Psychology and Behavioral Sciences
2026, Vol. 15, No. 1, pp. 11–20
https://doi.org/10.11648/j.pbs.20261501.12

Research Article

Digital Defenses: Effective Strategies for Responding to Online Child Sexual Abuse and Exploitation Zimbabwe

Daniel Masungwa[1], Livingson Moyo[2,*], Tafadzwa Zulu[3], Dorcas T Hove[3], Nyaradzo Mhizha[3], Elsie Whacha[4], Abel Bohwasi[3], Ketty Chirangwanda[2]

[1]Department of Social Work, Great Zimbabwe University, Masvingo, Zimbabwe
[2]Department of Social Work and Applied Psychology, Zimbabwe Ezekiel Guti University (ZEGU), Bindura, Zimbabwe
[3]Department of Social Work, Reformed Church University, Masvingo, Zimbabwe
[4]Department of Social Work, Midlands State University, Gweru, Zimbabwe

Abstract

The rapid expansion of digital technologies has fundamentally transformed children's social environments, creating new and complex risks for online child sexual abuse and exploitation (CSA). This systematic literature review examines effective strategies for preventing and responding to online CSA, with particular attention to low- and middle-income contexts, including Zimbabwe. Drawing on peer-reviewed research, international policy documents, and grey literature published between 2010 and 2024, the review synthesises evidence on pathways to exploitation, risk factors, prevention approaches, law enforcement responses, and survivor support mechanisms. Guided by PRISMA principles, the study employs a thematic synthesis to identify recurring patterns and systemic gaps across global and regional literature. Findings indicate that online CSA is most commonly facilitated through grooming on social media, messaging platforms, gaming environments, and livestreaming services, often exploiting children's emotional vulnerabilities, limited digital literacy, and unsupervised internet access. Structural risk factors—such as poverty, caregiver absence, disability, and weak child protection systems—further heighten vulnerability in the Global South. Preventive education and digital literacy initiatives are shown to be effective when embedded within broader child protection frameworks and supported by parental and institutional engagement. However, access to such programmes remains uneven. Law enforcement responses benefit from specialized cybercrime units and technological tools, yet significant capacity gaps persist in resource-constrained settings. Survivor support systems emerge as the least developed component, with limited access to trauma-informed, long-term psychosocial and legal services. The review underscores the necessity of integrated, multisectoral, and child-centered responses that combine prevention, enforcement, and survivor care. Strengthening national coordination mechanisms and equitable international collaboration is critical to building sustainable digital protection systems and ensuring safer online environments for children.

Keywords

Online Safety, Child Protection, Cybercrime, Digital Literacy, Sexual Abuse

*Correspondence: Livingson Moyo (livingsonmoyo@gmail.com)

Received: 15 April 2026; **Accepted:** 24 April 2026; **Published:** 8 May 2026

1. Introduction and Background

The rapid digitisation of societies has fundamentally transformed the social, educational, and developmental environments in which children grow. Digital technologies now play a central role in children's learning, communication, entertainment, and identity formation. While these developments present unprecedented opportunities for social inclusion and access to information, they have simultaneously generated new risks, particularly in relation to online child sexual abuse and exploitation (CSA). Online CSA encompasses a broad spectrum of harmful practices, including sexual grooming, coercive sexual solicitation, exposure to sexually explicit material, live-streamed sexual abuse, sextortion, and the creation, distribution, and consumption of child sexual abuse material (CSAM) [1]. In contrast to what is typically thought of as 'offline' abuse, the same anonymity (such as anonymity), and ability of abusers to operate in almost all geographical jurisdictions against very little risk of being caught for such crimes as are facilitated through the anonymous, rapid-growth capabilities of the Internet. These technologies now have directly contributed to where we see the significant levels of online abuse of children occurring [2].

