Child Online Sexual Exploitation and Abuse: understanding adversarial tactics, techniques, and procedures

social sciences

MDPI

Article

Child Online Sexual Exploitation and Abuse: Understanding Adversarial Tactics, Techniques, and Procedures

Abel Yeboah-Ofori [1,*] and Awo Aidam Amenyah [2]

[1] School of Computing and Engineering, University of West London, London W5 5RF, UK
[2] Child Online Africa, Accra P.O. Box AN 7466, Ghana; awo@childonlineafrica.org
* Correspondence: abel.yeboah-ofori@uwl.ac.uk

Abstract

Background: Child Sexual Exploitation and Abuse is a longstanding global issue, increasingly amplified by digital technologies, mobile devices, and internet access. This shift has intensified Child Online Sexual Exploitation and Abuse (COSEA). WeProtect 2020, a Global Alliance Intelligence brief report, indicated a 200% rise in online abuse forums. Existing studies focus on child protection, grooming, and survey-based analyses and draw inferences regarding grooming tactics and thematic analysis. Social issues such as underreporting, limited threat intelligence sharing, and low cyber awareness persist, leading to vulnerabilities and various exploitations. Further, a lack of social engagement and support persists, posing serious challenges for victims and law enforcement. Multiple studies have used the term Online Child Sexual Exploitation and Abuse (OCSEA) that focus on a technology-centric approach. However, the paper considers Child Online Sexual Exploitation and Abuse (COSEA) child-centric approach as we explore challenges of a child accessing the internet and engaging in online activities. Methods: This study analyses COSEA using the MITRE tactics, techniques, and procedures (TTP) framework to examine perpetrator behavior, motives, and potential attribution, considering the evolving threat landscape. Results: TTP-based analysis enables the identification of adversary intent, methods, and opportunities. The study contributions are threefold: (1) we explore COSEA and its manifestations; (2) we apply the MITRE TTP framework with subjective expert judgment to analyze perpetrator behavior and the victim; for instance, what leads victims to become complicit in wrong acts; and (3) propose mitigation strategies and stakeholder roles. Conclusion: By integrating technical, social, and behavioral perspectives, it highlights the roles of economic, societal, and deterrence factors and recommends policy, education, and collaborative threat-intelligence sharing to enhance child online safety.

Keywords: child abuse; online Child Sexual Exploitation; tactics, techniques, and procedures (TTP); child online protection; child safety; cyberattacks; cyber threat intelligence

Academic Editor: Peter Hopkins

Received: 29 January 2026
Revised: 21 April 2026
Accepted: 21 April 2026
Published: 8 May 2026

1. Introduction

Child Online Sexual Exploitation and Abuse (COSEA) has increased exponentially due to current trends in digital transformation and phenomenal growth in the use of the internet, social media, and mobile devices (Joleby et al. 2021; Whittle et al. 2013; Kloess et al. 2014; Internet Watch Foundation 2018). These advancements have facilitated online

grooming, abuse, and technology-assisted exploitation (NSPCC 2020; Hamilton-Giachritsis et al. 2020), exacerbating risks for vulnerable children globally and resulting in severe psychological, social, and health consequences (Kloess et al. 2017a; Sivagurunathan et al. 2019; Wurtele 2009; Naebklang 2014; Palmer 2015). These risks highlight the digital dangers and the impact of technology usage for these exploits and abuses. OCSEA is a common terminology used in multiple studies to describe Child Online Sexual Exploitation and Abuse. However, given the evolving threat landscape and changing attack surface, understanding the drivers of COSEA and their implications is critical for investigation and mitigation.

COSEA differs from OCSEA in scope and analytical focus, as they represent distinct areas. For instance, COSEA adopts a child-centric perspective, emphasizing how a child's online presence, digital identity, and interactions increase vulnerability to exploitation and psychological harm (Joleby et al. 2021; Ramiro et al. 2019; Interagency Working Group 2019; Choi and Lee 2023). Specifically, COSEA focuses on child-centric threats, sexual exploitation, and child abuse in an online environment. It highlights the implications for child protection, policy development, and social sciences. Perpetrators exploit these vulnerabilities, particularly among children from disadvantaged backgrounds, using grooming, coercion, and extortion to produce and disseminate sexually explicit material (NSPCC 2020; Kloess et al. 2017b).

In contrast, OCSEA takes an environment-centric approach focusing on technological platforms and how children access the internet and interact, which has led to cyber-enabled threats, attack mechanisms, social engineering, cyberbullying, and online grooming (Fry et al. 2025). The analysis of these online platforms and social media forums provides an understanding of the technical aspects, impact on children's well-being, and media that facilitate these crimes. While both perspectives are complementary, they underscore the need for integrated child protection strategies and stakeholder collaboration.

The study explores challenges children face when they go online, and the methods perpetrators use to target them. It further examines how offenders exploit digital environments, identifies the associated risks and regulatory frameworks, and proposes security controls to inform policy development and enhance stakeholder awareness.

Increased Use of Smartphones Among Children

The rapid adoption of smartphones has intensified COSEA risks, enabling constant connectivity and facilitating the distribution of exploitative content. In the UK, 99% of children engage in online activities, with most possessing mobile devices and engaging on social media platforms at an early age. Despite age restrictions, many children under 13 maintain active accounts, thereby increasing their exposure to online harms. The contributing factors include the following:

- Nine in 10 children own a mobile phone by the time they reach the age of 11.
- Three-quarters of social media users aged between 8 and 17 have their own account or profile on at least one of the large social media platforms.
- Most platforms have a minimum age of 13. However, six in 10 children aged 8 to 12 who use them have signed up using their personal profile.
- Almost three-quarters of teenagers between the ages of 13 and 17 have encountered one or more potential harms online.
- Three in five secondary school-aged children have been contacted online in a way that potentially made them feel uncomfortable.

Studies indicate widespread exposure to risks, including unwanted contact, sexual solicitation, and harassment (NSPCC 2024; Finkelhor et al. 2022). The convergence of on/offline environments has amplified individual vulnerabilities, leading to significant

long-term psychological consequences, including mental health disorders, self-harm, and increased behavioral risks (Lefevre et al. 2017). That has greatly impacted parents and the victims in their later lives, leading to drug abuse and self-harm. Perpetrators use TTP to exploit these conditions using digital platforms, including messaging apps, social media, and chat forums, to manipulate and abuse victims. Tactics include deception, coercion, and trust-building strategies (e.g., "love bombing"), followed by exploitation through sextortion or content production (Joleby et al. 2021; Ioannou et al. 2018). When children perceive their rights and safety as neglected, their vulnerability increases, often leading to distrust in their immediate environment and greater reliance on online platforms (Hallett 2016). The COVID-19 pandemic intensified these trends, with notable rises in online abuse reports and activity across platforms such as Facebook, Snapchat, and other digital forums (WePROTECT Global Alliance 2020; Keller and Dance 2019; Brewster 2020) Existing studies have primarily adopted child-centered approaches to examine sexual exploitation and abuse (Lefevre et al. 2017; Westendorf and Searle 2017; Demetis and Kietzmann 2021; Merdian et al. 2020; Quayle 2020), while others have explored victims' online challenges and the impact of offenders (Kloess et al. 2017b; Cohen-Almagor 2013). However, the rapid growth in mobile device usage, internet access, and network connectivity has significantly increased COSEA incidents, a trend further intensified during the COVID-19 pandemic. Comparative research (Ioannou et al. 2018) has examined both online and offline grooming dynamics, including the application of victim role models to understand the exploitation processes of perpetrators. commonly employ manipulative strategies—such as coercion, deception, flattery, and false expressions of affection to gain trust and exert control over victims (Joleby et al. 2021).

Empirical evidence highlights the scale of the problem. A 2020 report by the WeProtect Global Alliance documented a 200% increase in child sexual abuse forums and downloads during the early months of the COVID-19 pandemic (WePROTECT Global Alliance 2020). Additionally, approximately 95% of children aged 12–17 have internet access, with one in five reporting exposure to unwanted sexual solicitation, particularly among those aged 11–15 (Keller and Dance 2019). In the United States, the National Center for Missing & Exploited Children reported a 106% rise in suspected exploitation cases, increasing from 983,734 in March 2019 to over 2 million in March 2020 (Brewster 2020). Similarly, The New York Times report (2019) indicated that technology companies flagged a record 45 million online child abuse images, including cases involving very young children (Keller and Dance 2019).

In Europe, Longobardi et al. (2021) examined the prevalence and sociodemographic risk factors associated with COSEA, reporting that 82% of minors in Italy use social networking platforms, with up to 39% of teenagers at risk of online sexual victimization (OSV). This is often linked to behaviors such as sexting and offline meetings initiated online. Similarly, in Spain, 61% of adolescents reported experiencing OSV within a year, with around 50% indicating the highest levels of exposure to online harassment.

Factors contributing to increased COSEA include greater online activity among children, particularly through social networking and engagement with sexually explicit content, including sexting and pornography websites. Affordable bandwidth and internet speeds are some of the factors leading to internet-based grooming and shaping sexual content for interest (Joleby et al. 2021; Whittle et al. 2013; Kloess et al. 2014; Ioannou et al. 2018). Perpetrators exploit digital platforms to manipulate, coerce, and abuse victims through tactics such as deception, luring, and live streaming, often pressuring children to produce and share explicit content (Interagency Working Group 2019). Evidence highlights the scale and severity of this issue. The Internet Watch Foundation report (2017) identified 2082 live-streamed abuse videos, with 96% involving children acting alone, 98% under the age of 13, and 96% girls; most content circulated, with 73% of the images

appearing on chat forums, advertisements, and downloads. Detection remains challenging due to the diverse nature of perpetrators, ranging from individual offenders and online pedophiles to organized groups who operate on encrypted and dark web platforms to evade law enforcement (Internet Watch Foundation 2018). Globally, the Childlight report (2024) estimates that over 300 million children annually experience technology-facilitated sexual exploitation, including solicitation, non-consensual image sharing, and sextortion (Childlight Global Child Safety Institute 2024). In the UK, an NSPCC report (2024), drawing on Ofcom data, shows that 84% of children aged 3–4 are already online, rising to 100% among those aged 12 and above (NSPCC 2024). Key findings indicate widespread exposure to online risks, including unsolicited contact and harmful interactions. Some of the key findings from the data show that:

- About 19% of children aged 10–15 years old exchanged messages with someone online whom they had never met before in the last year.
- Over 9000 child sexual abuse offenses involved an online element in 2023–24.
- Around a sixth of people who experienced online harassment offenses were under 18 years old.
- Under-18-year-olds were the subject of around a quarter of reported offenses of online blackmail in England, Wales, and Northern Ireland.

