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

Abel Yeboah-Ofori * and Awo Aidam Amenyah

Posted Date: 13 January 2026

doi: 10.20944/preprints202601.0975.v1

Keywords: child abuse; online child sexual exploitation; tactics techniques and procedures; child online protection; child safety; cyber attacks; cyber threat intelligence

 doi:10.20944/preprints202601.0975.v1



*Article*

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

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

[1] University of West London, UK

[2] Child Online Africa, Ghana

* Correspondence: abel.yeboah-ofori@uwl.ac.uk

**Abstract**

Background: Child sexual exploitation and abuse have been an existing global phenomenon. However, with increasing dependency on digital transformation, mobile devices, and the internet, the emphasis has shifted to child online sexual exploitation and abuse (COSEA), leading to an exponential growth of perpetrators. A 2020 report indicated a 200% increase in child sex abuse forums that are linked to the internet. Existing literature has emphasized child protection challenges, online attacks, and using surveys and questionnaires to gather and draw inferences regarding grooming tactics and thematic analysis. Social Issues, such as the lack of reporting platforms, limited sharing of threat information, cyber awareness, and social engagement and support, pose serious challenges for children, parents, and law enforcement. Several papers exist that have used the term Online Child Sexual Exploitation and Abuse (OCSEA). However, our paper considers Child Online Sexual Exploitation and Abuse (COSEA) as we explore and look at it from the challenges of a child going online and accessing the internet. Methods: The paper explores COSEA challenges and examines how perpetrators deploy MITRE Tactics, Techniques, and Procedures (TTPs) against victims to understand attack motives and establish potential attributions for cyber threat intelligence gathering and cyber profiling. The paper acknowledges existing research by considering the changing threat landscape and the evolving attack surface. It aims to contribute to the body of knowledge on adversarial TTPs and current trends, and to understand the threat actor's mindset and motives. Results: The results demonstrate that analyzing TTPs facilitates the establishment of attributions and the determination of the adversary's intents, motives, opportunities, and methods. The novelty contributions of this research are threefold. First, we explore existing challenges in online child abuse and exploitation by identifying and discussing what constitutes child abuse and exploitation, how COSEA manifests, and the attack methods used by perpetrators to exploit their victims. Secondly, we used the MITRE TTP and subjective judgment approach to identify the TTPs and determine how these factors make the child complicit. Finally, we discuss the strategies required to address the challenges and the stakeholder role in mitigating COSEA. Conclusion: The paper has considered TTPs from a technical perspective to understand the perpetrator's motives. The paper considers factors that could influence the victim, such as money, societal norms, and deterrence, including education, laws, regulations, and recommendations for threat information-sharing platforms and collaborations among stakeholders.

**Keywords:** child abuse: online child sexual exploitation: tactics techniques and procedures; child online protection; child safety; cyber attacks; cyber threat intelligence

## 1. Introduction

Child online sexual exploitation and abuse (COSEA) has increased exponentially due to current trends in digital transformation, and the phenomenal growth in the use of the internet, social media,

 doi:10.20944/preprints202601.0975.v1



and mobile devices [1–4]. These advancements in digital device usage and internet access have brought with them various online abuse, exploitation, and grooming techniques, leading to sexual exploitation [5] and technology-assisted child sexual abuse cases [6]. Child sexual exploitation has been in existence for some time now, with a global impact on vulnerable children [7–10]. Further, [11] highlights the digital dangers and the impact of the technology being used for child exploitation materials to sexually abuse children and young people. Several research studies exist that have used the term Online Child Sexual Exploitation and Abuse (OCSEA). However, assessing the challenges driving COSEA and how they affect investigation methods to mitigate threats is crucial, given the evolving threat landscape and attack surface. There are differences between COSEA AND OCSEA in how they are discussed and their significance from a child safety perspective. For instance, Online Child Sexual Exploitation and Abuse (OCSEA) considers a specific child who may actively access the internet for online activities that could be profiled with particular accounts, online presence, and digital identities, and could be targeted for exploitation and abuse. Fry et al. [12] discussed the prevalence of OCSEA, how it has increased victimization rates, and has been a primary global health concern for researchers, children's rights activists, practitioners, policy makers, governmental institutions, and law enforcement agencies, as reports of violence against children have existed for years. It emphasizes a child as a user who participates in online gaming websites, chat forums, social media, and other digital environments. In the context of identifying child online privacy, profiling, and interactions, OCSEA could provide personal information about online activity and identity that could allow perpetrators to target victims, exploit, and abuse them. Child Online Sexual Exploitation and Abuse (COSEA) considered how children in general access the internet and interact using mobile devices, computers, and the various online and social media networks from all aspects, as well as how it affects them and impacts their well-being. These children could be addicted to online activities and could be exposed to online social engineering, cyberbullying, and online grooming without safety awareness. Perpetrators target vulnerable children who may not realize they are victims, thereby lowering the probability of the victims reporting to the authorities [64]. The victims of COSEA usually come from low-income families [13] as sexual abuse and exploitation involve forcing or persuading a child or young person under the age of 18 years to engage in sexual activities, on the internet, whether or not the child is aware of what is happening. Whereas, child online sexual exploitation involves using various extortion methods such as money, coercion, and enticements to exploit the child or young person, leading to online grooming, production, dissemination, and possession of sexually explicit materials [5,14].

This paper considers the title Child Online Sexual Exploitation and Abuse (COSEA) as we explore it from the challenges of a child going online and accessing the internet, the attack methods used by perpetrators, the risks involved, and recommends child safety and security controls for stakeholders' awareness.

### *1.1. Increased Use of Smartphones Among Children*

There has been a significant increase in the use of mobile devices among children, with many of them having smartphones and an active online presence. Further, it has simplified the process of online child crimes and the distribution of online child exploitation materials. According to an Ofcom 2024 report, the online safety regulator, 99% of children in the UK spend time online.

- 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 eight and 17 have their own account or profile on at least one of the large platforms.
- Despite most platforms having a minimum age of 13, six in 10 children aged 8 to 12 who use them have signed up with their own 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.

 doi:10.20944/preprints202601.0975.v1



There is a blurred boundary between the lives children lead online and the 'real world. Several concerns have been raised regarding the effects of child sexual exploitation [15] and its social, psychological, physical, economic, mental, and sexual health issues. That has greatly impacted parents and the victims in their later lives, leading to drug abuse and self-harm. Cybercriminals deploy various tactics, techniques, and procedures to penetrate, manipulate, exploit, and abuse children online using multiple media such as MySpace, Facebook, instant messaging, chat rooms, Snapchat, webcams, and other dark web links. The challenges faced by vulnerable young children visiting these online chat forums have been exacerbated by how sexualized, digitized, and commodified they are to their own sexual choices and boundaries. The more children feel that their rights and safety have not been recognized or respected, the more vulnerable they become and the more likely they are to distrust those around them, thereby turning to online platforms [16].