Due to the complexity and variety of challenges faced by child protective services on a global scale, cooperation and coordination between governments is essential to address the growing number of children being abducted and abused via the internet. Over the course of the last ten years, an extensive amount of data has revealed a significant rise in the rate of online child sexual abuse (CSA) worldwide; particularly, the COVID-19 outbreak caused a significant spike in the rate during the peak periods of internet usage. Child protective services reported that the majority of school closings, social distancing measures, and very little to no adult supervision increased children's dependence on using electronic devices for socializing, thus resulting in increased exposure to online threats. Furthermore, many children in developing nations utilize their cell phones as their sole access point for the internet with little to no parental supervision and lack appropriate education for using the internet safely. Additionally, the prevalence of poverty, poverty-related issues, and inadequate resources (i.e., lack of trained law enforcement, regulatory enforcement, and adequate cybercrime systems) are detrimental to children's safety when using the internet.

This article examines effective strategies for responding to online CSA through a multisectoral and preventive lens. Drawing on regional and local research and policy frameworks, it explores the roles of education systems, families, law enforcement agencies, technology companies, and civil society organisations in addressing this complex and evolving form of abuse. By synthesising existing literature, the study seeks to identify best practices, persistent gaps, and priority areas for strengthening child-centred digital protection responses.

2. Statement of the Problem

Despite growing global awareness of online child sexual abuse and exploitation, responses remain fragmented, reactive, and unevenly implemented across regions. The rapid evolution of digital technologies continues to outpace legislative frameworks, institutional capacity, and professional expertise within child protection and law enforcement systems. As a result, many children remain inadequately protected in online environments, while perpetrators exploit regulatory loopholes, technological anonymity, and jurisdictional limitations. Existing prevention efforts are often undermined by low levels of digital literacy among children, parents, and educators, limited resources for specialised cybercrime investigations, and insufficient collaboration between key stakeholders. Survivor support services, including psychosocial care and access to justice, are frequently underdeveloped, particularly in resource-constrained settings. Furthermore, empirical evidence on the effectiveness of current interventions remains scattered, limiting the ability of policymakers and practitioners to adopt evidence-based strategies.

3. Literature Review

3.1. Nature and Scale of Online CSA

A significant increase in online child sexual abuse and exploitation (CSA) is attributed by researchers the rapid increase in the number of people able to access the internet via mobile devices, and the explosion of social networking sites and digital platforms [1-3]. The majority of the early research on the rise of CSA was conducted in Europe and North America; however, evidence gathered in recent years shows that most of the increase in online CSA has occurred in low- and middle-income countries, particularly in Africa and other countries with less-developed child protection systems.

Sex offenders are able to find sexual victims through various ways: using the capabilities of online technologies. In most cases, they do this by engaging in emotional manipulation rather than coercion. Online grooming occurs over time and usually goes through 4 stages: Trust Building, Developing Emotional Dependency, Desensitising the Child to Sexually Explicit Material, Coercion, and/or Blackmail [4]. Furthermore, The nature of child sexual abuse material (CSAM) allows for further revictimisation of the victim due to repeated distribution of CSAM to other users, allowing for the victimisation of the same child multiple times, often after they have been sexually assaulted [3, 5].

Mobile phone-based internet access, along with the increasing proliferation and regular use of online platforms such as Facebook, WhatsApp and Instagram, and a growing number of internet-based gaming environments, have been identified as primary routes for the perpetration of abuse against children, especially when there is limited regulatory oversight [6, 7] in the African context. In Zimbabwe, child protection agencies

have reported increasing incidents of online sexual grooming and sexual exploitation related to the use of social media [18]. Although substantial numbers of children throughout Zimbabwe continue to be victimised through the sexual abuse of children (CSA), the absence of comprehensive national data associated with example prevalence makes it difficult to quantify the overall impact, which is a concern echoed throughout the Global South with regards to under-reporting and lack of visibility within institutions [8].

