairs Institute for Research and European Studies*, vol. 6, no. 3, pp. 111–122, 2021. [Online]. Available: https://doi.org/10.47305/jlia2163111n

[54] R. Kaushal, J. Van De Kerkhof, C. Goanta, G. Spanakis, and A. Iamnitchi, "Automated transparency: A legal and empirical analysis of the Digital Services Act Transparency Database," *FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, pp. 1121–1132, 2024. [Online]. Available: https://doi.org/10.1145/3630106.3658960

[55] G. Lisanawati, "What can IT and Money Laundering Law do to fight against cyber child sexual crime?," *Journal of Social and Development Sciences*, vol. 6, no. 2, pp. 67–75, 2015. doi: 10.22610/jsds.v6i2.844.

[56] A. Trujillo, T. Fagni, and S. Cresci, "The DSA Transparency Database: Auditing self-reported moderation actions by social media," *Proceedings of the ACM on Human-Computer Interaction*, vol. 9, no. 2, pp. 1–28, 2025. [Online]. Available: https://doi.org/10.1145/3711085

[57] M. Švec, A. Madleňák, V. Hladiková,, and P. Mészáros, "Slovak mimicry of online content moderation on digital platforms as a result of the adoption of the European Digital Services Act," *Media Literacy and Academic Research*, vol. 7, no. 2, 2024. [Online]. Available: https://doi.org/10.34135/mlar-24-02-26

[58] D. Dushi, "Does the end justify the means? The European Commission's proposed regulation laying down rules to prevent and combat child sexual abuse," *International Journal of Law and Information Technology*, vol. 32, no. 1, eaae027, 2024. [Online]. Available: https://doi.org/10.1093/ijlit/eaae027

[59] N. Munns *et al.*, *Facilitation of Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines: Analysis and Recommendations for Better Detection, Deterrence and Prevention*. London: Justice and Care, 2024. [Online]. Available: https://justiceandcare.org/app/uploads/2024/04/Facilitation-of-Online-Sexual-Abuse-and-Exploitation-of-Children-OSAEC-in-the-Philippines-FR-FINALpdf.pdf

[60] V. M. Ngo, R. Gajula, C. Thorpe, and S. McKeever, "Discovering child sexual abuse material creators' behaviors and preferences on the dark web," *Child Abuse & Neglect*, vol. 147, p. 106558, 2024. [Online]. Available: https://doi.org/10.1016/j.chiabu.2023.106558

[61] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Viet Nam: Evidence on Online Child Sexual Exploitation and Abuse.* Global Partnership to End Violence Against

Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4181/file/DH-Viet-Nam-Report-2022.pdf

[62] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Uganda: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence Against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4126/file/DH-Uganda-Report-2022.pdf

[63] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Thailand: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4151/file/DH-Thailand-Report-2022.pdf

[64] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Tanzania: Evidence on Online Child Sexual Exploitation and Abuse.* Global Partnership to End Violence Against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4131/file/DH-Tanzania-Report-2022.pdf

[65] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Malaysia: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence Against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4146/file/DH-Malaysia-Report-2022.pdf

[66] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Kenya: Evidence on Online Child Sexual Exploitation and Abuse.* Global Partnership to End Violence against Children, 2021. [Online]. Available: www.unicef.org/innocenti/media/4111/file/DH-Kenya-Report-Nov-2022.pdf

[67] ECPAT, INTERPOL, and UNICEF, *Disrupting Harm in Ethiopia: Evidence on Online Child Sexual Exploitation and Abuse*. Global Partnership to End Violence against Children, 2022. [Online]. Available: www.unicef.org/innocenti/media/4121/file/DH-Ethiopia-Report-2022.pdf

[68] E. Bursztein *et al*., "Rethinking the detection of child sexual abuse imagery on the internet," *WWW '19, The World Wide Web Conference*, Association for Computing Machinery, New York, USA, pp. 2601–2607, 2019. [Online]. Available: https://doi.org/10.1145/3308558.3313482

[69] J. De Geest *et al*., "Perceptual hashing using pretrained vision transformers," *2024 IEEE Gaming, Entertainment, and Media Conference, GEM 2024*, pp. 19–24, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10585453

[70] P. Borj and P. Bours, "Predatory conversation detection," *2019 International Conference on Cyber Security for Emerging Technologies (CSET)*, vol. 30. pp. 1–6, 2019. doi: 10.1109/CSET.2019.8904885.

[71] D. Cook, M. Zilka, H. DeSandre, S. Giles, S. Maskell, and ACM, "Protecting children from online exploitation: Can a trained model detect harmful communication strategies?," *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society, AIES 2023*, pp. 5–14, 2023. doi: 10.1145/3600211.3604696.

[72] J. Rodríguez, S. Durán, D. López, J. Pastor-Galindo, and F. Mármol, "C3-Sex: A conversational agent to detect online sex offenders," *Electronics*, vol. 9, no. 11, pp. 1779–1779, 2020.

[73] K. C. Seigfried-Spellar, M. K. Rogers, J. T. Rayz, S. F. Yang, K. Misra, and T. Ringenberg, "Chat Analysis Triage Tool: Differentiating contact-driven vs. fantasy-

driven child sex offenders," *Forensic Science International*, vol. 297, pp. E8–E10, 2019. doi: 10.1016/j.forsciint.2019.02.028.

[74] X. Li *et al*., "SafeGen: Mitigating sexually explicit content generation in text-to-image models," *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, Association for Computing Machinery, New York, USA, pp. 4807–4821, 2024. [Online]. Available: https://doi.org/10.1145/3658644.3670295

[75] T. Coelho, L. S. F. Ribeiro, J. Macedo, J. A. dos Santos, and S. Avila, "Minimizing risk through minimizing model-data interaction: A protocol for relying on proxy tasks when designing child sexual abuse imagery detection models," *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, Association for Computing Machinery, New York, USA, pp. 1543–1553, 2025. [Online]. Available: https://doi.org/10.1145/3715275.3732102

[76] W. Gutfeter, J. Gajewska, and A. Pacut, "Detecting sexually explicit content in the context of the child sexual abuse materials (CSAM): End-to-end classifiers and region-based networks," *Machine Learning and Principles and Practice of Knowledge Discovery in Databases*, 2025. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-74627-7_11

[77] P. Lakkur, M. Iyyer, and B. N. Levine, "Triage of messages and conversations in a large-scale child victimization corpus," *WWW '24, Proceedings of the ACM Web Conference 2024*, pp. 4544–4554, 2024. [Online]. Available: https://doi.org/10.1145/3589334.3648142

[78] P. H. V. Valois, J. Macedo, L. S. F. Ribeiro, J. A. dos Santos, and S. Avila, "Leveraging self-supervised learning for scene classification in child sexual abuse imagery," *Forensic Science International: Digital Investigation*, vol. 53, p. 301918, 2025.