Existing studies considered child-centered approaches to evaluate child sexual exploitation and attacks [15,17–20]. Further, [14,21] explored online challenges for victims and the impact of child sex offenders. However, the increasing use of mobile devices, network penetration, and internet access has exponentially increased COSEA attacks. The effects of the COVID-19 pandemic further exacerbated the challenges, leading to a spiral in COSEA. [22] compared online and offline grooming characteristics and considered the application of the victim roles model to explore grooming characteristics. Perpetrators usually use manipulative strategies to expose children to such abuses. [1] postulate that negative pressures are exerted on victims, including threats, bribes, or nagging and deceitful and flattering words to act as a friend or expression of love. For instance, WeProtect (2020), a global alliance intelligence brief on the impact of COVID-19 on online child sexual exploitation, reported a 200% increase in post-known child sexual abuse forums and downloads between February and March 2020 [23]. Approximately 95% of children between the ages of 12 and 17 years have online access, with one in five admitting that they have received unwanted sexual solicitation via a web link, with the targets being mainly between 11 and 15 years [24]. In the USA, the National Center for Missing & Exploited Children (NCMEC) has registered a 106% increase and risen from 983,734 reports in March 2019 to 2,027,520 in suspected child sexual exploitation [25]. A New York Times 2019 report indicated that technology companies reported a record 45 million online child abuse images were flagged, with some as young as 3-4 years old [24].

Factors leading to increased COSEA include more children being active online due to increased social networking usage, including visiting sexually explicit websites, accessing sexting and pornography websites. Other challenges include internet-based grooming and shaping sexual content for interest [1–3,22]. Some factors contributing to COSEA challenges include increased use of mobile devices, higher bandwidth and data speeds, and affordable internet services and access at home. COSEA involves using mobile devices and the internet as a medium by perpetrators to exploit and abuse their victims sexually. Children could be tricked or lured, use live streaming to film sexual acts, and sometimes have casual sex acts such as sexting online, then coerced to send or post these sexually explicit images of themselves [26]. For instance, IWF 2017 reported on the online distribution and capture of live streams of 2,082 videos. The report indicated that 96% depicted children using devices independently, 98% were children below 13 years old, and 96% were girls, with 73% of the images appearing on chat forums, pop-ups, advertisements, and downloads. Other detection challenges are that the perpetrator could be an individual who may be an online predator, an online pedophile, or an organized group (gang) that uses the dark web to encrypt their websites to prevent detection of their online forums and conceal their activities [4]. According to the CHILDLIGHT report 2024, a global child safety institute, over 300 million children a year are victims of technology-facilitated sexual exploitation and abuse, including online solicitation, non-consensual taking, sharing, and exposure to sexual images and videos, online sexual exploitation, and sexual extortion [27]. A report by NSPCC (2024) highlighted that the latest research by Ofcom (2024) indicates that the internet is increasingly part of children's lives, with 84% of 3-to-4-year-olds in the UK going online. The proportion rises to 100% for children aged 12 years and over [28]. Key findings from the data show that:

 doi:10.20944/preprints202601.0975.v1



- 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 9,000 child sexual abuse offences involved an online element in 2022/23.
- Around a sixth of people who experienced online harassment offences were under 18 years old.
- Under 18-year-olds were the subject of around a quarter of reported offences of online blackmail in England, Wales, and Northern Ireland.

Further, Finkelhor et al. [29] highlighted some finding 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%, nonconsensual 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 300 million plus children under the age of 18 have been affected by online child sexual exploitation and abuse in the last 12 months [30]. 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 [31]:

- There were around 107,000 offences 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 offences relate to sexual crimes committed directly against children, and around 25% relate to online offences 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 offences. 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 contact 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 offences 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 and concerning trends involve a wide range of abuse, coercion, extortion, and other forms of offending. The report highlights that some include exploratory online sexual behaviors, while some of the most prevalent abuses include sexual assaults, including rape. Perpetrators use pseudonymity and various blackmail, tricks, interactions, persuasions, intimidations, extortions, bribes, and violent means to coerce the children into these acts. [4,5,32]. Perpetrators use cybercrime tactics, techniques, and procedures (TTP) such as social engineering, online grooming, deception, sexting, extortion, and live streaming using webcams over the internet to capture videos and images of children [5]. Additionally, COSEA methods used on children are generally through an invitation to parties, gifts, drugs, giving them alcohol, and paying poor parents to allow their children to be exploited. For instance, a study shows that 75% of children are willing to share their personal information online about themselves and their families in exchange for goods and services [33].

This paper explores COSEA challenges and examines how perpetrators deploy MITRE Tactics, Techniques, and Procedures (TTPs) against victims to understand threat actors' motives and establish potential attributions for cyber threat intelligence gathering and cyber profiling. Considering the

 doi:10.20944/preprints202601.0975.v1



changing threat landscape and the evolving attack surface, the paper acknowledges existing research. It aims to contribute to the body of knowledge on adversarial TTPs, current trends, and the threat actor's mindset and motives. The novelty contributions of this research are threefold. First, we explore existing challenges in online child abuse and exploitation by identifying and discussing what constitutes child abuse and exploitation, how COSEA manifests, and the attack methods used by perpetrators to exploit their victims. Secondly, we used the MITRE Framework and a subjective judgment approach to identify the TTPs and determine how these factors impact victims and make them complicit. Finally, we discuss the strategies required to address the challenges and the stakeholders' role in mitigating the COSEA challenges. The results show that analyzing TTPs helps establish attributions and determine the adversary's intents, motives, opportunities, and methods. The papers consider TTPs from a technical perspective to understand the perpetrator's motives. The paper considers factors that could influence the victim, such as money, societal norms, and deterrence, including education, laws, regulations, and recommendations for threat information-sharing platforms and collaborations among stakeholders.

## 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 impacts children, parents, society, law enforcement, organizations, and legal frameworks, requiring extensive research to curb their proliferation. Fry et al. [12] 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, [6] 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, [34] 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, [35] 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, [20] presented an argument that centered around the role of technology in the prevention and changing of the environment that supports disruption and deterrence of online child sexual exploitation and abuse. Lefevre et al. [15] 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. [1] 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, [14] explored the modus operandis of offenders by analyzing their sexually exploitative interactions with children online, including discursive tactics. Demetis & Kietzmann [18] 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. The paper discussed the role information systems play in detecting online CSE, but not from perpetrators or TTPs. Whittle et al. [2] 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

 doi:10.20944/preprints202601.0975.v1



al. [38] 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. [19] 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. [3] reviewed current knowledge and understanding of the OCSE process, prevalence, and offending characteristics of grooming and exploitation of children on the internet. Cohen-Alm [21] explored various online child sex offense challenges on victims, their impact, and recommendations for countermeasures. Regarding abusive behaviors on children, [17] considered how different forms of sexually exploitative and abusive behaviors are perpetrated at peacekeeping missions and the risk factors. Kloess et al. [14] 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. [39,40] 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, [41] surveyed global kids' online child sexual exploitation and abuse. Further, [42] 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, [43] 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 sexual exploitation and abusive acts on children online, the UNODC [32] considers COSEA as sexual acts on children where the perpetrators use an exchange of some sort, such as food, affection, drugs, and shelter, to lure and deceive the child. The Interagency Working Group [26] 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, [51] 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 [44] posits that no single state can prevent and combat online child exploitation and abuse alone. Additionally, [45] 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 contribute 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, [52] analyzed various sexually exploitative interactions between offenders and victims on online platforms. However, the threat landscape and the attack surface keep changing, allowing threat actors to change their mode of 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

 doi:10.20944/preprints202601.0975.v1



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 [27]. Thus, the rationale for this paper is to use the qualitative (TTP) attack method to understand the perpetrator's motive, 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 [32]. In the UK, a group of perpetrators were charged and convicted (R v. Costi 2006) under the Sexual Offences Act (2003) [47]. 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 [32]. In the USA, Megan Meier committed 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 [46]. 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 [32].