Further, (Finkelhor et al. 2022) highlighted some findings of online child sexual abuse on 2639 US individuals as follows: image-based sexual abuse, 15.6%; self-produced child sexual abuse images, 11.0%; non-consensual sexting 7.2%; online grooming by adults, 7.2%; revenge pornography, 5.4%; sextortion, 3.1%; and online commercial sexual exploitation, 1.7%. A recent report by WeProtect Global Alliance 2024 indicates that over 300 million children under the age of 18 have been affected by Online Child Sexual Exploitation and Abuse in the last 12 months (WePROTECT Global Alliance 2024). The new report by the UK National Police Chiefs' Council (NPCC) 2024 on the Vulnerability Knowledge and Practice Programme (VKPP) on Child Sexual Abuse and Exploitation (CSAE) crimes across England and Wales indicates (National Police Chiefs' Council 2024):

- There were around 107,000 offenses reported in 2022, a 7.6% increase compared to 2021, nearly quadruple what they were 10 years ago. Evidence continues to suggest many crimes remain unreported.
- About 75% of CSAE offenses relate to sexual crimes committed directly against children, and around 25% relate to online offenses of Indecent Images of Children.
- The crime types regarding CSAE are changing. For example, historically, Child-on-Child abuse accounted for around a third of offenses. The data in the report suggests that today, this is just over half.
- CSAE within the family environment remains a common form of reported abuse, accounting for an estimated 33% of reported CSAE crime. Parents and siblings were the two most common relationships featured.
- Group-based CSAE accounts for 5% of all identified and reported CSAE, ranging from unorganized peer group sharing of imagery to more organized, complex, high-harm cases with high community impact.
- Reported CSAE is heavily gendered, as expected, with males (82% of all CSAE perpetrators) predominantly abusing females (79% of victims). Sexual offending involving male victims is more common in offenses involving indecent images and younger children.
- The number of recorded incidents of Online Sexual Abuse continues to grow, and it accounts for at least 32% of CSAE.
- About 52% of all CSAE cases involved reports of children (aged 10 to 17) offending against other children, with 14 being the most common age.

These growing trends reflect a broad spectrum of abuse, including coercion, extortion, and severe offenses such as sexual assault. Perpetrators exploit pseudonymity and employ manipulative strategies such as deception, intimidation, and blackmail to coerce victims (Internet Watch Foundation 2018; NSPCC 2020; United Nations Office on Drugs and Crime 2020). Their tactics align with cybercrime TTPs, including social engineering, grooming, sextortion, and live streaming to produce exploitative content (NSPCC 2020). Child exploitation may also involve offline elements, such as inducements through gifts, substances, or financial incentives to guardians. Notably, studies indicate that up to 75% of children are willing to share personal information online in exchange for goods or services, further increasing their vulnerability (PureSight 2018).

The paper explores COSEA by analyzing how perpetrators employ MITRE tactics, techniques, and procedures (TTPs) to understand adversarial behavior, underlying motives, and support attribution for cyber threat intelligence and profiling. In light of the evolving threat landscape, it builds on existing research to enhance insight into attacker methodologies and emerging trends. The study makes three primary contributions. First, it defines COSEA and examines its manifestations and common exploitation methods. Second, it applies the MITRE framework, supported by expert judgment (Section 3), to systematically analyze perpetrator behavior and its influence on victim complicity. Third, it proposes mitigation strategies, emphasizing the role of stakeholders in addressing COSEA. The findings show that TTP-based analysis improves the identification of adversary intent, capability, and opportunity, while informing policy development, education, and collaborative threat intelligence sharing.

2. State of the Art

This section reviews the state of the art and related works in child online exploitation and abuse, including some reported cases of incidents and perpetrator exploits on victims. COSEA challenges are a global phenomenon that significantly affects children, parents, society, law enforcement, organizations, and legal frameworks, and they require extensive research to curb their proliferation. Fry et al. (2025) explored the prevalence estimates and nature of Online Child Sexual Exploitation and Abuse by using a systematic review and meta-analysis approach to derive results from the 47,097 literature searches, with 86 records reported on 123 studies to provide mean prevalence estimates of children younger than 18 years who have experienced different forms of OCSEA on a global scale. Further, Hamilton-Giachritsis et al. (2020) explored the impact of technology-assisted child sexual abuse and how this is similar to or differs from offline abuse from the perspective of young people by using quantitative data and qualitative interviews to gather and identify additional elements or complexities arising from the digital elements. Furthermore, Palmer and Foley (2017) explored the complexities and dilemmas faced by young people and professionals in CSE cases, using thematic analysis to understand the uncertainties in the domain and their impact on females, to assist social workers in interventions to support young people. However, the work did not consider TTPs used by the perpetrators on the victims to have a balanced, objective view.

Regarding factors that impact children in the UK, Radford et al. (n.d.) carried out a survey of child abuse and neglect cases in the UK and presented findings on the prevalence, impact, and severity of child maltreatment in the UK, leading to poor emotional well-being, self-harm, suicidal ideation, and delinquent behaviors. Additionally, Quayle, 2020, presented an argument that centered around the role of technology in the prevention and changing of the environment that supports the disruption and deterrence of Online Child Sexual Exploitation and Abuse. Lefevre et al. (2017) evaluated a child-centered framework for working with Child Sexual Exploitation (CSE). The authors used a survey and qualitative methods to analyze relationship-based practice issues, a child-centered

approach, an ethically grounded approach, and a knowledge-based relationship with CSE. Joleby et al. (2021) explored offending strategies for engaging children in online sexual activity by using mixed methods with thematic analysis to identify patterns of abuse on victims and characteristics of offenders. To understand perpetrators' motives, Kloess et al. (2017b) explored the modus operandi of offenders by analyzing their sexually exploitative interactions with children online, including discursive tactics. Demetis and Kietzmann (2021) proposed a consolidated model for online CSE that combines the staging of the phenomenon with key dimensions depicting how the use of technology and imagery both fuel and defuse it. However, the study discussed the role of information systems in detecting online CSE, but not in detecting it among perpetrators or TTPs. Whittle et al. (2013) conducted a survey using thematic analysis to gather victims' responses on their vulnerabilities to grooming, interviewing eight young people to understand how they were groomed for policy formulation, practices, and presentations. Regarding legislative issues, Choo et al. (2014) analyzed legislative and prosecution-based responses in Australia and the United Kingdom. The authors highlighted the definitions and procedures for collecting data on child online exploitation to support a coherent approach to policy formulation. Merdian et al. (2020) proposed an etiological model specific to CES material offending. The study resulted in seven superordinate themes: development context, individual risk propensities, psychological vulnerabilities, personal circumstances, permission-giving thoughts, and the internet environment. Kloess et al. (2014) reviewed current knowledge and understanding of the OCSE process, prevalence, and offending characteristics of grooming and exploitation of children on the internet. Cohen-Almagor (2013) explored various online child sex offense challenges on victims, their impact, and recommendations for countermeasures. Regarding abusive behaviors on children, Westendorf and Searle (2017) considered how different forms of sexually exploitative and abusive behaviors are perpetrated at peacekeeping missions and the risk factors. Kloess et al. (2017b) assessed the reliability with which images of children are classified as indecent or non-indecent and considered using thematic analysis to determine the implications of sexual abuse and exploitation and how the law categorizes it. Further, Laws and Hall (2019) and Baines (2019) presented particular issues that address Child Sexual Abuse and Exploitation, and suggested improvements required to understand the practice. To gain a deeper understanding of children's digital experiences and online risks attuned to their individual and contextual diversities, Quayle (2016) surveyed global kids' Online Child Sexual Exploitation and Abuse. Further, ECPAT International (2017) examined children's online behaviors and vulnerabilities across five countries. It indicated that about 70% of the children use internet cafes, with about 405 of the children having accessed child pornography online before. However, the digital landscape has changed recently due to the increasing use of mobile devices, ISPs, and internet access. Furthermore, Salter and Hanson (2021) examined the phenomenon of internet users' attempts to report and prevent online Child Sexual Exploitation (CSE) and Child Sexual Abuse Material (CSAM) in the absence of adequate intervention by the government, ISPs, and social media platforms by focusing on the regulatory stance. Regarding the prevalence and sociodemographic risk factors associated with the COSEA phenomenon, Longobardi et al. (2021) investigated the prevalence of online sexual victimizations (OSV) and related risk factors among males and females who are in their early adolescence by conducting a cross-sectional study on 310 Italian adolescents between 12 and 14 years old in middle school. However, several factors influence the prevalence and sociodemographic risks leading to vulnerable victims, including social isolation, family breakdowns, single-parent families, poverty and financial difficulties, and neglect of children in care homes without proper parental care (Tunagur et al. 2025). Recent indicators have pointed to children identifying as LGBTQ+ having become vulnerable to COSEA due to social isolation. Thereby, using online and social networking

platforms to seek an online social community for acceptance and affection (Montiel et al. 2016). This leads to the child being vulnerable to online abuse or exploitation.