[79] C. da Silva, J. Macedo, S. Avila, and J. Dos Santos, "Seeing without looking: Analysis pipeline for child sexual abuse datasets," *2022 ACM Conference on Fairness, Accountability, and Transparency*, pp. 2189–2205, 2022. [Online]. Available: https://doi.org/10.1145/3531146.3534636

[80] M. Salter and L. Richardson, "The Trichan takedown: Lessons in the governance and regulation of child sexual abuse material," *Policy and Internet*, vol. 13, no. 3, pp. 385–399, 2021. doi: 10.1002/poi3.256.

[81] B. B. Westlake and E. Guerra, "Using file and folder naming and structuring to improve automated detection of child sexual abuse images on the Dark Web," *Forensic Science International: Digital Investigation*, vol. 47, p. 301620, 2023. [Online]. Available: https://doi.org/10.1016/j.fsidi.2023.301620

[82] M. Steinebach, "An analysis of PhotoDNA," *Proceedings of the 18th International Conference on Availability, Reliability and Security*, no. 44, pp. 1–8, 2023. [Online]. Available: https://doi.org/10.1145/3600160.3605048

[83] P. Samanta and S. Jain, "SmartHash: Perceptual hashing for image tampering detection and authentication," *CIKM '24: Proceedings of the 33rd ACM Conference on Information and Knowledge Management*, pp. 1983–1993, 2024. [Online]. Available: https://doi.org/10.1145/3627673.3679827

[84] J. Yoon, A. X. Zhang, and J. Seering, "'It's great because it's ran by us': Empowering teen volunteer Discord moderators to design healthy and engaging youth-led online communities," *Proceedings of the ACM on Human-Computer Interaction*, vol. 9, no. 2, pp. 1–30, 2025. [Online]. Available: https://doi.org/10.1145/3711114

[85] O. Cullen, K. Z. Ernst, N. Dawes, W. Binford, and G. Dimitropoulos, "'Our laws have not caught up with the technology': Understanding challenges and facilitators in investigating and prosecuting child sexual abuse materials in the United States," *Laws*, vol. 9, no. 4, 2020. doi: 1 0.3390/laws9040028.

[86] E. Ferguson and C. Wilkinson, "Juvenile age estimation from facial images," *Science & Justice*, vol. 57, no. 1, pp. 58–62, 2017. [Online]. Available: https://doi.org/10.1016/j.scijus.2016.08.005

[87] E. Martelozzo, "Policing online child sexual abuse: The British experience," *European Journal of Policing Studies*, vol. 3, no. 1. p. 32, 2015. doi: 10.5553/EJPS/2034760X2015003001003.

[88] J. A. Kloess, J. Woodhams, and C. E. Hamilton-Giachritsis, "The challenges of identifying and classifying child sexual exploitation material: Moving towards a more ecologically valid pilot study with digital forensics analysts," *Child Abuse & Neglect*, vol. 118, p. 105166, 2021. doi: 10.1016/j.chiabu.2021.105166.

[89] H. L. Merdian *et al*., "Secondary prevention of the use of online child sexual exploitation material: An initial overview of international efforts," *Forensische Psychiatrie Psychologie Kriminologie*, vol. 17, no. 4, pp. 377–388, 2023. doi: 10.1007/s11757-023-00796-2.

[90] L. Kiss, A. Iuliano, A. P. Portella, H. Paiva, M. Pires, and B. Leurent, "Growing up without violence (GWV): Study protocol for a cluster randomised trial and process evaluation of a school-based intervention preventing adolescent sexual exploitation in Brazil," *Contemporary Clinical Trials*, vol. 150, 2025. doi: 10.1016/j.cct.2024.107802.

[91] E. J. Reeves *et al*., "May and Bay: Online child sexual exploitation and abuse in Southeast Asia—Using digital games in preventative education," *Journal of Human Rights and Social Work*, vol. 9, no. 4, pp. 615–629, 2024. doi: 10.1007/s41134-024-00314-2.

[92] D. Lindenbach *et al*., "Capacity, confidence and training of Canadian educators and school staff to recognize and respond to sexual abuse and internet exploitation of their students," *Child Abuse & Neglect*, vol. 112, p. 104898, 2021. [Online]. Available: https://doi.org/10.1016/j.chiabu.2020.104898

[93] S. Kantipudi and M. Chuemchit, "Teach to say 'NO'—A mixed methods evaluation of a child sexual abuse prevention training for primary school teachers in Phnom Penh, Cambodia," *Child Abuse & Neglect*, vol. 158, 2024. doi: 10.1016/j.chiabu.2024.107097

[94] E. Celiksoy and K. Schwarz, *Investigation into Financial Transactions Used in the Online Sexual Exploitation of Children: The State of Evidence*, Nottingham: University of Nottingham Rights Lab, 2023. [Online]. Available: www.nottingham.ac.uk/research/beacons-of-excellence/rights-lab/resources/reports-and-briefings/2023/october/investigation-into-financial-transactions-used-in-the-online-sexual-exploitation-of-children.pdf

[95] A. Hendrick, A. Jupit, and A. Nordin, "Empowering youth through play: Promoting awareness of sexual grooming among schoolchildren through game-based learning," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 51, no. 2. pp. 34–44, 2024. [Online]. Available: https://semarakilmu.com.my/journals/index.php/appl...

[96] N. Bennett and W. O'Donohue, "Identifying grooming of children for sexual abuse: Gender effects and increased false positives from internet information," *International Journal of Psychology and Psychological Therapy*, vol. 20, no. 2, pp. 133–145, 2020.

[97] J. L. McCain, J. H. Herbst, M. Merrill-Francis, L. A. Willis, S. S. Miedema, and J. W. Shortt, "Review of policies and practices to prevent technology-facilitated child sexual abuse within youth-serving organizations in the United States," *Journal of Child Sexual Abuse*, vol. 33, no. 5, pp. 545–564, 2024. doi: 10.1080/10538712.2024.2381457.

[98] E. Newman *et al*., "The impact of a public health campaign to deter viewing of child sexual abuse images online: A case study of the UK Stop It Now! campaign," *Sexual Abuse*, vol. 36, no. 6, pp. 635–661, 2023. [Online]. Available: https://doi.org/10.1177/10790632231205784

[99] J. Häikiö and V. Uusoksa, "644 new and innovative ways to tackle child sexual abuse—www.otanvastuun.fi," *Injury Prevention*, vol. 22, Suppl. 2, pp. A231.3–A231, 2016. doi: 10.1136/injuryprev-2016-042156.644.