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. 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 section discusses our approach to addressing the COSEA issues and the rationale for adopting the MITRE TTP method for the study. The purpose of the study is to add to the body of knowledge for identifying potential attributions for cyber threat intelligence gathering and cyber profiling. Considering the evolving threat landscape and attack surface, the paper acknowledges all existing research. It aims to contribute to the existing body of knowledge of understanding the adversarial TTPs, current trends, and the threat actor's mindset and motives. A growing body of evidence from industry, MITRE TTP-Based Hunting and MITRE ATT&CK, and government experimentation confirms that collecting and filtering data based on knowledge of adversary tactics, techniques, and procedures (TTPs) is an effective method for detecting malicious activity [48][49]. Our work considers the MITRE ATT&CK Kill Chain Framework, reconnaissance concepts [48], and TTP concepts [50] for our implementation techniques to exploit the victims. The ATT&CK knowledge base serves as a foundation for developing specific threat models and methodologies.

There are several existing pieces of literature that have used both quantitative and qualitative approaches to identify, analyze, and evaluate COSEA challenges. For instance, [2,15,21,34,40,41,51,52] adopted the quantitative approach and methods to address the challenges, including surveys, questionnaires, and interviews to gather data. Meanwhile, qualitative methods relied on subjective expert judgment, opinions, and systematic literature reviews to identify and analyze data. Additionally, [54] 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. Regarding qualitative research, [1,6,19,36,53,55,59] explored various

 doi:10.20944/preprints202601.0975.v1



approaches to determine how perpetrators deploy multiple attack methods and modus operandi, grooming tactics, and predatory behaviors against victims.

The paper considers the MITRE Kill Chain Framework [48] and a subject-judgment approach to identify the tactics, techniques, and procedures deployed by perpetrators against victims online. It provides analysis and understanding of the threat actor's motives, intents, and purposes [50][56]. Modelling COSEA threats from the attacker's perspective is a proactive approach to understanding and raising awareness of an adversary's goals, modes of operation, and deployed TTPs [50]. The rationale is to understand the perpetrator's methods and intentions, and to use that understanding to educate stakeholders. Further, the paper proposes recommendations for mitigating and managing such cyber threats. To ensure the applicability of our work, we identify how perpetrators deploy TTPs, exploit victims, use online platforms, employ consumer tactics, detect, and implement control mechanisms. TTPs related to a COSEA incident assist in establishing potential attribution and an attack context in a cyber threat intelligence gathering environment and drive research and responses.

## 4. Implementation

This section explores how the TTP method is implemented from a subjective judgment perspective and identifies perpetrators' approaches to exploiting their victims. Adversaries use different strategies on victims depending on their levels of experience and expertise [48–50]. Thus, the TTP is used to gather threat intelligence and understand the COSEA threat landscape and the various platforms. For instance, the dark web is an encrypted network of social networks and chat forums where illegal activities are carried out unsolicited. Further, [57] proposed 12 different approaches used by offenders after analyzing 71 posts from six child abuse forums.

Figure 1 discusses the various TTP methods that perpetrators deploy on their victims. The perpetrators include the predators and paedophiles who could be the gang leaders and individuals operating independently. In addition, they are sometimes used as groomers, and they could be parents, friends, family members, teachers, faith group leaders, guardians, or sports coaches.

### *4.1. Tactic Techniques and Procedures (TTP) Used by Perpetrators on Victims*

Tactic Techniques and Procedures (TTP) describe the approaches of analyzing an APT's operations and how it is used as a means of profiling a particular threat actor or perpetrator [50,56]. The perpetrators use TTPs to orchestrate and exploit their victims. TTPs are patterns of attack activities, methods, and vectors associated with a specific threat actor or group of threat actors. TTPs provide an understanding of cyber threat intelligence solutions and situational awareness of COSEA threats to all stakeholders. In addition, TTPs assist 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 in a campaign using online tools such as the Dark Web and Virtual Private Networks (VPNs) to leverage attacks and conceal their identities [50][56].
- **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 go on to deceive the victim or use force, coercion, bribes, and other persuasive means to trick the victim into personally divulging information that could lead to further exploitation [50,56].

 doi:10.20944/preprints202601.0975.v1

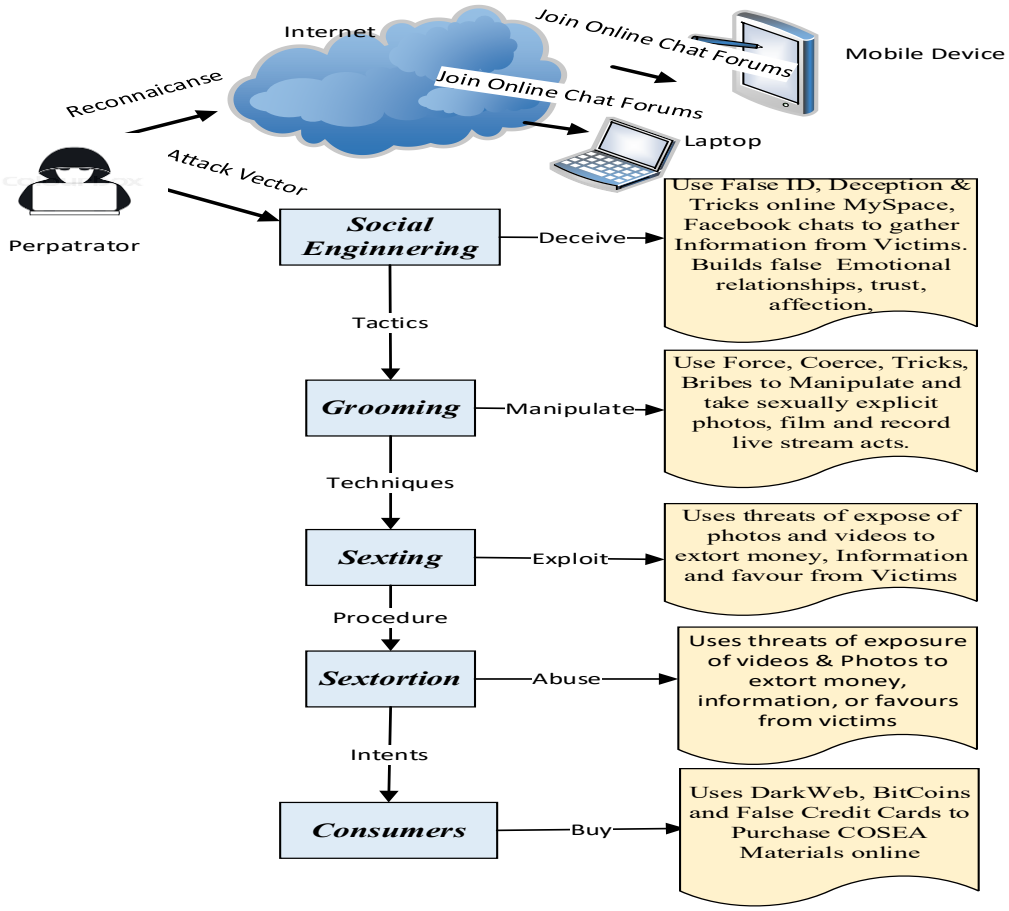


- **Procedures:** include a set of tactics and techniques put together that the adversary uniquely uses to perform an attack. The procedures for each exploitation may vary depending on the nature of the abuse, purpose, and the money involved. A well-orchestrated procedure may not show any sign of exploitation or abuse. For instance, the perpetrator may decide to use the internet, a webcam to capture images and film the explicit sexual abuses on the children, and may choose to live stream the abuses to an audience in a private online forum [50,56].