Other factors, such as developmental psychology, provide crucial backgrounds for understanding why children and adolescents are vulnerable to COSEA. These factors include cognitive development, vulnerability, and distinguishing the reality of adolescence. This provides an understanding of the differences between safe and unsafe online interactions when threat actors and groomers use sophisticated manipulation skills to trick victims. These perpetrators can use manipulative skills to gain trust and attention from the children, including "love bombing", inordinate affections to develop trust and secret relationships, validations, and later use of coercion to trap the child to feel powerless to seek help (NSPCC 2026). These have led to psychological impact, such as mood swings, guilt, self-blame, shame, depression, trauma, suicidal thoughts, feelings of being the instigator, and post-traumatic stress disorder (PTSD) on victims.

Regarding sexual exploitation and abusive acts on children online, the UNODC (United Nations Office on Drugs and Crime 2020) considers COSEA as sexual acts on children where the perpetrators use an exchange of some sort, such as food, affection, drugs, or shelter, to lure and deceive the child. The Interagency Working Group (Interagency Working Group 2019) considered it a crime that the perpetrators abuse a position of trust, exploit vulnerable children, and use different powers and tricks for sexual exploitation purposes. However, Radford (2018) posits that measuring the extent of child abuse and neglect and comparing abuse rates is difficult because of conceptual and methodological differences in measuring child abuse and violence. Furthermore, the Council of Europe (Council of Europe 2019) posits that no single state can prevent and combat online child exploitation and abuse alone. Additionally, Bailey et al. (2021) explored the impact of technology-facilitated violence and mistreatment from international perspectives, including the spectrums of behaviors of perpetrators online and offline. The authors considered technologies such as AI, live streaming, GPS tracking, and social media from a regulatory perspective. Hence, organized and collaborative projects, reporting platforms, and threat information-sharing platforms are required to mitigate COSEA.

All the related works are relevant and contributed to improving COSEA challenges and research areas. However, our work considered the MITRE Kill Chain approach to addressing the adversary's tactics, techniques, and procedures from a technical perspective to understand the mindset, intent, motives, opportunities, and methods perpetrators exploit for threat intelligence gathering and to improve security.

2.1. Incidents of Child Online Sexual Exploitation and Abuse

There are several child online exploitations and abuse cases by perpetrators involving individuals, gangs, online pedophiles, and online predators who use the dark web, instant messaging, pop-ups, chat rooms, and internet forums. To determine the perpetrator's method and motives, WePROTECT Global Alliance (2015) analyzed various sexually exploitative interactions between offenders and victims on online platforms. However, the threat landscape and attack surface continue to evolve, allowing threat actors to adapt their operations to exploit their victims. A report by Childlight (2024) posits that one in nine men in the United States (10.9%, equating to almost 14 million men) has admitted to online sexual offending against children at some point in their lives. Representative surveys found the same to be true among 7% of men in the UK, equating to 1.8 million offenders, and among 7.5% of men in Australia, that is, nearly 700,000 (Childlight Global Child Safety Institute 2024). Thus, the rationale for the study is to use the qualitative (TTP) attack method to understand the perpetrator's motives, mindset, and strategies, considering the invincibility nature of the attacks. Hence, identifying a few COSEA cases will provide us with a basis for adopting this approach. The perpetrators use various

reconnaissance, social engineering, and interception methods to identify their victims and then deploy multiple tactics, techniques, and procedures to exploit and abuse them. Online predators are individuals and gangs that use the internet to commit Child Sexual Abuse and Exploitation, which leads to offline contact. Predators use online platforms such as instant messaging, pop-ups, chat rooms, internet forums, social network sites, and video game consoles. There have been instances of live-streaming cases of child sexual abuse that involve women forcing their children to perform sexual acts or serving on the children in the UK, Romania, and the Philippines (United Nations Office on Drugs and Crime 2020). In the UK, a group of perpetrators were charged and convicted (R v. Costi 2006) under the Sexual Offences Act (2003) (United Kingdom 2003). The group met a minor after grooming her online using an internet chat relay and performed a sexual act on her. The US investigator's report revealed that a Romanian woman was sexually abusing her one-year-old daughter and three-year-old son by exposing them online via Skype for payment, UNODC 2020 (United Nations Office on Drugs and Crime 2020). In the USA, Megan Meier died by suicide after experiencing cyberbullying by a mother and her teenage daughter in 2006 through a social networking website, MySpace, which led to the introduction of the Megan Meier Cyber Bullying Prevention Act of 2009 (Espelage and Hong 2017). Through the catfishing method, Paris Dunn was groomed by Shelly Chartier and groomed into exchanging nude photos and sexually explicit acts under the pretense of using a false ID (United Nations Office on Drugs and Crime 2020).

2.2. Analytical Synthesis of Child Online Sexual Exploitation and Abuse

Existing research on COSEA has demonstrated a rapidly evolving threat landscape and a changing attack surface shaped by increased mobile device usage, technological transformation, socio-psychological vulnerabilities, and inadequate stakeholder engagement and regulation. The literature establishes a systemic global threat phenomenon that impacts all victims, including children, families, and society, and requires urgent interventions by government institutions and regulatory bodies.

Multiple studies focused on global COSEA prevalence estimates, including (Fry et al. 2025; WePROTECT Global Alliance 2020; Childlight Global Child Safety Institute 2024; Palmer and Foley 2017; Salter and Hanson 2021; Radford 2018; Longobardi et al. 2021; Tunagur et al. 2025; Montiel et al. 2016), as well as a systematic analysis of victimization across diverse online exploitation platforms. Although these studies are critical in using adolescents to quantify the magnitude of the challenges of the prevalence, they are inherently constrained by methodological inconsistencies, as they consider particular jurisdictions, leading to underreporting of real incidents of exploitation and abuse, thereby providing ambiguities that limit global cross-study comparability and analysis, which obscure the true scale of global abuse. These issues highlight the broader challenges facing researchers in measuring the extent of child exploitation and abuse globally. Thus, the conceptual understanding of criminals' mindsets using TTPs provides stakeholders with a stronger strategic imperative to address methodological fragmentation in policy formulation.

Regarding technological-facilitated abuse and victim vulnerabilities, multiple researchers (Kloess et al. 2014; Hamilton-Giachritsis et al. 2020; Ioannou et al. 2018; Keller and Dance 2019; Quayle 2016; ECPAT International 2017; Council of Europe 2019; Bailey et al. 2021) examining technological-facilitated abuse dynamics have emphasized how the digital transformation has reshaped abuse patterns. Additionally, studies that highlighted the emergence of hybrid abuse patterns compared instances where online interactive abuse transitioned to offline exploitation. However, most of these works focus on the experiences of victims and the impact rather than systematically exploring perpetrator behaviors and attack patterns.

Furthermore, qualitative and thematic studies provided valuable insights into how vulnerable victims are during the grooming process, what leads them to become complicit in wrongdoing, illegal activity, or unethical situations. These studies (Joleby et al. 2021; Whittle et al. 2013; Kloess et al. 2017b; United Nations Office on Drugs and Crime 2020; Radford et al. n.d.; Laws and Hall 2019; Baines 2019; Montiel et al. 2016; NSPCC 2026) identified socio-psychological factors leading to exploitation and abuse, such as the lack of awareness, unstable family background, social isolation, immaturity, and identity seeking among the LGBTG+ adolescent community. The work reveals how perpetrators exploit the victims' psychological and emotional needs through using manipulative tactics and extorsions such as building relationships, giving attention, or gifts ("Love Bombing"), then deploying coercive methods to control the victim. Despite these contributions, the literature tends to present descriptive rather than analytical studies, lacking structured models of attacks, adversary behaviors, and patterns.

Multiple studies (Ramiro et al. 2019; Kloess et al. 2017b; Merdian et al. 2020; Cohen-Almagor 2013; Interagency Working Group 2019; WePROTECT Global Alliance 2015) examining offending characteristics and etiological factors have proposed models that integrate psychological vulnerabilities and environmental conditions across different regions. Although they advance understanding of perpetrators' motives and intentions, they remain largely explanatory, offering limited insights into dynamic attack patterns on online platforms and into cognitive justifications, especially in African and Asian digital environments, where knowledge of offender motivations remains limited.

Further, multiple studies (Demetis and Kietzmann 2021; Quayle 2020; Cohen-Almagor 2013; Choo et al. 2014; Baines 2019; Council of Europe 2019; Holt et al. 2020; Vold et al. 2002) explored legal frameworks, jurisdictional laws, regulatory challenges, and intervention strategies, emphasizing international cooperation, reporting mechanisms, and technological safeguards such as parental controls. Nonetheless, these approaches often operate at a strategic level with less impact on the integration at the victim's level. This has created a disconnect between policy formulation and implementation in understanding perpetrators' actions. A growing body of the literature highlights how digital transformation and emerging technologies such as social media platforms, AI, and live-streaming services are expanding the attack surface and evolving the threat landscape. These platforms are used to lure victims, which has led to increased accessibility, vulnerabilities, anonymity, and exploitation. Consequently, there have been challenges and limited efforts to formalize these activities into structured threat models that could support proactive detection and prevention. Thus, applying the TTP method could help create stakeholder management awareness, decision-making, and strategic policy formulation. There are several gaps in COSEA incidents and threat actor behaviors across multiple studies (Childlight Global Child Safety Institute 2024; United Nations Office on Drugs and Crime 2020; Espelage and Hong 2017; United Kingdom 2003), ranging from social media exploitation, organized gangs, grooming networks, and cyberbullying. These include live-streaming abuse that perpetrators deploy against victims, such as reconnaissance, social engineering attacks, and password exploits, among others, that have not been analyzed using the established MITRE Framework and TTP methods.