[100] H. L. Merdian, H. K. Bradshaw, and D. Perkins, "Circles ReBoot: A feasibility study and preliminary outcome evaluation," *International Journal of Offender Therapy and Comparative Criminology*, 2025. doi: 10.1177/0306624X251334907.

[101] N. Walker, N. Bell, and D. Woodlock, "Rolling out the red carpet: Non-offending partners and affected family members as allies in disruption," *Child Abuse & Neglect*, vol. 157, p. 106995, 2024. doi: 10.1016/j.chiabu.2024.106995.

[102] B. Kardos, "Beyond the consent paradigm: Problematizing representations of AI-generated pornography in the education discourse of the UN," *Policy Futures in Education*, vol. 23, no. 5, pp. 1021–1039, 2025. [Online]. Available: https://doi.org/10.1177/14782103251321045

[103] L. Popa, "National and international cooperation in investigating crimes of child sexual abuse or sexual exploitation committed by using information technologies," *AGORA International Journal of Juridical Sciences*, vol. 18, no. 1. pp. 102–111, 2024.

[104] N. Zubaidi, "Monitoring internet child pornography (ICP) in Malaysia," *Pertanika Journal of Social Science & Humanities*, vol. 29, 2021. [Online]. Available: https://doi.org/10.47836/pjssh.29.s2.13

[105] D. Tselenti *et al*., "Policing child sexual exploitation and abuse cases: A qualitative PRIORITY study of the challenges faced by law enforcement officers in Germany, Portugal, and Sweden," *Policing & Society*, vol. 35, no. 7, pp. 983–1000, 2025. [Online]. Available: https://doi.org/10.1080/10439463.2024.2447842

[106] H. Farid, "An overview of perceptual hashing," *Journal of Online Trust and Safety*, vol. 1, no. 1, 2021. [Online]. Available: https://doi.org/10.54501/jots.v1i1.24

[107] A. El-Asam, A. Katz, C. Street, N. M. Nazar, and M. Livanou, "Children's services for the digital age: A qualitative study into current procedures and online risks among service users," *Children and Youth Services Review*, vol. 122, p. 105872, 2021. [Online]. Available: https://doi.org/10.1016/j.childyouth.2020.105872

[108] P. Fussey and A. Sandhu, "Surveillance arbitration in the era of digital policing," *Theoretical Criminology*, vol. 26, no. 1, pp. 3–22, 2022. [Online]. Available: https://doi.org/10.1177/1362480620967020

[109] B. Leclerc, J. Cale, T. Holt, and J. Drew, "Child sexual abuse material online: The perspective of online investigators on training and support," *Policing: A Journal of Policy and Practice*, vol. 16, no. 4, pp. 762–776, 2022. [Online]. Available: https://doi.org/10.1093/police/paac017

[110] L. A. Steedman and E. L. Jeglic, "Child sexual abuse prevention among a sample of US parents," *Journal of Child and Family Studies*, vol. 34, no. 4, pp. 1099–1113, 2025. [Online]. Available: https://doi.org/10.1007/s10826-025-03036-9

[111] E. Deldari, P. Thakkar, and Y. Yao, "Users' perceptions of online child abuse detection mechanisms," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. 147, pp. 1–26, 2024. [Online]. Available: https://doi.org/10.1145/3637424

[112] R. Allsup, E. Thomas, B. Monk, R. Frank, and M. Bouchard, "Networking in child exploitation: Assessing disruption strategies using registrant information," *ASONAM '15: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015*, pp. 400–407, 2015. [Online]. Available: https://doi.org/10.1145/2808797.2809297

[113] R. Pfefferkorn, "Content-oblivious trust and safety techniques: Results from a survey of online service providers," *Journal of Online Trust and Safety*, 2021. [Online]. Available: https://doi.org/10.54501/jots.v1i2.14

[114] M. Y. Lu, M. Lamond, and D. Fry, "A content analysis of metrics on online child sexual exploitation and abuse used by online content-sharing services," *Child Abuse & Neglect*, vol. 157, p. 107046, 2024. [Online]. Available: https://doi.org/10.1016/j.chiabu.2024.107046

[115] D. Thakur and R. Gorwa, *Real Time Threats: CSEA Prevention on Livestreaming Platforms*. Center for Democracy & Technology, November 2024. [Online]. Available: https://cdt.org/insights/real-time-threats-analysis-of-trust-and-safety-practices-for-child-sexual-exploitation-and-abuse-csea-prevention-on-livestreaming-platforms

[116] M. Santopietro, R. Guest, K. C. Seigfried-Spellar, and S. J. Elliott, "A multi-factor knuckle and nail bed verification tool for forensic imagery analysis," *Child Abuse & Neglect*, vol. 154, p. 106910, 2024. doi: 10.1016/j.chiabu.2024.106910.

[117] A. Razi *et al.*, "Sliding into my DMs: Detecting uncomfortable or unsafe sexual risk experiences within Instagram direct messages grounded in the perspective of youth," *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. 89, pp. 1–29, 2023. [Online]. Available: https://doi.org/10.1145/3579522

[118] Statute Law Database, *Online Safety Act 2023 (UK)*. Accessed: Nov. 07, 2025. [Online]. Available: www.legislation.gov.uk/ukpga/2023/50

[119] *Online Safety Act 2021 (Australia)*. Accessed: Nov. 07, 2025. [Online]. Available: https://classic.austlii.edu.au/au/legis/cth/consol_act/osa2021154

[120] European Union, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)*, vol. 277, 2022. Accessed: Nov. 07, 2025. [Online]. Available: http://data.europa.eu/eli/reg/2022/2065/oj

[121] E. M. Chiang, "'Send me some pics': Performing the offender identity in online undercover child abuse investigations," *Policing: A Journal of Policy and Practice*,

vol. 15, no. 2, pp. 1173–1187, 2021. [Online]. Available: https://doi.org/10.1093/police/paaa065.

[122] J. E. Reid, "The Computerized Voice Stress Analyzer (CVSA)." Accessed: Dec. 01, 2025. [Online]. Available: https://reid.com/resources/investigator-tips/the-computerized-voice-stress-analyzer-cvsa.

[123] J. Lätth *et al*., "Effects of internet-delivered cognitive behavioral therapy on use of child sexual abuse material: A randomized placebo-controlled trial on the Darknet," *Internet Interventions: The Application of Information Technology in Mental and Behavioural Health*, vol. 30, p. 100590, 2022. doi: 10.1016/j.invent.2022.100590.

[124] D. Kristiningsih and I. Kasuma, "Settlement of online child sexual exploitation cases in Indonesia (Cases study: Facebook group 'Club Brondong Puncak' and 'Official Candy's Group')," *PEOPLE International Journal of Social Sciences*, vol. 4, no. 3, pp. 482–495, 2018. doi: 10.20319/pijss.2018.43.482495.