*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 and 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 favours 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.



 doi:10.20944/preprints202601.0975.v1



**Figure 1.** Tactics, Techniques & Procedures (TTPs) Deployed on Children Online.

## 5. Discussions on Child-Centred 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 [40]. 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 [60].

### *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 [39]. Further, psychosocial challenges related to cultural interrelations among social factors, individual mindsets, and behaviors increase COSEA cases. Furthermore, the irresponsibility of the telecommunications industry and ISPs in identifying, censoring, preventing, and reporting the online platforms, apps, websites, and payment methods used by perpetrators has further 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, mode of operations, and intents will provide a basis for understanding their motives, such as financial gain, pleasure, extortion, exploitation, or revenge [57]. 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 use to acquire them poses a more significant threat globally. Consequently, the issues of online child protection do not only involve arresting and prosecuting perpetrators. It includes providing support, liaison, mitigations, rehabilitation, and counselling to minimize the impact [58]. Thus, TTPs offer knowledge and understanding of the patterns of behavior, motives, intents, vulnerable social media platforms, marketing platforms, financial benefits, and threat-related issues required to establish intelligence and attributions needed to address COSEA challenges by 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.

 doi:10.20944/preprints202601.0975.v1



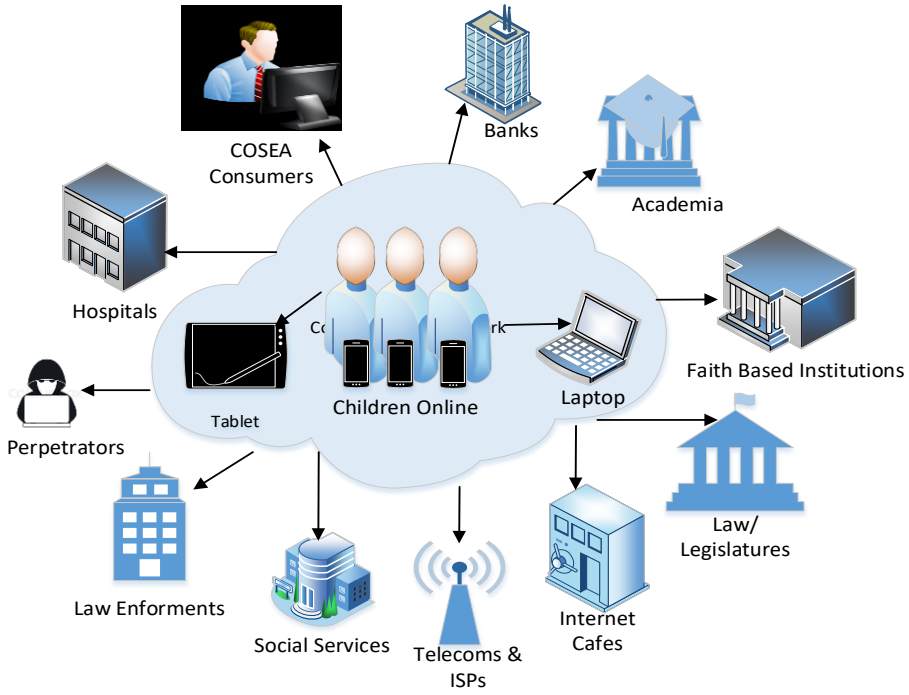



**Figure 2.** Child-Centred Approach to Factors that Influence COSEA Challenges.

*5.2. Child-Centred Approaches to Factors that Influence COSEA Challenges*

Figure 2 discusses the various stakeholder issues related to using a child-centred approach and the factors that influence COSEA challenges by placing the child in the middle, with the multiple devices they use to access online materials. Then the child is surrounded online by various entities, institutions, and stakeholders. That includes social services, hospitals, educating children, banks, faith-based institutions, internet cafes, telecommunications and ISPs, laws and legislatures, parental control, academia, law enforcement, perpetrators, and COSEA consumers. We consider the various challenges that impact the children's well-being as follows.

**Child Online:** Addressing online child safety has become imperative. However, identifying the various child-centred approaches and factors that could create awareness and build trust with children and young persons at risk of being sexually exploited and abused is a challenging issue [35]. Further, the psychological impact it has on the victims and their families cannot be overemphasized. William et al. (2012) [59] used thematic analysis to identify three themes used by internet sex offenders in sexual grooming methods, including Rapport-building, Sexual Content, and Assessment to detect adults posing as children. Other challenges that need to be addressed include providing the right environment for the child and monitoring their access to online activities. For instance, in the Universal Declaration of Human Rights Act 1989, the United Nations states that the child should be able to grow up in a family environment, in an atmosphere of happiness, love, and understanding, in particular in the spirit of peace, dignity, tolerance, freedom, equality, and solidarity [UNHR 1989 REF] [61]. However, the child is always vulnerable due to a lack of awareness, a lack of parental care, poverty, fear of being abused by peers, and a lack of trust in people around them.

Common factors that show signs of exploitation and abuse among children include behavioral changes such as mood swings, withdrawal from family and friends, locking themselves up in a room, anxiety, changing passwords often to hide their screens and conversations, and having new gifts and secret discussions with unknown persons. In some settings, cultural factors may prevent the child from saying anything about any abuse that they may be experiencing to avoid the fear of being judged wrongly and sometimes being beaten by older people. Thus, they might choose to hide their phones and online activities.

- **Perpetrators:** The perpetrators are more IT savvy and understand their cultural demographics and target groups (Radford et al., 2011) (Radford et al., 2018) [35][51]. They know the domains,

 doi:10.20944/preprints202601.0975.v1



search engines, dark web, deep web, digital currencies, cloud, and social media platforms used to target victims. In addition, the perpetrator can use anonymized software and end-to-end encryption to cover their tracks. Thus, they can pseudonymize themselves, carry out reconnaissance, target their victims using social media, groom, exploit, and abuse using webcams to film and take pictures, and cover their tracks. WeProtect Global Alliance [52], proposed a six stage model for national response to critical elements for protecting children including, Legislation and Policy Frameworks to address OCEA, Prevention Strategies required to raise awareness, Equip Law Enforcement agencies with the necessary skills to carry out investigations, Collaborations with Private Sector to implement safety measures, Data Collection and Research to inform policy decisions and information sharing, and finally Victim Support Services for the victims and families [52]. However, implementing this model will be challenging as it does not address the key issues of understanding the methods, opportunities, and motives of the perpetrators and the TTPs they deploy on their victims.