Furthermore, critical gaps in merging highlight the absence of a unified global framework and the adversary's analytical approach to identifying COSEA TTPs, which emphasizes victim impact over attack patterns. Additionally, the existing literature is more focused on descriptive than on technical insights into perpetrators' mindsets, resulting in inadequate integration with threat intelligence methodologies to meet the stakeholder imperative. Considering these cases and existing practices provides the basis for implementing the TTPs that could determine the perpetrators' intents and motives, including

grooming, catfishing, sexting, sextortion, photos, filming, and live-streaming sexually explicit activities of child abuse.

To address this gap, this study adopts a MITRE Kill Chain-inspired analytical approach, reframing COSEA through a cyber threat intelligence lens. By modeling perpetrator behavior in terms of tactics, techniques, and procedures (TTPs), this approach:

- Transforms fragmented observations into a structured, stage-based framework for CTI gatherings.
- Enables systematic analysis of threat actor capability, opportunity, and motive.
- Bridges the gap between a child's behavioral insights and technical security applications.
- Supports all stakeholders in developing proactive detection, disruption, and prevention mechanisms.

Furthermore, grounding this framework in documented case studies allows for empirical validation of TTP patterns, revealing how perpetrators adapt their strategies across platforms and contexts. This shift from a predominantly victim-centric narrative to an adversary-informed model provides a more balanced and actionable understanding of COSEA. The paper explores the various tactics, techniques, and procedures that perpetrators deploy on their victims and how they complicate the child. The rationale is to understand the methods, opportunities, and motives used by perpetrators and provide recommendations to stakeholders to improve security.

3. Approach

This study adopts a structured, adversarial analysis approach to examine Child Online Sexual Exploitation and Abuse (COSEA) by integrating the MITRE ATT&CK framework with a tactics, techniques, and procedures (TTP)-driven methodology. The objective of the study is to systematically identify perpetrator behaviors, infer motives, and support attribution within cyber threat intelligence (CTI) and profiling contexts. Given the evolving threat landscape and expanding digital attack surface, this approach builds on and extends prior research by introducing a formalized adversarial modeling perspective.

3.1. MITRE ATT&CK and TTP-Based Analytical Approach

The MITRE ATT&CK framework provides a continuously evolving, evidence-based taxonomy of adversarial behavior, widely used to analyze intrusion patterns across cyber domains. It enables the decomposition of complex attacks into observable tactics and techniques, supporting threat detection, analysis, and response. Prior work in TTP-based threat hunting demonstrates that structuring data around adversarial behaviors enhances the identification of malicious activity and improves situational awareness (MITRE ATT&CK: Ten Reconnaissance Techniques 2025; Daszczyszak et al. 2019).

In this study, the ATT&CK framework is adapted to the COSEA context to model offender behavior as a sequence of goal-oriented actions. For instance, multiple studies (Whittle et al. 2013; Lefevre et al. 2017; Cohen-Almagor 2013; Palmer and Foley 2017; Baines 2019; Quayle 2016; Radford 2018; WePROTECT Global Alliance 2015) adopted quantitative approaches and methods to address the challenges, using surveys, questionnaires, and interviews to gather data. However, the qualitative method applied relied on subjective expert judgment, opinions, and systematic literature reviews to identify and analyze data.

3.2. Justification of the Subjective Expert Judgment Approach

Subjective expert judgment refers to a decision-making approach in which specialists draw on their knowledge, experience, and informed intuition to evaluate situations, make predictions, or estimate outcomes, particularly in the absence of complete or purely

quantitative data. Given the dynamic and often opaque nature of cyberattacks, alongside the rapidly evolving threat landscape and attack surface, this study adopts an expert-informed approach suited to contexts characterized by uncertainty, ambiguity, and incomplete data, such as cybersecurity, risk assessment, child protection, and emerging technologies.

A qualitative, expert-informed analytical design was employed, and data were derived from the peer-reviewed literature on COSEA, grooming, and cyber-enabled abuse, institutional and law enforcement reports, documented case studies, and incident reports. To ensure methodological rigor, expert-informed assessment was applied to interpret and synthesize the data. This involved systematically identifying recurring behavioral patterns, validating them against the established literature, and mapping them to ATT&CK-aligned TTP categories (MITRE ATT&CK: Ten Reconnaissance Techniques 2025; Daszczyszak et al. 2019; Azeria Labs 2017). Further, our expertise in the areas of cybersecurity and online child protection issues provides the impetus and analytical procedure, which follows four stages:

1. Data Extraction: Identification of relevant behavioral indicators, grooming patterns, and exploitation methods from the literature.
2. TTP Identification: Classification of these behaviors into discrete tactics and techniques based on adversarial intent and function.
3. Stage Mapping: Alignment of identified TTPs with ATT&CK-style adversarial stages.
4. Synthesis and Interpretation: Analysis of relationships between stages to infer attacker motives, capabilities, and operational patterns.

This structured approach ensures transparency, reproducibility, and theoretical grounding in both cybersecurity and socio-behavioral research domains. Specifically, we operationalize TTPs as behavioral indicators derived from documented cases, empirical studies, and qualitative evidence. This enables a transition from predominantly victim-centric analyses to a balanced adversarial perspective. Additionally, (Berelowitz et al. 2013) proposed a framework that used a child-centered approach for preventing Child Sexual Exploitation, including identifying victims, protecting them, providing support, prosecuting, and convicting perpetrators. The qualitative research, multiple researchers (Joleby et al. 2021; Hamilton-Giachritsis et al. 2020; Merdian et al. 2020; Kloess et al. 2017c; Benson and Benson 2005; Kloess et al. 2017a; Williams et al. 2013) explored various approaches to determine how perpetrators deploy multiple attack methods and modus operandi, grooming tactics, and predatory behaviors against victims.

3.3. Mapping COSEA to MITRE ATT&CK-Style Adversarial Stages

This section discusses how TTPs were identified, categorized, and analyzed by mapping COSEA to MITRE ATT&CK-Style adversarial stages to understand the attack methods and adversary behaviors. Although prior work has not explicitly adopted cybersecurity frameworks, the literature and documented case studies collectively reveal patterns that can be mapped to a MITRE ATT&CK Kill Chain-inspired model of the TTP and adversarial behavior:

- Reconnaissance: Offenders identify and profile potential victims through social media, online forums, gaming platforms, and chat environments, leveraging publicly available information and behavioral cues (e.g., vulnerability indicators such as loneliness or identity exploration).
- Resource Development: Perpetrators create fake identities, deploy anonymization tools, and establish communication channels (e.g., aliases, bot accounts, or encrypted messaging platforms) to support their operations.

- Initial Access (Engagement): Contact is initiated through social engineering techniques, including impersonation, flattery, and shared-interest narratives, often via instant messaging, social networks, or gaming platforms.
- Persistence (Relationship Building): Offenders cultivate ongoing relationships through trust-building strategies, emotional manipulation, and reinforcement mechanisms, ensuring continued engagement with the victim.
- Privilege Escalation (Control and Dependency): Psychological leverage is established through tactics such as "love bombing," secrecy enforcement, and normalization of inappropriate interactions, increasing the offender's influence over the victim.
- Execution (Exploitation): Victims are coerced or manipulated into engaging in sexual activities, including sharing explicit content, participating in live-streamed abuse, or facilitating offline encounters.
- Collection and Exfiltration: Exploitative material (e.g., images, videos, personal data) is obtained, stored, and potentially distributed or monetized across networks, including the dark web.
- Command and Control (Coercion and Sextortion): Offenders maintain control through threats, blackmail, or emotional coercion, ensuring continued compliance and preventing disclosure.
- Impact: The consequences include severe psychological harm, long-term trauma, and, in some cases, self-harm or suicide, alongside broader societal and legal implications.

This mapping demonstrates that COSEA perpetration exhibits characteristics analogous to structured cyber adversarial campaigns, involving multi-stage, adaptive, and goal-oriented behaviors.

3.4. Rationale and Contribution of the Approach

The integration of ATT&CK Framework and TTP analysis (MITRE ATT&CK: Ten Reconnaissance Techniques 2025) and the subject-judgment approach provides a novel methodological contribution by enabling systematic modeling of perpetrator behavior rather than isolated incident analysis. It provides analysis and understanding of the threat actor's motives, intents, and purposes (Azeria Labs 2017; Radford 2018; WePROTECT Global Alliance 2015; Benson and Benson 2005; Berelowitz et al. 2013; Kloess et al. 2017b; Barnum 2014). Further, it supports attribution and profiling through behavioral pattern recognition and bridging cyber threat intelligence and socio-psychological perspectives that inform proactive detection, prevention, and policy development.

By modeling COSEA from an adversarial perspective, this study advances understanding of offender strategies, consumer tactics, operational workflows, intents, and exploits used on online platforms. The approach also supports the development of targeted mitigation strategies and stakeholder interventions, including law enforcement, policymakers, and child protection agencies.

3.5. Applicability to Cyber Threat Intelligence

TTP-based modeling provides actionable insights for CTI by linking observed behaviors to adversarial objectives and operational contexts. In COSEA, this facilitates:

- Identification of threat actor patterns across social media platforms;
- Contextualization of incidents for investigative purposes post-incident;
- Development of detection and prevention mechanisms for victims;
- Enhanced information sharing among stakeholders.

In Sections 4.1 and 4.2, we have applied the framework to characterize post-compromise behavior for stakeholder involvement, strategic management imperatives, and refined response measures.

4. Implementation

This section outlines how the MITRE Kill Chain framework and TTP methodology (Section 3.1) are applied using a subjective expert judgment approach to identify how perpetrators exploit victims. Adversaries employ varied strategies depending on victims' levels of vulnerability, experience, and digital awareness (MITRE ATT&CK: Ten Reconnaissance Techniques 2025; Daszczyszak et al. 2019; Azeria Labs 2017). Accordingly, TTP analysis is used to support threat intelligence gathering and to characterize the COSEA threat landscape across multiple platforms. For example, the dark web provides encrypted environments, including forums and chat networks, where illicit activities are conducted. Moreover, Chiang (2020) identified twelve offender strategies based on the analysis of 71 posts from six child abuse forums.