[125] D. L. Midani, A. Deliege, P. Burton, and J. Amo-Adjei, "The legal, policy, institutional and programmatic context for protecting children against online sexual exploitation in Tunisia," *Children & Society*, vol. 39, no. 1, pp. 74–93, 2025. doi: 10.1111/chso.12895.

[126] L. Struppek, D. Hintersdorf, D. Neider, and K. Kersting, "Learning to break deep perceptual hashing: The use case NeuralHash," *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency,* pp. 58–69, 2022. [Online]. Available: https://doi.org/10.1145/3531146.3533073

[127] R. Sakpal and N. Jain, "Revenge pornography matching using computer vision," *2023 6th International Conference on Information and Communications Technology (ICOIACT)*, pp. 407–412, 2023. doi: 10.1109/ICOIACT59844.2023.10455933.

[128] A. Lindholm, O. Rantatalo, O. Lindberg, and R. Lundmark, "The investigation of online child sexual abuse cases in Sweden," *Nordic Journal of Studies in Policing*, vol. 11, no. 1, pp. 1–15, 2024. doi: 10.18261/njsp.11.1.7.

[129] É. Gauvin, N. Deslauriers-Varin, M. Noc, F. Fortin, and S. Paquette, "Question types in online sex offender interviews: Unveiling the influence on information retrieval," *Journal of Criminal Psychology*, 16 May, 2025. [Online]. Available: https://doi.org/10.1108/jcp-12-2024-0127

[130] T. R. Ringenberg, K. C. Seigfried-Spellar, and J. Rayz, "Are you a cop? Identifying suspicion in online chat operations with online groomers," *Child Abuse & Neglect*, vol. 154, pp. 1–12, 2024. [Online]. Available: https://doi.org/10.1016/j.chiabu.2024.106919

[131] A. Hayes, "Understanding peer-to-peer (P2P) services: Key facts, and examples," Investopedia. Accessed: Dec. 01, 2025. [Online]. Available: www.investopedia.com/terms/p/peertopeer-p2p-service.asp

[132] D. Thiel, *Identifying and Eliminating CSAM in Generative ML Training Data and Models*. Stanford, CA: Stanford Internet Observatory Cyber Policy Center, 2023. [Online]. Available: https://stacks.stanford.edu/file/kh752sm9123/ml_training_data_csam_report-2023-12-23.pdf

[133] S. Gupta, "Child pornography and internet subcultures in India: A legal perspective," *Journal of Law and Sustainable Development*, vol. 12, no. 1, pp. e2997–e2997, 2024.

[134] ICO (Information Commissioner's Office), "UK GDPR Guidance and Resources | Definitions." [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/explaining-decisions-made-with-artificial-intelligence/part-1-the-basics-of-explaining-ai/definitions.
[135] IBM MediaCenter, "What is the Dark Web?" Accessed: Dec. 01, 2025. [Online]. Available: https://mediacenter.ibm.com/media/What+is+the+Dark+Web/1_tytynhg9
[136] IBM, "What is deep learning?" Accessed: Dec. 01, 2025. [Online]. Available: www.ibm.com/think/topics/deep-learning
[137] IBM, "What is machine learning?" Accessed: Dec. 01, 2025. [Online]. Available: www.ibm.com/think/topics/machine-learning
[138] UN (United Nations) Economic and Social Commission for Western Asia, "Supranational organizations." Accessed: Jan. 29, 2026. [Online]. Available: https://archive.unescwa.org/supranational-organizations

ENDNOTE

[1] The "4Cs" of child online risks refers to content, contact, conduct, and contract risks, with the addition of cross-cutting risks that intersect with these four risk categories [8]. Livingstone and Stoilova [8, p. 4] define these risks as follows: content risks refer to children's engagement or exposure to potentially harmful content; contact risks refer to children's online (unintended or targeted) encounters that lead to inappropriate, risky, harmful, or problematic interactions; conduct risks refer to children's behaviors and actions that expose them to risk, or put themselves or others at risk; and contract risks refer to children being party to, or exploited by, potentially harmful exchanges or contracts.

APPENDICES

Appendix A: Coding Frame and Definitions.

Coding categories	Questions asked	Coding labels (short answers)	Definitions/explanations/ instructions
Publication title	What is the title of the paper, article, or report?	Title, copied from the title of the document being coded	*Copy the title from the paper, article, or report being coded*
Publication date (year)	What is the year of publication?	Year of publication	*Copy the year of publication from the paper, article, or report*
Author(s)	What is the last name of the first author?	First author's last name (add *et al*. if there are more than two authors)	*Copy from the paper, article, or report*
Publication type	Is this an academic paper, journal article or an organization's report?	Publication type as stated in the document	*Copy from the paper, article, or report*
Decision on full-text analysis (Keep or Reject)	Having read the full text, does this paper, article, or report fit the inclusion criteria?	Keep	*Record "Keep" or "Reject"*
		Reject	
Number of interventions discussed	How many separate interventions does the paper, article, or report address?	1, 2, 3, etc.	*Fill in the number of interventions discussed. By "separate intervention" we mean a variety of solutions rather than various phases of the same intervention*
Intervention development	Who developed the intervention?	National government	*Nation states and central government agencies that make decisions for and govern a country, including providing public services*
		Local government	*Provincial, county, or district administrations*
		International organizations (add organization name, e.g., UNICEF)	*Entities established by a treaty or other international legal instruments endorsed by two or more states or organizations formed to address global issues through collaborations of various national governments*
		Supranational organization (e.g., European Union)	*An international organization whereby member states transcend national boundaries or interests to share in decision-making and vote on issues affecting the wider grouping* [138]

		Nongovernmental organizations (NGOs) (add organization name, e.g., Safe Online)	*A non-profit group, independent of government control*
		Parents	*Father, mother or another primary caregiver for the child*
		Schools	*An educational institution for children*
		Tech companies	*Companies that develop and/or provide digital products or services, including platforms, such as Facebook and Google*
		Law enforcement agencies (LEAs)	*A government agency responsible for enforcing the law*
		Academics	*Scholars working in higher-education institutes or research institutes*
		No distinct development phase or developers	*The paper, article, or report focuses on existing practices, processes, laws, or regulations*
		Other (add your own description)	*Any types of organizations or entities not included in the list*
		Information not available	*The paper, article, or report did not include this information*
Intervention implementation	Who carried out the intervention? Type in the relevant answer, choosing all applicable answers from the following options	National government	*Nation states and central government agencies that make decisions for and govern a country, including providing public services*
		Local government	*Provincial, county, or district administrations*
		International organizations (add organization name, e.g., UNICEF)	*Entities established by a treaty or other international legal instruments endorsed by two or more states or organizations formed to address global issues through collaborations of various national governments*
		Supranational legislative body (e.g., European Union)	*An international organization whereby member states transcend national boundaries or interests to share in decision-making and vote on issues affecting the wider grouping* [138]
		NGOs (add organization name e.g., Safe Online)	*A non-profit group, independent of government control*
		Parents	*Father, mother or another primary caregiver for the child*