- **Consumers:** Consumers are mainly users of COSEA materials. They are willing to pay a lot of money to the perpetrators, parents, third-party agencies, and individuals for these sexually explicit materials. The methods used to exchange money include Mobile Money, Credit cards, online transfers, cash, and others. Thus, the consumer could be ordinary individuals, faith leaders, teachers, groups, or young people. Identifying consumers of these sexually explicit materials has been one of the significant challenges, as they use threats and secrecy to maintain anonymity [62].
- **Parents and Guardians:** Parental guidance provides a safeguarding environment for children and young persons, especially during online activities. Several approaches emphasize how illegal activities lead to direct contact with predatory COSEA cybercrimes. These are motivated offenders, suitable targets, and a capable guardian's absence to prevent these cybercrimes [63]. First, provide parents with education on the risks, dangers, and impact of COSEA on children. The awareness will help parents have open discussions about the risks of visiting certain websites. How it may impact their wellbeing, talk to their children about online safety, set time limits, and help them make better online and offline choices. Organizing Training and workshops for parents will orient them to the mobile device's safety features and to how to monitor and use parental controls to safeguard their children and detect any signs of exploitation or abuse. Further, the parents will know the importance of using strong passwords and how to set them, restrict device privacy settings so that apps cannot access them, and turn off webcams and geolocation on the devices. Those awareness forums will create trust among parents and authorities and provide information-sharing and reporting platforms.
- **Cyber or Internet Cafes:** Cyber or Internet cafes provide fast internet facilities and computers for users who may not have smartphones, tablets, and laptops at their disposal due to financial challenges. Most children and young people are not taken to or picked up from school at a certain age, as considered grown-ups, and most of their parents may be working by the time they leave school. These children go to cybercafés after school, pay, and access the internet, making them vulnerable to perpetrators. The victims end up accessing pornographic materials on websites and chat forums, clicking on pop-ups that take the victims to exploitative websites, and watching sexually explicit cartoons and videos. The cybercafé owners may be aware of the dangers of exposing these young children to these websites. However, they depend on the payments from these children and young persons, or victims, to keep their business going. That has caused the various disparities between the cybercafé owners, regulatory bodies, and law enforcement agencies in censoring the cybercafé owners who are not installing, configuring, filtering, and blocking these sexually explicit materials exposed to the victims. Inadequate enforcement has caused many challenges, as most are aware of the dangers but have looked the other way for economic and business reasons.
- **Social Services:** The social services institutions have the overall responsibility of overseeing the well-being of children and parents in terms of providing support, education, and awareness of

 doi:10.20944/preprints202601.0975.v1



the issues of COSEA. Identifying what is required to avoid forming any preconceptions regarding the child's feelings is essential [16]. For instance, social care practitioners in the UK need to make legal and ethical decisions to ensure the child's well-being and safeguarding online, in line with the legal frameworks under Section 17 of the Children's Act 1989. The challenge of promoting the child's welfare and protection, including not being sensitive to their feelings and emotions, can prove counterproductive.

- **Hospitals:** The hospitals are one of the key places victims will visit after experiencing any form of exploitation and abuse. Thus, legal institutions could help establish appropriate channels for medical practitioners and health workers to report such cases. However, these health workers may encounter legal and ethical challenges, including data protection and patient confidentiality.
- **Youth Intervention Groups and NGOs:** Child online sexual exploitation and abuse have been recognized globally as a significant factor impacting children's mental and physical health. Other factors include socio-psychological, socio-sexual, and socio-religious well-being, and the risk of getting involved in crime and drugs to fund such behaviors. Thus, bringing together the youth intervention groups to brainstorm and discuss the various COSEA issues on how to detect, intervene, mitigate, and promote COSEA awareness is paramount in eradicating the challenges with young people at risk. In addition, there are Non-governmental organizations (NGOs) and other organizations such as UNICEF, UNESCO, WHO, and INTERPOL that can assist in promoting awareness.
- **Faith-Based Organizations and Religious Leaders:** Society thrives on faith-based communities, religious leaders, and activists for advocacy, moral guidance, spiritual strength, advice, growth, a strong moral compass, and social well-being. Parents and families entrust their children to these faith-based and religious leaders with absolute confidence that their children's lives are in safe hands. Faith-based organizations and religious leaders can assist in information sharing and mitigating child online exploitation and abuse with authorities. However, history has shown that this has not been the case, as these religious leaders are not well-engaged in the fight to understand the risks and consequences of COSEA. Faith-based and religious leaders require education, awareness, detection mechanisms, and support from national and international organizations to spearhead the fight against COSEA and offer safety for victims. There has to be effective national and international collaboration, cooperation, and coordination of resources with UNICEF, UNODC, WHO, and UNESCO, as well as with faith-based leaders, to protect victims. Society should look up to these religious leaders and report any exploitations, abuses, and stigma on the victims.
- **Education and Awareness:** The inadequate amount of education and awareness on the issues of COSEA in most nations and cultures, schools, among teachers, faith-based activities, the media, and research institutions are significant factors [15]. Currently, ongoing projects spearheaded by these empowerment initiatives, in collaboration with UNICEF, NGOs, and governmental agencies, have not brought together all nations to fight COSEA cybercrime [42]. There is minimal effort in providing research funding for the subject area. COSEA issues, although internationally acclaimed, are more jurisdictional and cultural, depending on how each society thinks and does things. Thus, the emphasis must be placed not only on funding for other continents but also on local context and expert judgment. Children's rights to be heard and educated regarding the use and abuse of the internet are not adhered to and prioritized.
- **Telecommunications Industries and Internet Service Providers (ISPs):** The telecommunications industries and ISPs provide internet access to all users, including MSN, Facebook, Instagram, and other social networking sites. Therefore, they can provide tools to monitor, detect, and manage any online child activities. However, technological and different approaches used for detection, intervention, and interception have significantly protected children online. Factors such as a lack of cybersecurity tools configured to detect cyber threats and child online activities automatically, and to block these behaviors, are not available to most

 doi:10.20944/preprints202601.0975.v1



ISPs, law enforcement agencies, mobile users, and victims at large. Moreover, there is inadequate government support, a lack of expertise in the subject area, and inadequate digital forensics investigators, laboratories, and tools to investigate such cybercrime cases. That includes identifying steganography materials, image analysis, and identifying activity patterns. Lack of reporting platforms and fear of intimidation by offenders have also prevented intelligence gathering. These have led to increased COSEA vulnerabilities, exploits, abuse, and obfuscation.