Figure 1 illustrates the range of TTPs used by perpetrators to gain access to victims and execute their objectives within social networking platforms. These perpetrators include online predators and pedophiles, operating either individually or within organized groups. They may assume roles such as groomers and can include individuals known to the victim, such as parents, relatives, peers, teachers, faith leaders, guardians, or sports coaches.

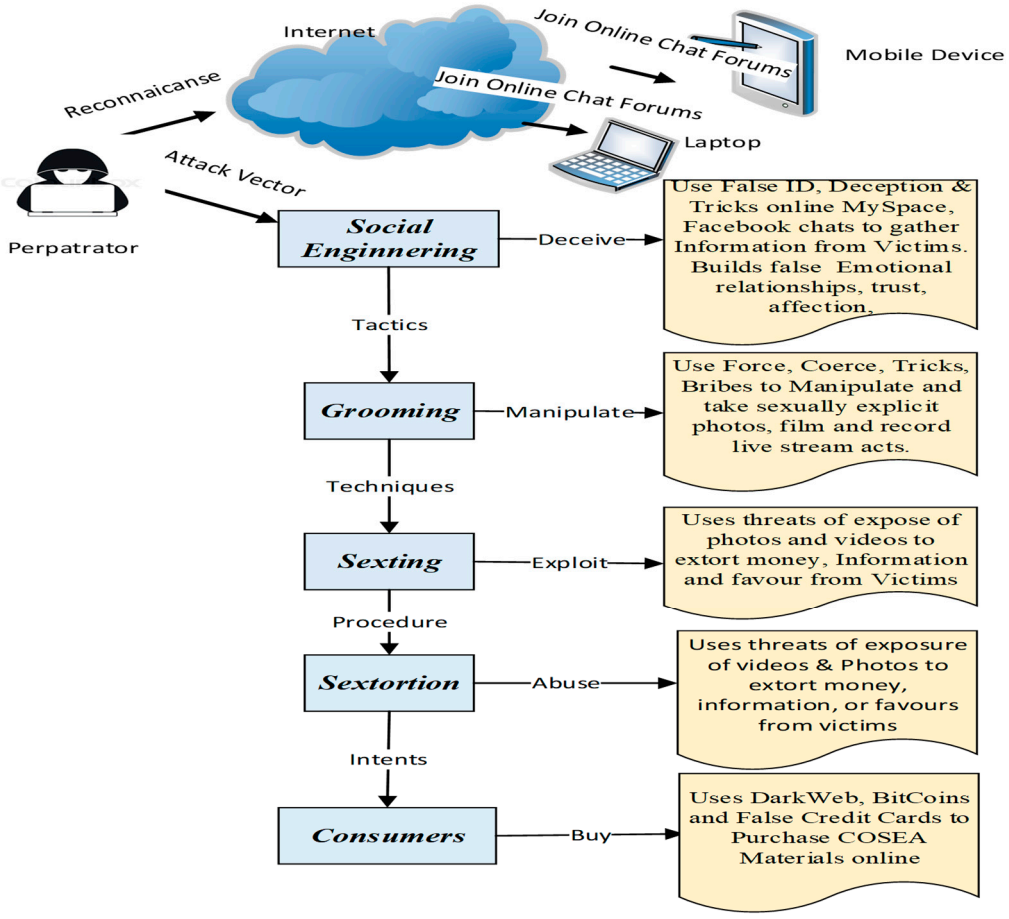

Figure 1. Tactics, techniques, and procedures (TTPs) deployed on children online.

4.1. Tactics, Techniques, and Procedures (TTP) Used by Perpetrators on Victims

Tactics, techniques, and procedures (TTPs) describe approaches for analyzing an APT's operations and profiling a particular threat actor or perpetrator (Azeria Labs 2017; Radford 2018; WePROTECT Global Alliance 2015; Benson and Benson 2005; Berelowitz et al. 2013; Kloess et al. 2017a; Barnum 2014). The perpetrators use the method to orchestrate and exploit their victims. They are patterns of attack activities, methods, and vectors

associated with a specific threat actor or group of threat actors. It provides an understanding of cyber threat intelligence solutions and situational awareness of COSEA threats to stakeholder policy formulation. In addition, it assists in attributing individuals and groups of adversaries, enabling knowledge of their intents and motives.

- **Tactics:** The perpetrator carries out reconnaissance on various social network sites, video game consoles, and online chat forums to identify the victims. Then the threat actor uses a social engineering method to gather information or passwords from victims. The online platforms and live streaming websites include MySpace, Facebook, instant messaging, pop-ups, chat rooms, and other internet forums to identify their victims for possible Child Sexual Exploitation and Abuse. Additionally, threat agents communicate with other agents within a campaign via online tools such as the dark web and Virtual Private Networks (VPNs) to execute attacks and conceal their identities (Azeria Labs 2017; Radford 2018; WePROTECT Global Alliance 2015; Benson and Benson 2005; Berelowitz et al. 2013; Kloess et al. 2017b; Barnum 2014).
- **Techniques:** Do the perpetrators adopt the strategies to facilitate the initial contact with the victim before the exploitation, such as social engineering, online grooming, sexting, sextortion, and other capabilities deployed? For instance, after the adversary establishes contact with the victim online, they may deceive the victim or use force, coercion, bribes, and other persuasive means to induce the victim to personally disclose information that could lead to further exploitation (Azeria Labs 2017; Radford 2018; WePROTECT Global Alliance 2015; Benson and Benson 2005; Berelowitz et al. 2013; Kloess et al. 2017b; Barnum 2014).
- **Procedures:** Include a set of tactics and techniques put together that the adversary uniquely uses to perform an attack. The procedures for each exploitation may vary depending on the nature of the abuse, purpose, and the money involved. A well-orchestrated procedure may not show signs of exploitation or abuse. For instance, the perpetrator may decide to use the internet, a webcam to capture images and film the explicit sexual abuse of the children, and may choose to live stream the abuse to an audience in a private online forum (Azeria Labs 2017; Radford 2018; WePROTECT Global Alliance 2015; Benson and Benson 2005; Berelowitz et al. 2013; Kloess et al. 2017b; Barnum 2014).

4.2. COSEA Attack Steps Deployed by Perpetrators to Exploit Victims Online

The perpetrator adopts the following steps to exploit their victims online, including reconnaissance, social engineering or catfishing, grooming, sexting, sextortion, and consuming, as depicted in Figure 1.

1. Reconnaissance: The perpetrator carries out online searches and visits various online forums to identify which platforms they can join and conceal themselves to identify vulnerable children.
2. Social Engineering or Catfishing: The perpetrator uses a false identity and tricks the child into revealing personal information about themselves and their families.
3. Grooming: Perpetrators use deception to gather intelligence about the child to build emotional relationships, trust, and affection to manipulate, exploit, and abuse the victims later.
4. Sexting: Perpetrators use force, bribes, tricks, and persuasion to get the victims online and into sexually explicit acts. They connect via smartphones with webcams to share sexually explicit photos, images, and live streaming of themselves and the child inappropriately online.

5. Sextortion: Perpetrators use the threat to extort money, information, or sexual favors from their victims by threatening to reveal the sexually explicit activities they have secretly recorded unlawfully on social media.
6. Consumers: They purchase COSEA materials online using false Credit Card details on the dark web and Bitcoins.

5. Discussions on a Child-Centered Approach to COSEA and the Influencing Factors

COSEA and child online protection issues have focused on national and international challenges that require extensive research to ensure adequate protection for victims. The goal is to bring together all victims, parents, experts, government, law enforcement, legislatures, ISPs, industries, academia, and stakeholders to mitigate these issues (Baines 2019). Perpetrators are becoming stealthy and taking advantage of the surge in mobile device usage by children, internet usage, and the digital transformation to exploit and abuse children. The primary reasons behind unreported sexual abuse involve confusion, fear of retaliation, guilt, shame, lack of confidence, religion, and other socio-cultural pressures (Ali et al. 2023).

5.1. Child Online Sexual Exploitation and Abuse (COSEA) Challenges

COSEA issues have been a significant challenge due to the inability to categorize victim characteristics, including children's behaviors, online activities, and content monitoring, among others. Factors that highlight emerging thinking could provide opportunities for education, awareness, attitudinal changes, victim support, and information-sharing platforms (Laws and Hall 2019). Furthermore, psychosocial challenges arising from cultural interrelations among social factors, individual mindsets, and behaviors contribute to the increased COSEA cases. Furthermore, the telecommunication industries and ISPs' irresponsibility in identifying, censoring, preventing, and reporting on the online platforms, apps, websites, and payment methods used by perpetrators has exacerbated exploitation. That has increased the number of offenders who produce the materials. Additionally, the challenge of employing competent staff to identify the TTPs used by cybercriminals is lacking. Gathering threat intelligence, modes of operation, and intent will provide a basis for understanding their motives, such as financial gain, pleasure, extortion, exploitation, or revenge (Chiang 2020). Additionally, dark web studies have also revealed how threat actors get involved in online pedophile communities.

Furthermore, identifying the challenges posed by offenders who consume COSEA materials and the channels they exploit to acquire them is a more significant global concern. Consequently, issues in online child protection do not involve only the arrest and prosecution of perpetrators. It includes providing support, liaison, mitigation, rehabilitation, and counseling to minimize the impact (Rook 2019). Thus, TTPs provide knowledge and understanding of behavioral patterns, motives, intentions, vulnerable social media platforms, marketing platforms, financial benefits, and threat-related issues required to establish intelligence and attributions needed to address COSEA challenges for all stakeholders. Thus, providing cyber threat information-sharing platforms for all stakeholders will foster awareness, collaboration, and reporting. Figure 2 depicts all stakeholders involved in this collaborative process.