		Schools	*An educational institution for children*
		Tech companies	*Companies that develop and/or provide digital products or services, including platforms, such as Facebook and Google*
		Legal professionals	*Lawyers, para-legals, judges, attorneys general*
		Law enforcement	*A government agency responsible for enforcing the law*
		Academics	*Scholars working in higher-education institutes or research institutes*
		Other (add your own description)	*Any types of organizations or entities not included in the list*
		Information not available	*The paper, article, or report did not include this information*
Problem statement	Why is the intervention needed?	Copy relevant texts from the literature	*This coding category identifies the problem statement to which the intervention responds, as described in the literature coded*
Funding	Who funds the research, development, or intervention?	Name(s) of funding organization(s)	*Type in the name of the funding organization as stated in the document*
		No funding	*If there is no funding, say "No funding"*
		No information available	*If there is no information about funding, type "No information available"*
Types of intervention	In which category does this intervention fit?	Education, literacy, or awareness-raising campaign	*Learning modules, courses, or training, or programs aimed at raising public awareness, or educating the public, particular populations, or professions about tech-facilitated CSEA*
		Technological tools and protocols	*The development, deployment, and use of digital technologies by commercial companies, academics, governments, NGOs, or LEAs to detect, deter, and curb tech-facilitated CSEA, including removal of CSAM and impeding digital money transfers for tech-facilitated CSEA*
		Policy intervention	*Company or government policies for combating tech-facilitated CSEA*

		Financial intervention	*Financial mechanisms to detect and block payments for tech-facilitated CSEA*
		Policing and investigation	*LEA efforts to police, investigate, arrest, and prosecute those involved in TF-CSEA*
		Legal and regulatory intervention	*National or international laws aimed at curbing tech-facilitated CSEA*
		Behavioral intervention	*Interventions aimed at changing the behaviors of people who are the subjects of intervention, such as perpetrators, children, parents, teachers, or healthcare professionals, to prevent tech-facilitated CSEA*
		Hybrid approach	*A combination of various interventions*
		Other (add your own description)	*Any interventions not listed*
Scale of the intervention implementation (as stated in the documents)	How would you describe the size of the affected population or content (e.g., CSAM) primarily addressed by this intervention?	Community	*Interventions aimed at making changes at community level to prevent, detect, and address tech-facilitated CSEA*
		School	*Interventions implemented in schools for education professionals and/or children to prevent, detect, and address tech-facilitated CSEA*
		State(s)	*Interventions implemented across one or more states (mostly in the USA)*
		District	*Interventions aimed at making changes at a district level to prevent, detect, and address tech-facilitated CSEA*
		Nationwide	*Interventions that are implemented nationwide*
		Regional	*Interventions that are implemented across various countries within the same region (e.g., ASEAN or Asia Pacific [APAC])*
		Global	*Interventions that are implemented globally across various countries across different continents*
		Surface or dark web networks	*Technological tools and protocols applied at network level, either on the surface (the open internet) or on the dark web*

		An online platform	*Technical (e.g., user privacy control function or content moderation system) or policy (e.g., Discord's teen and child safety policy) solutions applied at (digital) platform level*
		Other (add your own description)	*Any other scales of intervention not listed*
		Unstated	*The paper, article, or report does not give any indication of the scale of possible intervention impact*
Intervention operation	How does this intervention operate?	Online (at a system level)	*Technological tools and protocols that target operating systems (e.g., Windows, macOS, iOS) or devices, e.g., a client side detection mechanism or client side scanning*
		Online (at a network level)	*Technological tools and protocols that filter and/or investigate data packets as they travel through the networks or their routing direction*
		Online (at a platform or browser level or as a standalone application)	*Technological tools and protocols that operate as a standalone application on specific platforms or environments, e.g., a content moderation system or an application for teaching and learning*
		Offline (single agency operation)	*Any interventions applied in a physical environment, carried out by one agency*
		Offline (multi-agency collaboration)	*Any interventions applied in a physical environment, carried out in collaboration across various agencies*
		Hybrid (online and offline)	*A combination of online and offline interventions*
		Other (add your own description)	*Any other interventions not listed*
Geographic location of the intervention	If the intervention is in a physical environment, in which country or region does it take place?	Country and/or region name(s)	*Type in the country name or the region, as shown in the document*
		Not applicable (N/A)	*If the intervention is online, type "N/A" for "Not applicable"*
Intervention targets	Who or what is the target of the intervention? Who does the intervention aim to enable or support?	Perpetrators or potential perpetrators	*People who are involved in tech-facilitated CSEA offending (e.g., convicted offenders) or are at risk of offending*
		Children	*Anyone aged between 0 and 17 (under 18)*

		Law enforcement agencies (LEAs)	*State agencies responsible for enforcing the law*
		Government agencies	*Organizations that form part of the government machinery*
		Healthcare professionals	*Professionals providing health and social care services (e.g., doctors, nurses, social workers)*
		Teachers	*Including school staff and school safeguarding officers*
		Legal professionals	*Lawyers, para-legals, judges, attorneys general, prosecutors*
		Parents	*Father, mother, or another caregiver for the child*
		Laws and regulations	*Legally binding rules which a particular country or region (e.g., European Union) recognizes as regulating the actions of its members, enforceable through imposing penalties*
		Policies	*The establishment of objectives, values, and interests that set the agenda and shape the structure and behaviors of relevant stakeholders within a particular system, such as digital platforms*
		CSAMs	*Sexually explicit images or videos of a child being sexually abused, raped, molested, or exploited*
		Other (add your own description)	*Any other targets not listed here*
Intervention objectives	What is the primary objective of the intervention?	Making policing and investigation more effective	*To make law enforcement agency detection, deterrence, and investigation of tech-facilitated CSEA more effective*
		Making laws, policies, and regulations fit-for purpose for tech-facilitated CSEA	*To improve the fitness for purpose of existing polices, laws, and regulations, or the creation of new policies, laws, and regulations to curb tech-facilitated CSEA*
		Making the judiciary system more effective	*To enable victims to gain access to the justice system, be provided with the necessary adjustment and support services, and be compensated for (i.e., have access to remedies) the damage done to them*