- **Banks and Financial Institutions:** Banks and other financial institutions have a significant role in monitoring and reporting any illegal and suspicious financial activities online. These industries are out to make money, and their existence depends mainly on financial sustainability. However, the need to bring together the various credit card companies to understand the impact of COSEA, the socio-economic factors, and the socio-psychological effects on children and society is pertinent. Further, the banking industry could form a coalition with the mobile money industry and law enforcement agencies to identify these transactions, block the activities, and share information to track the trails of perpetrators and consumers.
- **Law Enforcement Agencies:** The law enforcement agencies have a significant role to play in arresting, investigating, and sending perpetrators to court for prosecuting COSEA crimes. That requires better cooperation among law enforcement agencies, NGOs, and industry for strategic planning and safety awareness. Further, inadequate coordination among national and international law enforcement agencies, financial institutions, ISPs, and social services has heightened COSEA, especially in forensic investigations [62]. Furthermore, there has been inadequate cooperation among the agencies and victims in reporting and combating these cyberthreats as perpetrators use aliases and pseudonymization techniques to trick the victims, groom them online and offline, and obfuscate to prevent arrest and prosecution. Moreover, law enforcement agencies need a legal framework that provides clear legal ramifications to support their roles and responsibilities in implementing, enforcing, arresting, and investigating online child exploitation. Lack of expertise is also a significant factor in the gathering of cyber threat intelligence and in digital forensic investigations.
- **Laws and Regulatory Frameworks:** Laws and Regulatory frameworks exist nationally and internationally regarding COSEA [63]. For instance, the UK Online Safety Act 2023 requires social media companies to quickly remove any illegal content, such as child sexual abuse material and grooming, or prevent it from appearing online. To prevent children from accessing harmful content online, including content that encourages, promotes, or provides instructions for suicide, self-harm, eating disorders, bullying, and violent content. To use or configure age-checking mechanisms and measures to prevent children's access to pornographic material and other age-inappropriate content. However, implementing these laws and legislature has proved challenging due to inadequate enforcement mechanisms, poor interpretations of the laws, and a lack of collaboration among law enforcement agencies and the courts [40]. Some efforts have been made to combat COSEA, and some controls have been implemented to address the issues. For instance, the CoE Lanzarote [21][44] and the African Charter on the Rights and Welfare of the Child provide comprehensive benchmarks that highlight the need to address COSEA. In addition, WeProject and the ECPTA International organized an annual human capacity-building workshop on child online safety in Malawi in 2016 to create awareness of child online exploitation. Legal frameworks such as the Convention on the Rights of the Child. Cyber Security & Personal Data Protection (2014) provides regulatory measures. However, all these efforts from the various countries lack coordination, coalitions, and corporations that consider the perpetrators' tactics, techniques, and procedures to exploit and abuse children online. Hence, the increase in child online exploitation and abuse challenges has led to the need for regular child online safety initiatives.

We trust that by establishing these collaborations with all the stakeholders to discuss the various strategic initiatives, understand the TTPs of perpetrators, threat intelligence gathering, implement safety mechanisms, create awareness, that will assist in proper threat information sharing,

 doi:10.20944/preprints202601.0975.v1



monitoring, and detection mechanisms, child safety initiatives, improve laws and regulatory controls, and educate victims and stakeholders at large.

## 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 provides a recommendation matrix that maps key stakeholder collaborations and strategic management initiatives, along with 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 & International Laws | Implement laws that supports all stakeholders' initiatives |
| Telecom Industries & ISPs | Set Standards and Directives. Understand Perpetrator motives ad intents. | Implement standards, policies, configuration tools & triggers to detect, report and prevent. |
| Law Enforcement Agencies | Employ expertise with understanding of COSEA threats | International Collaborations & Information sharing, Organize Training & Workshops. Set up forensic labs. |
| Banks & Financial Institutions | Report any financial irregularities and transfers | Banks Form Coalitions to detect and support international COSEA initiatives |
| Internet & Cyber Cafes | Install IDS/IPS, Firewalls and Anti malwares to detect sexually explicit materials | Sep up enforcement regulators to monitor cafes. Implement licenses and security policies |
| Social Services | Provide Social Care, Education, and support parents and children. | Organize Training & Workshops to educate staff and create awareness of risk factors |
| Faith Based leaders | Provide Moral & Spiritual Guidance to children and families in social settings | Organize Forums that brings sensitizations, collaborations, corporations, trust and reporting platforms. |
| NGOs & Interventions Groups | Promote awareness and interventions between victims and state institutions | Liaise with global agencies to promote the wellbeing of victims |
| Academia/Research Institutions | Provide Research Initiatives in the COSEA subject areas. Train teachers to be aware of risk factors and impact on children | Provide funding for research that provide threat intelligence and situational awareness for all stakeholders |

 doi:10.20944/preprints202601.0975.v1



| | | |
|---|---|---|
| Hospitals | Gather health issues pertaining to victims and risk factors | Provide statistics to Government institutions with health and risk factors for policy formulation |
| Parents & 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 gatherings are necessary to provide knowledge, understanding, and situational awareness to the domain. Additionally, the study has used cyberattack tactics, techniques, and procedures (TTPs) to explain the perpetrator's methods, motive, 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, how they manifest, attack settings, and the systems that must address these issues. 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.

Future works will explore the use of AI algorithms and models to detect, flag, and block any child online sexual exploitation and abuse before it gets to the consumer.

**Acknowledgments:** The authors have reviewed and edited the output and take full responsibility for the content of this publication.

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

## References

1. M. Joleby, S. Landström, C. Lunde, and L. S. Jonsson, "Experiences and psychological health among children exposed to online child sexual abuse – A mixed methods study of court verdicts," *Psychology, Crime & Law*, pp. 1–23, 2021, doi:10.1080/1068316X.2020.1781120.
2. H. Whittle, C. Hamilton-Giachritsis, A. R. Beech, and G. Collings, "A review of young people's vulnerabilities to online grooming," *Aggression and Violent Behavior*, vol. 18, pp. 135–146, 2013.
3. J. A. Kloess, A. R. Beech, and L. Harkins, "Online child sexual exploitation: prevalence, process, and offender characteristics," *Trauma, Violence & Abuse*, vol. 15, no. 2, pp. 126–139, Apr. 2014, doi:10.1177/1524838013511543.
4. Internet Watch Foundation, "Trends in online child sexual exploitations: Examining the distributions of captures of live-stream child sexual abuse," 2018. [Online]. Available: https://www.iwf.org.uk