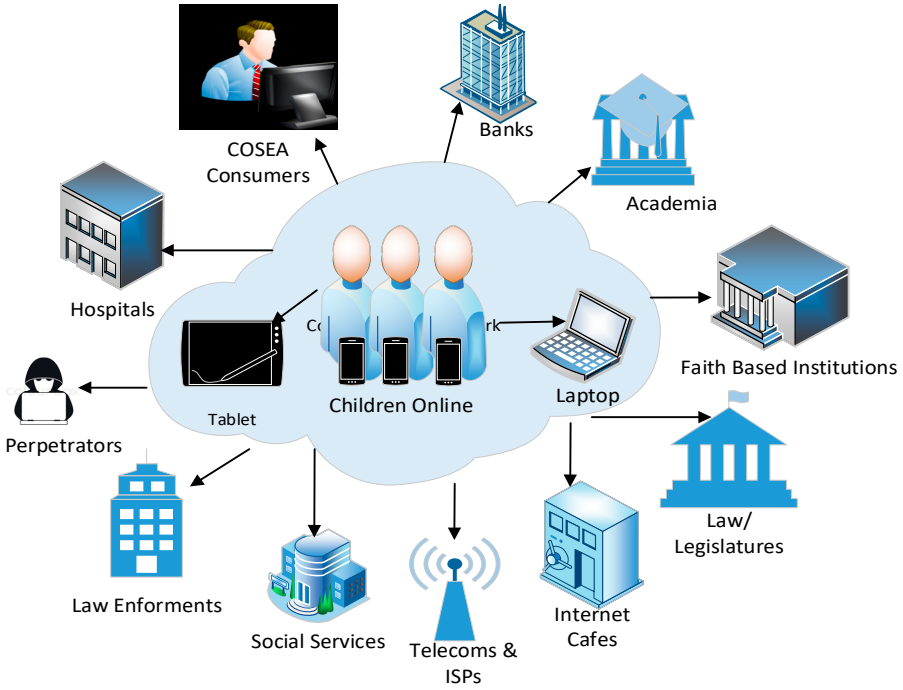

Figure 2. Child-centered approach to factors that influence COSEA challenges.

5.2. Child-Centered Approaches to Factors Influencing COSEA Challenges

Figure 2 presents a child-centered model that situates the child at the core of the COSEA ecosystem, surrounded by interconnected stakeholders, institutions, and digital environments. This includes social services, healthcare systems, educational institutions, financial entities, faith-based organizations, internet service providers (ISPs), law enforcement agencies, regulatory frameworks, and perpetrators.

The section synthesizes key challenges affecting children's well-being and maps them to systemic vulnerabilities.

Child Online: Ensuring child online safety remains a critical challenge. Building trust and awareness among children at risk of exploitation is difficult due to limited digital literacy, inadequate parental supervision, and socio-economic vulnerabilities (Radford et al. n.d.). Grooming strategies such as rapport-building, sexualization, and risk assessment enable offenders to manipulate victims effectively (Williams et al. 2013). Children's vulnerability is further shaped by developmental and contextual factors, including limited ability to distinguish safe from unsafe interactions and fear of disclosure. Behavioral indicators of victimization include withdrawal, secrecy, mood instability, and sudden possession of unexplained items. Cultural stigma and fear of blame may further suppress reporting. These risks contrast with the principles outlined in the Convention on the Rights of the Child (United Nations Human Rights 1989), which emphasizes a safe and supportive developmental environment.

Perpetrators: Perpetrators demonstrate high technical adaptability and exploit digital infrastructures, including social media, encrypted platforms, and anonymization tools (Radford et al. n.d.; Radford 2018). Their operations follow structured patterns involving reconnaissance, targeting, grooming, exploitation, and obfuscation. While existing frameworks emphasize prevention and response strategies (WePROTECT Global Alliance 2015), they often overlook the need to systematically analyze perpetrators' tactics, techniques, and procedures (TTPs). This gap limits the ability to anticipate evolving threats and develop proactive countermeasures.

Consumers: Consumers of COSEA material sustain the ecosystem through financial incentives. Transactions occur via digital payments, mobile money, and other channels,

often under anonymity. Identifying consumers remains difficult due to concealment strategies and the limited integration of financial monitoring across jurisdictions (Holt et al. 2020).

Parents and Guardians: Parental supervision is a critical protective factor. The absence of capable guardianship increases exposure to motivated offenders and accessible targets, consistent with routine activity theory (Vold et al. 2002). Effective interventions include parental education, awareness of online risks, use of privacy controls, and open communication with children. However, gaps in digital literacy and engagement limit the effectiveness of these measures.

Cybercafés and Access Points: Public internet access points expose children to significant risks, particularly in low-resource settings. Lack of content filtering, weak regulatory enforcement, and economic incentives contribute to the availability of harmful material. These environments facilitate accidental or deliberate exposure to exploitative content and interactions.

Social Services: Social services play a central role in safeguarding children, but face challenges in balancing legal, ethical, and emotional considerations (Hallett 2016). Misinterpretation of children's experiences or insufficient sensitivity can undermine intervention efforts. Effective practice requires child-centered, trauma-informed approaches aligned with legal mandates.

Healthcare Systems: Healthcare providers are often first responders in cases of abuse, but face barriers related to confidentiality, legal reporting obligations, and resource limitations. Strengthening reporting protocols and interdisciplinary coordination is essential for timely intervention.

Youth Interventions and NGOs: Youth organizations and NGOs contribute to prevention, awareness, and rehabilitation efforts. However, fragmented initiatives and inconsistent global coordination reduce their overall impact. Strengthening collaboration among international bodies (e.g., UNICEF, WHO, INTERPOL) is critical to addressing cross-border challenges.

Faith-Based Organizations: Faith-based institutions influence community norms and can support awareness and reporting mechanisms. However, limited engagement and insufficient training reduce their effectiveness. Enhancing collaboration with formal safeguarding systems is necessary to improve outcomes.

Education and Awareness: Insufficient education and awareness across schools, communities, and institutions remain a major barrier (Lefevre et al. 2017; ECPAT International 2017). While global initiatives exist, they often lack contextual adaptation and sustained funding. Integrating digital safety education into curricula and community programs is essential.

Telecommunications and ISPs: ISPs and technology providers are key actors in monitoring and mitigating online risks. However, limitations in automated detection tools, digital forensics capabilities, and reporting systems hinder effective intervention. Weak collaboration between industry and law enforcement further exacerbates these gaps.

Financial Institutions: Financial systems could enable or disrupt COSEA activities through transaction monitoring. While there is capacity to detect suspicious transaction flows, their effectiveness is limited by the inadequate coordination with law enforcement. Cross-sector collaboration is required to track and block illicit financial networks.

Law Enforcement: Law enforcement agencies face challenges in investigation, attribution, and prosecution due to anonymization techniques, jurisdictional barriers, and limited technical expertise (Holt et al. 2020). Strengthening cyber forensic capabilities and international cooperation is essential for effective enforcement.

Legal and Regulatory Frameworks: Legal frameworks provide the foundation for combating COSEA, including the Sexual Offences Act 2003 and international conventions (Baines 2019; United Nations Human Rights 1989). However, enforcement gaps, inconsistent interpretation, and limited cross-border coordination reduce their effectiveness.

Existing policies rarely incorporate adversarial TTP analysis, limiting their ability to address evolving threats.

5.3. Limitations of the Study

Across all stakeholders, a key limitation is the insufficient integration of perpetrator-centric threat intelligence. Current approaches emphasize prevention, policy, and victim support but often neglect systematic analysis of attacker behaviors. A coordinated, intelligence-driven approach incorporating TTP analysis, stakeholder collaboration, and enhanced detection capabilities is essential to strengthen prevention, disruption, and response efforts.

The study did not employ quantitative methods, such as surveys or questionnaires, and the authors' lack of psychological expertise may limit insights into children's cognitive and socio-psychological issues. However, the focus on perpetrators' TTPs supports stakeholder awareness, policy development, and knowledge exchange to improve online child safety.

6. Recommendations

Child online exploitation and abuse is a global phenomenon that takes many forms of exploitation of digital media to harm children. Table 1 presents a recommendation matrix that maps key stakeholder collaborations and strategic management initiatives to the roles they could play in mitigating these exploitations and abuses.

Table 1. Strategic management initiatives.

Stakeholders	Roles and Responsibilities	Strategic Management Initiatives
Law and Legislature	National and international laws.	Implement laws that support all stakeholders' initiatives.
Telecom Industries and ISPs	Set standards and directives. Understand the perpetrator's motives and intents.	Implement standards, policies, configuration tools and triggers to detect, report, and prevent.
Law Enforcement Agencies	Employ expertise with an understanding of COSEA threats.	International collaborations and information sharing. Organize training and workshops. Set up forensic labs.
Banks and Financial Institutions	Report on any financial irregularities and transfers	Banks should form coalitions to detect and support international COSEA initiatives.
Internet and Cyber Cafes	Install IDS/IPS, firewalls, and anti-malware to detect sexually explicit materials.	Set up enforcement regulators to monitor cafes. Implement licenses and security policies.
Social Services	Provide social care, education, and support for parents and children.	Organize training and workshops to educate staff and create awareness of risk factors.
Faith-Based leaders	Provide moral and spiritual guidance to children and families in social settings.	Organize forums that foster sensitization, collaboration, corporate partnerships, trust, and reporting platforms.
NGOs and Interventions Groups	Promote awareness and interventions between victims and state institutions.	Liaise with global agencies to promote the well-being of victims.
Academia/Research Institutions	Provide research initiatives in the COSEA subject areas. Train teachers to be aware of risk factors and their impact on children.	Provide funding for research that provides threat intelligence and situational awareness for all stakeholders.
Hospitals	Gather health issues about victims and risk factors	Provide statistics to government institutions with health and risk factors for policy formulation.
Parents and Guardians	Provide parental guidance, protection, and support for children and young persons.	Provide governmental support for social services, hospitals, teachers, faith leaders, and law enforcement agencies to educate parents and guardians.