		CSAM or livestreaming detection and analysis	*To detect, investigate, or remove sexually explicit images, videos, or livestreams of a child being sexually abused, raped, molested, or exploited*
		Disrupting payment for CSAM or tech-facilitated CSEA	*To disrupt payment for CSAM or tech-facilitated CSEA*
		Behavioral or attitude change (offenders)	*To change the behavior or attitudes of offenders*
		Behavioral or attitude change (professionals working with children)	*To change the behavior or attitudes of professionals working with children, e.g., teachers or healthcare professionals*
		Behavioral or attitude change (parents)	*To change the behavior or attitudes of parents*
		Behavioral or attitude change (children)	*To change the behavior or attitudes of children*
		Other (add your own description)	*Any other objectives of tech-facilitated CSEA interventions*
Locus of the intervention within the TF-CSEA ecosystem	Which part of the tech-facilitated CSEA offending chain does the intervention target?	Recruitment	*The process of identifying either prospective perpetrators (e.g., local adults who sexually exploit or abuse a child on demand) or children for tech-facilitated CSEA*
		Grooming	*The process of establishing or building a relationship with a child, either in person or using the internet or other digital technologies, to facilitate either online or offline sexual contact with that person*
		Service advertisement	*Announcement of or invitation to use available tech-facilitated CSEA materials or services*
		Payment system	*Channels, both online and offline, through which consumers of tech-facilitated CSEA materials or services pay for their requested products or services*
		CSAM storage and distribution	*Storage and distribution of sexually explicit images or videos of a child being sexually abused, raped, molested, or exploited*

		Promotion of online safety	*Policies, programs, or campaigns aimed at raising awareness and improving online safety, including child online protection*
		Detection and investigation	*Efforts to detect and investigate tech-facilitated CSEA*
		Prosecution	*Provision of support for victims, parents, or legal guardians of the victims to enable victims to access justice and remedies*
		Recidivism	*Convicted offenders re-offending*
		Potential offenders offending	*People at risk of offending committing CSEA offences*
		Other (add your own description)	*Type in your answer*
Intervention appraisal	Is there information about how well this intervention works?	1	*Yes*
		0	*No*
Intervention appraisal: Who?	If "Yes", who carried out the intervention?	1	*Independent third party. Here, academic researchers count as independent third parties*
		0	*Same organization(s) that developed or implemented the intervention*
Intervention appraisal methods	Does the paper, article or report provide information on its appraisal method?	1	*Yes*
		0	*No*
Findings from the appraisal	Does the paper, article, or report provide findings?	1	*Yes*
		0	*No*
Appraisal limitation reporting	Does the paper, article, or report outline its limitations?	1	*Yes*
		0	*No*
Intervention evaluation data collection method	How was the intervention appraised or assessed? Using what methods?	Interviews	*One-to-one conversations to obtain information in a research context (not as part of a policing investigation)*
		Focus group	*A group conversation to obtain information in a research context (not as part of policing)*
		Survey	*A systematic way of collecting information from a sample of the population by asking them questions to understand their*

			characteristics, preferences, opinions, or beliefs
		Mixed methods	*A research approach that combines the collection of quantitative and qualitative data to gain a deeper and more complete understanding of a research problem*
		Automated web crawler	*A software program (bot), typically operated by search engines, that systematically browses the surface web for web indexing*
		Observational studies or ethnography	*A research method that involves observing research subjects without intervening or manipulating any variables to understand the research subjects' natural behaviors, risk factors, etc.*
		Randomized controlled trial (RCT)	*A gold standard research method for testing the effectiveness of an intervention by randomly assigning participants to an intervention group, or a control group that receives a different intervention, or no intervention in order to establish causal links between the intervention and the outcomes*
		Anecdotal records	*Factual accounts of an occurrence, behavior, action, or event observed by the researcher*
		Controlled experiments or experimental design	*A research methodology to establish a causal link between a variable and an outcome, focusing on one independent variable change to observe its effect on another variable, or experimentation with a solution, or variation of a solution to establish the level of performance of the solution(s) being tested*
		Other (add your own description)	*Other data collection methods not listed*
Intervention evaluation analytical method	What is the data analysis method?	Content or text analysis	*A method for systematically identifying themes and patterns from recorded communications in various forms including texts, images, and audio and video clips, to make sense of these records*

		Other qualitative analysis	*Any other qualitative approaches to make sense of data*
		Descriptive statistical analysis	*A quantitative method for summarizing and presenting basic characteristics of data*
		Multivariate analysis	*A statistical method for interpreting and quantifying relationships between a dependent variable and one or more independent variables*
		Other quantitative analysis	*Any other quantitative methods not listed*
		Computer forensics analysis	*Specialized computing techniques used to investigate and report on digital evidence found on electronic devices, networks, and the cloud environment in support of legal proceedings, investigations, and cybersecurity incident responses*
		Other (add your own description)	*Any other analytical methods not listed here*
Description of the results (authors' statements)	How do the authors describe the results of their evaluation of the intervention?	Copy relevant texts from the literature	*Copy relevant texts from the literature*
Description of the results (coders' summary)	How would you summarize the author(s)' appraisal results?	Free text	*Type in your summary*
Authors' stated limitations	What are the authors' stated limitation(s)?	Copy relevant texts from the literature	*Copy relevant texts from the literature*

Appendix B: List of Included Peer-Reviewed Publications.

Author(s)	Year	Publication title
Allsup *et al.*	2015	Networking in child exploitation: Assessing disruption strategies using registrant information
Beier	2019	Preventing child sexual abuse and the use of child abuse images: The Prevention Project *Dunkelfeld* as an international perspective
Bennett and Donohue	2020	Identifying grooming of children for sexual abuse: Gender effects and increased false positives from internet information

Bernasconi	2017	The risks inherent in using the Web as a potential tool for the sexual exploitation of minors: The implementation of the Lanzarote Convention in Italy and the strengthening of repressive instruments
Borj and Bours	2019	Predatory conversation detection
Bursztein *et al.*	2019	Rethinking the detection of child sexual abuse imagery on the internet
Chiang	2021	'Send me some pics': Performing the offender identity in online undercover child abuse investigations
Choi *et al*.	2024	Digital shadows: Analyzing factors influencing sentencing in child sexual abuse material (CSAM) cases
Coelho *et al.*	2025	Minimizing risk through minimizing model-data interaction: A protocol for relying on proxy tasks when designing child sexual abuse imagery detection models
Cook *et al.*	2023	Protecting children from online exploitation: Can a trained model detect harmful communication strategies?
Cullen *et al.*	2020	'Our laws have not caught up with the technology': Understanding challenges and facilitators in investigating and prosecuting child sexual abuse materials in the United States
da Silva *et al.*	2022	Seeing without looking: Analysis pipeline for child sexual abuse datasets
De Geest *et al.*	2024	Perceptual hashing using pretrained vision transformers
Deldari *et al.*	2024	Users' perceptions of online child abuse detection mechanisms
Dushi	2024	Does the end justify the means? The European Commission's proposed regulation laying down rules to prevent and combat child sexual abuse
El-Asam *et al.*	2021	Children's services for the digital age: A qualitative study into current procedures and online risks among service users
Farid	2021	An overview of perceptual hashing
Ferguson and Wilkinson	2017	Juvenile age estimation from facial images
Fromberger *et al.*	2021	@myTab—A placebo controlled randomized trial of a guided web-based intervention for individuals who sexually abused children and individuals who consumed child sexual exploitation material: A clinical study protocol
Fussey and Sandhu	2022	Surveillance arbitration in the era of digital policing
Gauvin *et al.*	2025	Question types in online sex offender interviews: Unveiling the influence on information retrieval