 doi:10.20944/preprints202601.0975.v1




5. NSPCC, "What is child sexual exploitation?" 2020. [Online]. Available: https://www.nspcc.org.uk/what-is-child-abuse/types-of-/child-sexual-exploitation/
6. C. Hamilton-Giachritsis, E. Hanson, H. Whittle, F. Alves-Costa, and A. Beech, "Technology-assisted child sexual abuse in the UK: Young people's views on the impact of online sexual abuse," *Children and Youth Services Review*, vol. 119, p. 105451, 2020, doi:10.1016/j.childyouth.2020.105451.
7. J. A. Kloess, C. E. Hamilton-Giachritsis, and A. R. Beech, "Offence processes of online sexual grooming and abuse of children via internet communication platforms," *Sexual Abuse*, vol. 31, no. 1, pp. 73–96, 2019.
8. M. Sivagurunathan, T. Orchard, and M. Evans, "Barriers to utilisation of mental health services amongst male child sexual abuse survivors: Service providers' perspective," *Journal of Child Sexual Abuse*, 2019, doi:10.1080/10538712.2019.1610823.
9. S. A. Wurtele, "Preventing sexual abuse of children in the twenty-first century: Preparing for challenges and opportunities," *Journal of Child Sexual Abuse*, vol. 18, no. 1, 2009. [Online]. https://www.tandfonline.com/doi/abs/10.1080/10538710802584650
10. M. Naebklang, *The Commercial Sexual Exploitation of Children in Africa*. Ghana: ECPAT International, 2014. [Online]. Available: https://www.ecpat.org/wp-content/uploads/2016/04/Regional%20CSEC%20Overview_Africa.pdf (accessed Apr. 18, 2025).
11. T. Palmer, *Digital Dangers. The Impact of Technology on the Sexual Abuse and Exploitation of Children and Young Persons*. Barnardo's, 2015. [Online]. Availahttps://www.celcis.org/files/5715/4871/8578/Barnardos_2015_Digital_Dangers_The_impact_of_technology_on_the_sexual_abuse_and_exploitation_of_children_and_young_people.pdf
12. D. Fry, A. Krzeczkowska, J. Ren, M. Lu, X. Fang, and the Into the Light Index Study Group, "Prevalence estimates and nature of online child sexual exploitation and abuse: a systematic review and meta-analysis," *Lancet Child & Adolescent Health*, vol. 9, no. 3, pp. 184–193, Mar. 2025, doi:10.1016/S2352-4642(24)00329-8.
13. L. S. Ramiro, A. B. Martinez, J. R. D. Tan, K. Mariano, G. M. J. Miranda, and G. Bautista, "Online child sexual exploitation and abuse: A community diagnosis using the social norms theory," *Child Abuse & Neglect*, vol. 96, p. 104080, 2019.
14. J. A. Kloess, J. Woodhams, H. Whittle, T. Grant, and C. E. Hamilton-Giachritsis, "The challenges of identifying and classifying child sexual abuse material," *Sexual Abuse*, 2017, doi:10.1177/1079063217724768.
15. M. Lefevre, K. Hickle, K. Luckock, and G. Ruch, "Build trust with children and young people at risk of child sexual exploitation: The professional challenge," *British Journal of Social Work*, vol. 47, pp. 2456–2473, 2017, doi:10.1093/bjsw/bcw181.
16. S. Hallett, "'An Uncomfortable Comfortableness': 'Care', child protection and child sexual exploitation," *British Journal of Social Work*, vol. 46, no. 7, pp. 2137–2152, Oct. 2016, doi:10.1093/bjsw/bcv136.
17. J.-K. Westendorf and L. Searle, "Sexual exploitation and abuse in peace operations: trends, policy responses and future directions," *International Affairs*, vol. 93, no. 2, pp. 365–387, Mar. 1, 2017, doi:10.1093/ia/iix001.
18. D. S. Demetris and J. Kietzmann, "Online child sexual exploitation: a new MIS challenge," *Journal of the Association for Information Systems*, vol. 22, no. 1, pp. 5–40, 2021, doi:10.17705/1jais.00652.
19. H. L. Merdian, D. E. Perkins, E. Dustagheer, and E. Glorney, "Development of a case formulation model for individuals who have viewed, distributed, and/or shared child sexual exploitation material," *International Journal of Offender Therapy and Comparative Criminology*, vol. 64, no. 10–11, pp. 1055–1073, doi:10.1177/0306624X17748067.
20. E. Quayle, "Prevention, disruption and deterrence of online child sexual exploitation and abuse," *ERA Forum*, vol. 21, pp. 429–447, 2020, doi:10.1007/s12027-020-00625-7.
21. R. Cohen-Almagor, "Online child sex offenders: Challenges and countermeasures," *The Howard Journal of Criminal Justice*, 2013, doi:10.1111/hojo 12006.
22. M. Ioannou, J. Synnott, A. Reynolds, and J. Pearson, "A comparison of online and offline grooming characteristics: An application of the victim roles model," *Computers in Human Behavior*, vol. 85, pp. 291–297, 2018, doi:10.1016/j.chb.2018.04.011.

 doi:10.20944/preprints202601.0975.v1




23. WeProtect Intelligence Brief, "Impact of COVID-19 on child sexual exploitation," Global Alliance Intelligence Brief, 2020. [Online]. Available: https://www.alliancecpha.org/en/system/tdf/library/attachments/impactofcovid-19ononlinechildsexualexploitation.pdf?file=1&type=node&id=38359.
24. M. H. Keller and G. J. X. Dance, "Preying on children: The emerging psychology of pedophiles," *The New York Times*, Sept. 29, 2019. [Online]. Available: https://www.nytimes.com/2019/09/29/us/pedophiles-online-sex-abuse.html
25. T. Brewster, "Child exploitation complaints rise 106% to hit 2 million in just one month: Is COVID-19 to blame," *Forbes*, Apr. 24, 2020. [Online]. Available: 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/#6e8116d54c9c
26. Interagency Working Group, "Trafficking definitions for working group," 2019. [Online]. https://www.ispcan.org/wp-content/uploads/2019/11/Trafficking-definitions-for-working-group-merged.pdf
27. CHILDLIGHT Global Child Safety Institute, 2024. [Online]. Available: https://www.childlight.org/newsroom/over-300-million-children-a-year-are-victims-of-online-sexual-exploitation-and-abuse.
28. NSPCC, "Statistics briefing: Online harm and abuse," OFCOM, 2024. [Online]. Available: https://learning.nspcc.org.uk/media/obfg0phz/online-harm-and-abuse-statistics-briefing.pdf
29. D. Finkelhor, H. Turner, and D. Colburn, "Prevalence of online sexual offenses against children in the US," *JAMA Network Open*, vol. 5, no. 10, p. e2234471, Oct. 3, 2022, doi:10.1001/jamanetworkopen.2022.34471.
30. WeProtect Global Alliance, "World's first estimate of the scale of online child sexual exploitation and abuse," 2024. [Online]. Available: https://www.weprotect.org/blog/worlds-first-estimate-of-the-scale-of-online-child-sexual-exploitation-and-abuse/
31. National Police Chiefs' Council, "Vulnerability Knowledge and Practice Programme (VKPP): National analysis of police-recorded child sexual abuse and exploitation crimes report 2022," 2024. [Online]. Available: https://news.npcc.police.uk/releases/vkpp-launch-national-analysis-of-police-recorded-child-sexual-abuse-and-exploitation-csae-crimes-report-2022
32. UN Office on Drugs and Crime, "Online child sexual exploitations and abuses: Promoting a culture of lawfulness," 2020. [Online]. Available: https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html
33. PureSight Online Child Safety, "Online predators statistics," 2018. [Online]. Available: https://www.puresight.com/Pedophiles/Online-Predators/online-predators-statistics.html
34. E. Palmer and M. Foley, "'I have my life back': Recovering from child sexual exploitation," *British Journal of Social Work*, vol. 47, no. 4, pp. 1094–1110, 2017, doi:10.1093/bjsw/bcw020.
35. L. Radford, S. Bradley, C. Fisher, H. Bassett, C. Howat, N. Collishaw, and C. Carol, "Child abuse and neglect in the UK today," NSPCC, London, 2011. [Online]. Available: https://learning.nspcc.org.uk/media/1042/child-abuse-neglect-uk-today-research-report.pdf
36. J. A. Kloess, S. Seymour-Smith, C. E. Hamilton-Giachritsis, M. L. Long, D. Shipley, and A. R. Beech, "A qualitative analysis of offenders' modus operandi in sexually exploitative interactions with children online," *Sexual Abuse*, vol. 29, no. 6, pp. 563–591, 2017.
37. D. S. Demetris and J. Kietzmann, "Online child sexual exploitation: a new MIS challenge," *Journal of the Association for Information Systems*, vol. 22, no. 1, pp. 5–40, 2021, doi:10.17705/1jais.00652.
38. K. K. R. Choo, K. R. Choo, H. Hillman, and C. Hooper, "Online child exploitation: challenges and future research directions," *Computer Law and Security Review*, vol. 30, no. 6, pp. 687–698, 2014, doi:10.1016/j.clsr.2014.09.007.
39. S. Laws and G. Hall, "Addressing child sexual abuse and exploitation: Improvement in understanding and practice," *Child Abuse Review*, vol. 28, pp. 399–404, 2019, doi:10.1002/car.2605.
40. V. Baines, "Council of Europe baseline mapping: Building Europe for and with children," 2019. [Online]. Available: https://rm.coe.int/191120-baseline-mapping-web-version-3-/168098e109