7. Conclusions

The phenomenon surrounding Child Online Sexual Exploitation and Abuse continues to evolve rapidly globally. The challenges are that COSEA issues are not easily detected. The manifestations and detection of COSEA and its effects require using key psychosocial risk indicators for children to identify and mitigate these cybercrimes. These indicators include the child going missing during school hours, having additional money, having additional mobile devices or phones, exhibiting secretive behaviors and disengaging from friends, irrational behaviors, and sexual health issues, including bleeding and showing signs of distress. Further, competent expertise with knowledge of cybersecurity and digital forensic tools and techniques for the detection and prevention of Child Sexual Exploitation and Abuse materials is required to arrest, prosecute, and deter criminals.

Furthermore, cyber threat intelligence gathering is necessary to provide knowledge, understanding, and situational awareness within the domain. Additionally, the study has used cyberattack tactics, techniques, and procedures (TTPs) to explain the perpetrator's methods, motives, and intentions, as well as the opportunities they exploit. Moreover, the study has identified all key stakeholders, perpetrators, and consumers of COSEA materials, as well as the challenges posed by these cyber threats and their impacts. The paper has explored COSEA challenges, their manifestations, attack settings, and the systems that must address them. Further, we have identified and recommended various roles the governments, civil society, parents, educators, and industries could play in mitigating COSEA challenges. Finally, we have discussed factors that could enforce deterrence and the legal frameworks for prosecution.

Sociodemographic risk factors of COSEA leading to prevalence, including economic, social, cultural, educational, and religious factors, have led to the victimization of the vulnerable child online. Furthermore, limited progress in addressing socio-psychological factors including emotional intelligence deficits, low self-esteem, weak support networks and coping mechanisms, insufficient community awareness programs, and poor stakeholder coordination, has significantly contributed to COSEA. The findings demonstrate that TTP-based analysis enables clearer identification of adversary intent, capability, and opportunity. The study integrates technical, social, and behavioral factors, including economic incentives, societal influences, and deterrence, and provides recommendations for policy, education, and collaborative threat intelligence sharing.

Future works will explore the use of AI algorithms, and models could be used to detect, flag, and block any Child Online Sexual Exploitation and Abuse content before it gets to the consumer.

Author Contributions: Conceptualization, A.Y.-O. and A.A.A.; Title, A.Y.-O.; methodology, A.Y.-O.; validation, A.Y.-O. and A.A.A.; formal analysis, A.Y.-O. and A.A.A.; investigation, A.Y.-O.; research sources, A.Y.-O.; Literature Review A.Y.-O.; writing—original draft preparation, A.Y.-O.; Implementation, A.Y.-O.; writing—review and editing using Grammarly tool, A.Y.-O. and A.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: The study did not require Ethical Approval.

Informed Consent Statement: Not Applicable.

Data Availability Statement: All data were gathered from online secondary sources and search engines, including Google Scholar and repositories.

Acknowledgments: The authors have reviewed and edited the output and take full responsibility for the content of this publication. The authors acknowledge that they both worked on the manuscript. A.Y.-O. and A.A.A. discussed the initial paper. A.Y.-O. carried out the initial research, the

title, introduction, literature review, methodology, implementation, and discussion and recommendations. A.A.A. was also involved in the initial discussion title, reviewed and edited. They both carried out discussions together, worked on the output and took full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

References

Ali, Sana, Hiba Abou Haykal, and Enaam Youssef. 2023. Child sexual abuse and the internet—A systematic review. *Human Arenas* 6: 404–21. https://doi.org/10.1007/s42087-021-00228-9.

Azeria Labs. 2017. Tactics, Techniques, and Procedures (TTPs). Available online: https://azeria-labs.com/tactics-techniques-and-procedures-ttps/ (accessed on 18 April 2025).

Bailey, Jane, Nicola Henry, and Asher Flynn. 2021. Technology-facilitated violence and abuse: International perspectives and experiences. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*; Leeds: Emerald Publishing, pp. 1–17. https://doi.org/10.1108/978-1-83982-848-520211001.

Baines, Victoria. 2019. Council of Europe Baseline Mapping: Building Europe for and with Children. Available online: https://rm.coe.int/191120-baseline-mapping-web-version-3-/168098e109 (accessed on 18 April 2025).

Barnum, Sean. 2014. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information Expression (STIX). Version 1.1. Available online: http://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf (accessed on 18 April 2025).

Benson, Ilene R., and Michael J. Benson. 2005. Challenging online behaviors of youth: Findings from a comparative analysis of young people in the United States and New Zealand. *Social Science Computer Review* 23: 29–38. https://doi.org/10.1177/0894439304271532.

Berelowitz, Sue, Jenny Clifton, Carlene Firmin, Sandra Gulyurtlu, and Gareth Edwards. 2013. *If Only Someone Had Listened: Office of the Children's Com-Missioner's Inquiry into Child Sexual Exploitation in Gangs and Groups*. London: Office of the Children's Commissioner. Available online: https://www.childrenscommissioner.gov.uk (accessed on 18 April 2025).

Brewster, Thomas. 2020. Child exploitation complaints rise 106% to hit 2 million in just one month: Is COVID-19 to blame? *Forbes*, April 24. Available online: https://www.forbes.com/sites/thomasbrewster/2020/04/24/child-exploitation-complaints-rise-106-to-hit-2-million-in-just-one-month-is-covid-19-to-blame (accessed on 18 April 2025).

Chiang, Emily. 2020. *Dark Web: Study Reveals How New Offenders Get Involved in Online Paedophile Communities*. Birmingham: Institute for Forensic Linguistic, Aston University. Available online: https://theconversation.com/dark-web-study-reveals-how-new-offenders-get-involved-in-online-paedophile-communities-131933 (accessed on 18 April 2025).

Childlight Global Child Safety Institute. 2024. Over 300 Million Children a Year Are Victims of Online Sexual Exploitation and Abuse. Available online: https://www.childlight.org/newsroom/over-300-million-children-a-year-are-victims-of-online-sexual-exploitation-and-abuse (accessed on 18 April 2025).

Choi, Kyung-Shick, and Hannarae Lee. 2023. The trend of online child sexual abuse and exploitation: A profile of online sexual offenders and criminal justice response. *Journal of Child Sexual Abuse* 33: 804–23. https://doi.org/10.1080/10538712.2023.2214540.

Choo, Kim-Kwang Raymond, Henry Hillman, and Christopher Hooper. 2014. Online child exploitation: Challenges and future research directions. *Computer Law & Security Review* 30: 687–98. https://doi.org/10.1016/j.clsr.2014.09.007.

Cohen-Almagor, Raphael. 2013. Online child sex offenders: Challenges and countermeasures. *The Howard Journal of Crime and Justice* 52: 190–215. https://doi.org/10.1111/hojo.12006.

Council of Europe. 2019. How Do We Prevent and Combat Online Child Sexual Exploitation and Abuse: Mapping and Comparative Review of Mechanisms for Collective Action. Available online: https://www.coe.int/en/web/children/-/how-do-we-prevent-and-combat-online-child-sexual-exploitation-and-abuse- (accessed on 18 April 2025).

Daszczyszak, Roman, Dan Ellis, Steve Luke, and Sean Whitley. 2019. *MITRE TTP-Based Hunting*. McLean: MITRE. Available online: https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf (accessed on 18 April 2025).

Demetis, Dionysios S., and Jan Kietzmann. 2021. Online child sexual exploitation: A new MIS challenge. *Journal of the Association for Information Systems* 22: 5–40. https://doi.org/10.17705/1jais.00652.

ECPAT International. 2017. *Online Child Sexual Exploitation: A Common Understanding*. Bangkok: ECPAT International.

Espelage, Dorothy L., and Jun Sung Hong. 2017. Cyberbullying prevention and intervention efforts: Current knowledge and future directions. *The Canadian Journal of Psychiatry* 62: 374–80. https://doi.org/10.1177/0706743716684793.

Finkelhor, David, Heather Turner, and Deirdre Colburn. 2022. Prevalence of online sexual offenses against children in the US. *JAMA Network Open* 5: e2234471. https://doi.org/10.1001/jamanetworkopen.2022.34471.

Fry, Deborah, Anna Krzeczkowska, Jingru Ren, Mengyao Lu, and Xiangming Fang. 2025. Prevalence estimates and nature of online child sexual exploitation and abuse: A systematic review and meta-analysis. *Lancet Child Adolesc Health* 9: 184–93. https://doi.org/10.1016/S2352-4642(24)00329-8.

Hallett, Sophie 2016. An uncomfortable comfortableness: Care, child protection and child sexual exploitation. *The British Journal of Social Work* 46: 2137–52.

Hamilton-Giachritsis, Catherine, Elly Hanson, Helen Whittle, Filipa Alves-Costa, and Anthony Beech. 2020. Technology-assisted child sexual abuse in the UK: Young people's views on the impact of online sexual abuse. *Children and Youth Services Review* 119: 105451.

Holt, Thomas J., Jesse Cale, Benoit Leclerc, and Jacqueline Drew. 2020. Assessing the challenges affecting investigative methods to combat online child exploitation material offences. *Aggression and Violent Behavior* 55: 101464. https://doi.org/10.1016/j.avb.2020.101464.

Interagency Working Group. 2019. *Trafficking Definitions for Working Group*. Washington, DC: Interagency Working Group.