Gupta	2024	Child pornography and internet subcultures in India: A legal perspective
Gutfeter *et al.*	2025	Detecting sexually explicit content in the context of the child sexual abuse materials (CSAM): End-to-end classifiers and region-based networks
Haginoya *et al.*	2023	AI avatar tells you what happened: The first test of using AI-operated children in simulated interviews to train investigative interviewers
Häikiö and Uusoksa	2016	644 new and innovative way to tackle child sexual abuse
Hendrick *et al.*	2024	Empowering youth through play: Promoting awareness of sexual grooming among schoolchildren through game-based learning
Henry	2020	Designing effective digital advertisements to prevent online consumption of child sexual exploitation material
Humann *et al.*	2023	Motivational interviewing in child sexual abuse investigations: Approaches shown to increase suspect engagement and information gathering during police interviews
Hunn *et al.*	2018	Exploring the educative role of judges' sentencing remarks: An analysis of remarks on child exploitation material
Hunn *et al.*	2023	How to implement online warnings to prevent the use of child sexual abuse material
Ilbiz and Kaunert	2023	Crowdsourcing to tackle online child sexual exploitation: Europol's 'Stop Child Abuse—Trace an Object' platform
Kantipudi and Chuemchit	2024	Teach to say 'NO'—A mixed methods evaluation of a child sexual abuse prevention training for primary school teachers in Phnom Penh, Cambodia
Kardos	2025	Beyond the consent paradigm: Problematizing representations of AI-generated pornography in the education discourse of the UN
Kaushal *et al.*	2024	Automated transparency: A legal and empirical analysis of the Digital Services Act Transparency Database
Kiss *et al*.	2025	Growing up without violence (GWV): Study protocol for a cluster randomised trial and process evaluation of a school-based intervention preventing adolescent sexual exploitation in Brazil'
Kloess *et al.*	2021	The challenges of identifying and classifying child sexual exploitation material: Moving towards a more ecologically valid pilot study with digital forensics analysts
Kristiningsih and Kasuma	2018	Settlement of online child sexual exploitation cases in Indonesia (Cases study: Facebook group 'Club Brondong Puncak' and 'Official Candy's Group'
Lakkur *et al.*	2024	Triage of messages and conversations in a large-scale child victimization corpus

Leclerc *et al.*	2022	Child sexual abuse material online: The perspective of online investigators on training and support
Levine *et al.*	2020	A forensically sound method of identifying downloaders and uploaders in Freenet
Li *et al*.	2024	SafeGen: Mitigating sexually explicit content generation in text-to-image models
Lindenbach *et al.*	2021	Capacity confidence and training of Canadian educators and school staff to recognize and respond to sexual abuse and internet exploitation of their students
Lindholm *et al.*	2024	The investigation of online child sexual abuse cases in Sweden
Lisanawati	2015	What can IT and Money Laundering Law do to fight against cyber child sexual crime?
Long *et al.*	2016	KIRAT: Law enforcement's prioritization tool for investigating indecent image offenders
Lu *et al.*	2024	A content analysis of metrics on online child sexual exploitation and abuse used by online content-sharing services
MacLeod and Grant	2017	'go on cam but dnt be dirty': Linguistic levels of identity assumption in undercover online operations against child sex abusers
Martelozzo	2015	Policing online child sexual abuse: The British experience
Martelozzo and DeMarco	2020	Exploring the removal of online child sexual abuse material in the UK: Processes and practice
McCain *et al.*	2024	Review of policies and practices to prevent technology-facilitated child sexual abuse within youth-serving organizations in the United States
Merdian *et al.*	2025	Circles ReBoot: A feasibility study and preliminary outcome evaluation
Midani *et al.*	2025	The legal, policy, institutional and programmatic context for protecting children against online sexual exploitation in Tunisia
Netkova and Mustafa	2021	International legal standards in combating child online sexual abuse and exploitation
Newman *et al.*	2023	The impact of a public health campaign to deter viewing of child sexual abuse images online: A case study of the UK Stop It Now! campaign
Ngo *et al.*	2024	Discovering child sexual abuse material creators' behaviors and preferences on the dark web
Nguyen *et al.*	2022	A deep learning-based application for recognition and preventing sensitive image
Pfefferkorn	2021	Content-oblivious trust and safety techniques: Results from a survey of online service providers

Popa	2024	National and international cooperation in investigating crimes of child sexual abuse or sexual exploitation committed by using information technologies
Prichard *et al.*	2021	Effects of automated messages on internet users attempting to access 'barely legal' pornography
Prichard *et al.*	2024	The effect of therapeutic and deterrent messages on internet users attempting to access 'barely legal' pornography
Rantatalo *et al.*	2025	Co-creation to increase cross-functional collaboration in police investigations of online child sexual abuse: A qualitative study protocol
Razi *et al.*	2023	Sliding into my DMs: Detecting uncomfortable or unsafe sexual risk experiences with Instagram direct messages grounded in the perspective of youth
Reeves *et al.*	2024	May and Bay: Online child sexual exploitation and abuse in Southeast Asia—Using digital games in preventative education
Rimer	2020	Discipline as prevention: Psychoeducational strategies in internet sexual offending group programs
Ringenberg *et al.*	2024	Are you a cop? Identifying suspicion in online chat operations with online groomers
Rodríguez *et al.*	2020	C3-Sex: A conversational agent to detect online sex offenders
Rudolph *et al.*	2022	Child sexual abuse prevention: Parental discussion, protective practices and attitudes
Sakpal and Jain	2023	Revenge pornography matching using computer vision
Salter and Richardson	2021	The Trichan takedown: Lessons in the governance and regulation of child sexual abuse material
Samanta and Jain	2024	SmartHash: Perceptual hashing for image tampering detection and authentication
Santopietro *et al.*	2024	A multi-factor knuckle and nail bed verification tool for forensic imagery analysis
Seigfried-Spellar *et al.*	2019	Chat Analysis Triage Tool: Differentiating contact-driven vs. fantasy-driven child sex offenders
Stathis and Marinakis	2022	Shadows into light: The investigative utility of voice analysis with two types of online child-sex predators
Steedman and Jeglic	2025	Child sexual abuse prevention among a sample of US parents
Steinebach	2023	An analysis of PhotoDNA
Struppek *et al.*	2022	Learning to break deep perceptual hashing: The use case NeuralHash
Švec *et al.*	2024	Slovak mimicry of online content moderation on digital platforms as a result of the adoption of the European Digital Services Act