 doi:10.20944/preprints202601.0975.v1




41. E. Quayle, "Researching online sexual exploitations and abuse: Are there links between online and offline vulnerabilities?" *Kids Global Online*, University of Edinburgh, 2016. https://www.research.ed.ac.uk/portal/files/59858120/Guide_7_Child_sexual_exploitation_and_abuse_Quayle.pdf
42. ECPAT, "Online child sexual exploitation: A common understanding," 2017. [Online]. http://www.ecpat.org/wp-content/uploads/2017/05/SECO-Booklet_ebook-1.pdf
43. M. Salter and E. Hanson, "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* (J. Bailey, A. Flynn, and N. Henry, Eds.), Bingley: Emerald Publishing, pp. 729–748, 2021, doi:10.1108/978-1-83982-848-520211053.
44. Council of Europe, "How do we prevent and combat online child sexual exploitation and abuse: New Council of Europe mapping and comparative review of mechanisms for collective action," 2019. [Online]. Available: https://www.coe.int/en/web/children/-/how-do-we-prevent-and-combat-online-child-sexual-exploitation-and-abuse-
45. J. Bailey, N. Henry, and A. Flynn, "Technology-facilitated violence and abuse: International perspectives and experiences," in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (J. Bailey, A. Flynn, and N. Henry, Eds.), Bingley: Emerald Publishing, pp. 1–17, 2021, doi:10.1108/978-1-83982-848-520211001.
46. D. L. Espelage and J. S. Hong, "Cyberbullying prevention and intervention efforts: Current knowledge and future directions," *Canadian Journal of Psychiatry*, vol. 62, no. 6, pp. 374–380, Jun. 2017, doi:10.1177/0706743716684793.
47. Sexual Offences Act 2003, United Kingdom, 2003. [Online]. Available: https://www.legislation.gov.uk/ukpga/2003/42/pdfs/ukpga_20030042_en.pdf
48. MITRE, *ATT&CK: Ten reconnaissance techniques*, 2025. https://attack.mitre.org/
49. R. Daszczyszak, D. Ellis, S. Luke, and S. Whitley, "MITRE TTP-based hunting," MITRE, 2019. https://www.mitre.org/sites/default/files/2021-11/prs-19-3892-ttp-based-hunting.pdf
50. Azeria Labs, "Tactics, techniques and procedures (TTPs)," 2017. [Online]. Available: https://azeria-labs.com/tactics-techniques-and-procedures-ttps/
51. L. Radford, *A review of international research on interpersonal violence*, Centre of Expertise on Child Sexual Abuse, University of Central Lancashire, Barbados, Essex, 2018. http://clok.uclan.ac.uk/21733/1/CSA%20international%20survey%20methodology.pdf
52. WeProtect, "Preventing and tackling child sexual exploitation and abuse (CSEA): A model national response," 2015. https://www.weprotect.org/the-model-national-response/
53. I. R. Benson and M. J. Benson, "Challenging online behaviours of youth: Findings from a comparative analysis of young people in the United States and New Zealand," *Social Science Computer Review*, vol. 23, no. 1, pp. 29–38, Spring 2005, doi:10.1177/0894439304271532.
54. S. Berelowitz, J. Clifton, C. Firmin, S. Gulyurtlu, and G. Edwards, *If only someone had listened: Office of the Children's Commissioner's inquiry into child sexual exploitation in gangs and groups: Final report*. London: Office of the Children's Commissioner, 2013. https://www.childrenscommissioner.gov.uk/wpcontent/uploads/2017/07/If_only_someone_had_listened.pdf
55. J. A. Kloess, S. Seymour-Smith, C. E. Hamilton-Giachritsis, M. L. Long, D. Shipley, and A. R. Beech, "A qualitative analysis of offenders' modus operandi in sexually exploitative interactions with children online," *Sexual Abuse*, vol. 29, no. 6, pp. 563–591, 2015, doi:10.1177/1079063215612442.
56. S. Barnum, "Standardizing cyber threat intelligence information with the structured threat information expression (STIX), v1.1, revision 1," 2014. [Online]. Available: http://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf
57. E. Chiang, "Dark web: Study reveals how new offenders get involved in online paedophile communities," Institute for Forensic Linguistics, Aston University, 2020. [Online]. Available: https://theconversation.com/dark-web-study-reveals-how-new-offenders-get-involved-in-online-paedophile-communities-131933

 doi:10.20944/preprints202601.0975.v1




58. P. Rook, *Prosecuting sexual offences*. JUSTICE, 2019. [Online]. Available: https://files.justice.org.uk/wp-content/uploads/2019/06/06170149/Prosecuting-Sexual-Offences-Report.pdf
59. R. Williams, I. A. Elliott, and A. R. Beech, "Identifying sexual grooming themes used by internet sex offenders," *Deviant Behavior*, vol. 34, pp. 135–152, 2013, doi:10.1080/01639625.2012.707550.
60. S. Ali, H. A. Haykal, and E. Youssef, "Child sexual abuse and the internet—A systematic review," *Human Arenas*, vol. 6, pp. 404–421, 2023, doi:10.1007/s42087-021-00228-9.
61. United Nations Human Rights, *Convention on the rights of the child*, 1989. [Online]. Available: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx
62. T. J. Holt, J. Cale, B. Leclerc, and J. Drew, "Assessing the challenges affecting the investigative methods to combat online child exploitation material offences," *Aggression and Violent Behavior*, British Journal of Social Work, vol. 55, p. 101464, 2020, doi:10.1016/j.avb.2020.101464.
63. G. B. Vold, T. J. Bernard, and J. B. Snipes, *Theoretical Criminology*, New York: Oxford University Press, 2002. http://www.ncjrs.gov/App/publications/abstract.aspx?ID=175350.
64. Choi, K. S., & Lee, H. (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*(6), 804–823. https://doi.org/10.1080/10538712.2023.2214540.
65. Quayle, E. Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum* 21, 429–447 (2020). https://doi.org/10.1007/s12027-020-00625-7.