Internet Watch Foundation. 2018. Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-Stream Child Sexual Abuse. Available online: https://www.iwf.org.uk (accessed on 18 April 2025).

Ioannou, Maria, John Synnott, Amy Reynolds, and John Pearson. 2018. A comparison of online and offline grooming characteristics: An application of the victim roles model. *Computers in Human Behavior* 85: 291–97. https://doi.org/10.1016/j.chb.2018.04.011.

Joleby, Malin, Sara Landström, Carolina Lunde, and Linda S. Jonsson. 2021. Experiences and psychological health among children exposed to online child sexual abuse—A mixed methods study of court verdicts. *Psychology, Crime & Law* 27: 159–81. https://doi.org/10.1080/1068316X.2020.1781120.

Keller, M. H., and G. J. X. Dance. 2019. Preying on children: The emerging psychology of pedophiles. *New York Times*, September 29. Available online: https://www.nytimes.com/2019/09/29/us/pedophiles-online-sex-abuse.html (accessed on 18 April 2025).

Kloess, Juliane A., Anthony R. Beech, and Leigh Harkins. 2014. Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma Violence Abuse* 15: 126–39. https://doi.org/10.1177/1524838013511543.

Kloess, Juliane A., Catherine E. Hamilton-Giachritsis, and Anthony R. Beech. 2017a. Offence processes of online sexual grooming and abuse of children via internet communication platforms. *Sex Abuse* 31: 73–96. https://doi.org/10.1177/1079063217720927.

Kloess, Juliane A., Jessica Woodhams, Helen Whittle, Tim Grant, and Catherine E. Hamilton-Giachritsis. 2017b. The challenges of identifying and classifying child sexual abuse material. *Sex Abuse* 31: 173–96. https://doi.org/10.1177/1079063217724768.

Kloess, Juliane A., Sarah Seymour-Smith, Catherine E. Hamilton-Giachritsis, Matthew L. Long, David Shipley, and Anthony R. Beech. 2017c. A qualitative analysis of offenders' modus operandi in sexually exploitative interactions with children online. *Sex Abuse* 29: 563–91. https://doi.org/10.1177/1079063215612442.

Laws, Sophie, and Gregory Hall. 2019. Addressing child sexual abuse and exploitation: Improvement in understanding and practice. *Child Abuse Review* 28: 399–404. https://doi.org/10.1002/car.2605.

Lefevre, Michelle, Kristine Hickle, Barry Luckock, and Gillian Ruch. 2017. Building trust with children and young people at risk of child sexual exploitation. *The British Journal of Social Work* 47: 2456–73. https://doi.org/10.1093/bjsw/bcw181.

Longobardi, Claudio, Matteo Angelo Fabris, Laura Elvira Prino, and Michele Settanni. 2021. Online sexual victimization among middle school students: Prevalence and association with online risk behaviors. *International Journal of Developmental Science* 15: 39–46. https://doi.org/10.3233/DEV-200300.

Merdian, Hannah L., Derek E. Perkins, Elspeth Dustagheer, and Emily Glorney. 2020. Development of a case formulation model for individuals involved in child sexual exploitation material. *International Journal of Offender Therapy and Comparative Criminology* 64: 1055–73.

MITRE ATT&CK: Ten Reconnaissance Techniques. 2025. Available online: https://attack.mitre.org/ (accessed on 18 April 2025).

Montiel, Irene, Enrique Carbonell, and Noemí Pereda. 2016. Multiple online victimization of Spanish adolescents: Results from a community sample. *Child Abuse & Neglect* 52: 123–34. https://doi.org/10.1016/j.chiabu.2015.12.005.

Naebklang, Manida. 2014. The Commercial Sexual Exploitation of Children in Africa. ECPAT International: Ghana. Available online: https://www.ecpat.org (accessed on 18 April 2025).

National Police Chiefs' Council. 2024. *Vulnerability Knowledge and Practice Programme (VKPP): National Analysis of Police-Recorded Child Sexual Abuse and Exploitation Crimes Report 2022*. London: National Police Chiefs' Council.

NSPCC. 2020. *What Is Child Sexual Exploitation?* London: NSPCC.

NSPCC. 2024. *Statistics Briefing: Online Harm and Abuse*. London: NSPCC.

NSPCC. 2026. Protecting Children from Sexual Exploitation. Available online: https://learning.nspcc.org.uk/child-abuse-and-neglect/child-sexual-exploitation (accessed on 18 April 2025).

Palmer, Catherine Emma, and Marian Foley. 2017. I have my life back: Recovering from child sexual exploitation. *The British Journal of Social Work* 47: 1094–110. https://doi.org/10.1093/bjsw/bcw020.

Palmer, Tink. 2015. Digital Dangers: The Impact of Technology on the Sexual Abuse and Exploitation of Children and Young Persons. Available online: https://www.celcis.org (accessed on 18 April 2025).

PureSight. 2018. Online Predators Statistics. Available online: https://www.puresight.com/Pedophiles/Online-Predators/online-predators-statistics.html (accessed on 18 April 2025).

Quayle, Ethel. 2016. Researching online sexual exploitation and abuse: Are there links between online and offline vulnerabilities? In *Global Kids Online*. Edinburgh: University of Edinburgh.

Quayle, Ethel. 2020. Prevention, disruption, and deterrence of online child sexual exploitation and abuse. *ERA Forum* 21: 429–47. https://doi.org/10.1007/s12027-020-00625-7.

Radford, Lorraine. 2018. *A Review of International Research on Interpersonal Violence; Centre of Expertise on Child Sexual Abuse*. Preston: University of Central Lancashire. Available online: http://clok.uclan.ac.uk/21733/1/CSA%20international%20survey%20methodology.pdf (accessed on 18 April 2025).

Radford, Lorraine, Susana Corral, Christine Bradley, Helen Fisher, Claire Bassett, Nick Howat and Stephan Collishaw. n.d. *Child Abuse and Neglect in the UK Today*. London: NSPCC. Available online: https://learning.nspcc.org.uk/media/1042/child-abuse-neglect-uk-today-research-report.pdf (accessed on 18 April 2025).

Ramiro, Laurie. S., Andrea B. Martinez, Janelle Rose D. Tan, Kachela Mariano, Gaea Marelle J. Miranda, and Greggy Bautista. 2019. Online child sexual exploitation and abuse: A community diagnosis using social norms theory. *Child Abuse & Neglect* 96: 104080.

Rook, Peter. 2019. *Prosecuting Sexual Offences*. Washington, DC: JUSTICE. Available online: https://files.justice.org.uk/wp-content/uploads/2019/06/06170149/Prosecuting-Sexual-Offences-Report.pdf (accessed on 18 April 2025).

Salter, Michael, and Elly Hanson. 2021. "I need you all to understand how pervasive this issue is": User efforts to regulate child sexual offending on social media. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*; Edited by Jane Bailey, Asher Flynn and Nicola Henry. Leeds: Emerald Publishing Limited, pp. 729–48. https://doi.org/10.1108/978-1-83982-848-520211053.

Sivagurunathan, Marudan, Treena Orchard, Joy C. MacDermid and Marilyn Evans. 2019. Barriers to Utilization of Mental Health Services amongst Male Child Sexual Abuse Survivors: Service Providers' Perspective. *Journal of Child Sexual Abuse* 28: 819–39. https://doi.org/10.1080/10538712.2019.1610823.

Tunagur, Mustafa Tolga, Hatice Oksal, Ömer Büber, Elif M. Kurt Tunagur, and Enes Sarıgedik. 2025. Risk factors and predictors of penetrative online child sexual abuse. *Journal of Pediatric Health Care* 39: 198–205. https://doi.org/10.1016/j.pedhc.2024.10.002.

United Kingdom. 2003. Sexual Offences Act 2003. Available online: https://www.legislation.gov.uk/ukpga/2003/42/pdfs/ukpga_20030042_en.pdf (accessed on 18 April 2025).

United Nations Human Rights. 1989. Convention on the Rights of the Child. Available online: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx (accessed on 18 April 2025).

United Nations Office on Drugs and Crime. 2020. Online Child Sexual Exploitation and Abuse: Promoting a Culture of Lawfulness. Available online: https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html (accessed on 18 April 2025).

Vold, George Brian, Thomas J. Bernard, and Jeffrey B. Snipes. 2002. *Theoretical Criminology*. Oxford: Oxford University Press.

WePROTECT Global Alliance. 2015. Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response. Available online: https://www.weprotect.org/the-model-national-response/ (accessed on 18 April 2025).

WePROTECT Global Alliance. 2020. *Impact of COVID-19 on Child Sexual Exploitation*. London: WePROTECT Global Alliance.

WePROTECT Global Alliance. 2024. World's First Estimate of the Scale of Online Child Sexual Exploitation and Abuse. Available online: https://www.weprotect.org/blog/worlds-first-estimate-of-the-scale-of-online-child-sexual-exploitation-and-abuse (accessed on 18 April 2025).

Westendorf, Jasmine-Kim, and Louise Searle. 2017. Sexual exploitation and abuse in peace operations. *International Affairs* 93: 365–87. https://doi.org/10.1093/ia/iix001.

Whittle, Helen, Catherine Hamilton-Giachritsis, Anthony R. Beech, and Guy Collings. 2013. A review of young people's vulnerabilities to online grooming. *Aggression and Violent Behavior* 18: 135–46.

Williams, Rebecca, Ian A. Elliott, and Anthony R. Beech. 2013. Identifying sexual grooming themes used by internet sex offenders. *Deviant Behavior* 34: 135–52. https://doi.org/10.1080/01639625.2012.707550.

Wurtele, Sandy K. 2009. Preventing sexual abuse of children in the twenty-first century: Preparing for challenges and opportunities. *Journal of Child Sexual Abuse* 18: 1–18. https://doi.org/10.1080/10538710802584650.