Trujillo *et al.*	2025	The DSA Transparency Database: Auditing self-reported moderation actions by social media
Tselenti *et al.*	2025	Policing child sexual exploitation and abuse cases: A qualitative PRIORITY study of the challenges faced by law enforcement officers in Germany, Portugal, and Sweden
Ubericht	2023	Sekundärprävention der Nutzung von Kindesmissbrauchsabbildungen im Internet: ein internationaler Überblicksversuch
Valois *et al.*	2025	Leveraging self-supervised learning for scene classification in child sexual abuse imagery
Walker *et al.*	2024	Rolling out the red carpet: Non-offending partners and affected family members as allies in disruption
Westlake and Guerra	2023	Using file and folder naming and structuring to improve automated detection of child sexual abuse images on the Dark Web
Wilkinson *et al.*	2024	A comparative analysis of legislative protections for online safety in the Global South: A case study of the Caribbean
Yoon *et al.*	2025	'It's great because it's ran by us': Empowering teen volunteer Discord moderators to design healthy and engaging youth-led online communities
Zubaidi	2021	Monitoring internet child pornography (ICP) in Malaysia

Appendix C: List of Included Organizations' Reports.

Author(s)	Year	Publication title
ECPAT *et al.*	2022	*Disrupting Harm in Cambodia: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al*.	2022	*Disrupting Harm in Ethiopia: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in Indonesia: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in Kenya: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in Malaysia: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in Mozambique: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in Namibia: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in the Philippines: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in South Africa: Evidence on Online Child Sexual Exploitation and Abuse*

ECPAT *et al*.	2022	*Disrupting Harm in Tanzania: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in Thailand: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al*.	2022	*Disrupting Harm in Uganda: Evidence on Online Child Sexual Exploitation and Abuse*
ECPAT *et al.*	2022	*Disrupting Harm in Viet Nam: Evidence on Online Child Sexual Exploitation and Abuse*
Munns *et al.*	2024	*Facilitation of Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines: Analysis and Recommendations for Better Detection, Deterrence and Prevention*
Thakur and Gorwa	2024	*Real Time Threats: CSEA Prevention on Livestreaming Platforms*
UNICEF	2020	*National Study on Online Sexual Abuse and Exploitation of Children in the Philippines: Final Report*
UNICEF	2021	*Ending Online Child Sexual Exploitation and Abuse: Lessons Learned and Promising Practices in Low- and Middle-Income Countries*
We Protect Global Alliance	2022	*Framing the Future: How the Model National Response Framework Is Supporting National Efforts to End Child Sexual Exploitation and Abuse Online*

ACKNOWLEDGMENTS

Contributors

Drafting authors: Kruakae Pothong (Consulting Scientist, Thailand/UK), Selcan Kaynak (Panel Chair, Turkey), Deborah Fry (Panel Member, USA/UK), Sakshi Ghai (Panel Member, India), Sonia Livingstone (Panel Member, UK), Andy Phippen (Panel Member, UK), Cheryll Ruth Soriano (Panel Member, Philippines), Lisa M. Given (Member of the IPIE Science & Methodology Committee, Australia), Philip Howard (IPIE President and CEO, Canada/UK), Sebastián Valenzuela (IPIE Chief Science Officer and Chair of the Science & Methodology Committee, Chile). Independent general reviews: Elena Martelozzo and Sun Sun Lin. Design: Domenico Di Donna. Copyediting: Dawn Rushen and Michelle Rosen. We gratefully acknowledge support from the IPIE Secretariat: Lola Gimferrer, Jessica Gold, Egerton Neto, Wiktoria Schulz, Donna Seymour, Anna Staender, and Alex Young.

Declaration of interests

IPIE reports are developed and reviewed by a global network of research affiliates and consulting scientists who constitute focused Scientific Panels and contributor teams. All contributors and reviewers complete declarations of interests, which are reviewed by the IPIE at appropriate stages of the work.

Preferred citation

An IPIE *Summary for Policymakers* provides a high-level precis of the state of knowledge and is written for a broad audience. An IPIE *Synthesis Report* makes use of scientific meta-analysis techniques, systematic review, and other tools for evidence aggregation, knowledge generalization, and scientific consensus building, and is written for an expert audience. An IPIE *Technical Paper* addresses particular questions of methodology, or provides a policy analysis on a focused regulatory problem. All reports are available on the IPIE website (www.ipie.info).

This document should be cited as:

International Panel on the Information Environment [K. Pothong, S. Kaynak, D. Fry, S. Ghai, S. Livingstone, A. Phippen, C. R. Soriano, L. M. Given, P.N. Howard, S. Valenzuela (eds.)], *Detecting, Deterring, Investigating, and Prosecuting Technology-Facilitated Child Sexual Exploitation and Sexual Abuse: A Systematic Review*. Zurich, Switzerland: IPIE, 2026. Synthesis Report, SR2026.1, doi: 10.61452/UZUS7376.

Funders

The International Panel on the Information Environment (IPIE) gratefully acknowledges the support of its funders. For a full list of funding partners please visit www.ipie.info. Any opinions, findings, conclusions, or recommendations

expressed in this report are those of the IPIE and do not necessarily reflect the views of the funders.

Authors' AI Contribution Statement

Large Language Models (LLMs) were used to support specific stages of this work, including generating an illustration for a diagram, identifying specific examples from the coded documents, and cross-checking human-identified thematic patterns. AI-based translation tools were used for back-translation and double-checking the translation between Italian and English and German and English. All AI-generated or AI-assisted content was critically reviewed, verified, and revised by the lead human author, who takes full responsibility for the final version of the work.

Copyright Information

ABOUT THE IPIE

The International Panel on the Information Environment (IPIE) is an independent and global science organization committed to providing the most actionable scientific knowledge about threats to the world's information environment. Based in Switzerland, its mission is to provide policymakers, industry, and civil society with independent scientific assessments on the global information environment by organizing, evaluating, and elevating research, with the broad aim of improving the global information environment. Hundreds of researchers from around the world contribute to the IPIE's reports.

For more information, please contact the International Panel on the Information Environment (IPIE), secretariat@IPIE.info. Seefeldstrasse 123, P.O. Box 8034, Zurich, Switzerland.

International Panel on the Information Environment

Seefeldstrasse 123
P.O. Box 8034 Zurich
Switzerland

ISBN 978-3-03983-013-8