3.2. Risk Factors and Vulnerabilities

A wide range of literature has established a "constellation" of intersecting risk factors that make children vulnerable to experiencing online CSA across various contexts. The most commonly identified include:

1) Internet access that is not supervised by an adult
2) Low levels of digital literacy
3) Limited parental mediation on the use of the internet
4) Low or very little awareness of online risks among children, caregivers and educators.

In addition, other factors such as a lack of governmental funding for creating adequate child online protection infrastructure and public education/evidence-based practices for the prevention of online CSA have contributed to increasing the vulnerabilities of children living in the Global South [7, 9].

Children from low-income families have much less access to the internet than children from middle-class and affluent families—their only access is usually through using shared devices or computers in a cybercafé (often with little or no adult supervision), personal mobile phones, or "hot spots". As such, poverty, overcrowded living conditions, limited access to formal child protection services, and higher dependence on technology for social interaction all contribute to increased risk for children in African contexts. Children with disabilities are particularly at risk for numerous reasons— they are more likely to be isolated from other children, communicate less frequently with their peers, and rely heavily on online interactions for their socialization, a situation that is documented in many studies that have focused specifically on children with sensory disabilities and children with physical/tactile disabilities [10, 11].

Adolescents are particularly vulnerable as developmental risk-taking, peer influence, and identity exploration intersect with unsupervised digital engagement [12]. In Zimbabwe, economic instability, labour migration, and caregiver absence have been linked to reduced parental supervision, increasing children's exposure to online risks while limiting adult capacity to provide guidance or protection (Mudege et al., 2017; UNICEF Zimbabwe, 2021).

3.3. Prevention Through Education and Digital Literacy

A digital literacy education programme or approach is seen as one of the most important components in assisting with the prevention of CSAOnline. The literature highlights that although digital literacy education must include the technical know-how of technology, it must go further than just this type of capability. In order to educate children effectively, digital literacy education must also teach about critical awareness of online grooming tactics, informed consent, sexual boundaries, the importance of privacy, and the mechanisms of reporting [1]. The literature also includes systematic review evidence that indicates when children learn about online safety as part of a child protection curriculum in schools, they develop greater recognition of risk, increased recognition of and openness to asking for help [14].

However, evidence from Africa and the Global South highlights substantial inequities in access to structured digital literacy education. Many programs continue to be driven by donors and are primarily geared toward cities or only involve private or wealthy schools [7, 9]. Family involvement is consistently found to be one of the most important protection factors for children, and using an active mediation approach with good lines of communication would decrease a child's overall risk of being harmed through use of the Internet [12]. The literature reviewed across several Sub-Saharan African countries indicates that caregivers often lack both digital skills and confidence, which hinders their ability to effectively teach or assist their children with safe online practices [8].

In Zimbabwe, online safety education remains fragmented, with limited integration into the national school curriculum and minimal systematic training for teachers and social service professionals [15]. The literature therefore underscores the need for culturally grounded, community-based digital literacy initiatives that simultaneously target children, parents, educators, and frontline child protection workers.

3.4. Law Enforcement and Technological Responses

The significant literature on the need for a dedicated police capacity that can respond effectively to online child sexual abuse has found that Cybercrime Police or Crime Units combining Cybercrime with some type of digital forensic capability, authority, and means of international cooperation provide the optimum opportunity to identify the offenders responsible for Commission of the Offence, retain electronic evidence regarding that commission; and dismantle those networks of exploitation operating using the Internet as a vehicle [3, 5]. However, many countries in Africa and the Global South appear to have more extensive gaps in the police capacity being able to effectively investigate and prosecute Cybercrime offences, therefore Police Forces from these areas are disadvantaged due to legislation on Cybercrime, lack of technical infrastructure, and lack of specialised training for investigators [7].

Advanced Technology, including Artificial Intelligence (AI), Hash-Matching Technologies and Automated Child

Sexual Abuse Material (CSAM) Detection Systems, have allowed High-Income Countries to improve efficiencies in identifying and reporting activity associated with CSA, while AI's and Technologies have not advanced to the same degree in Low Resource Areas, where the Technical Infrastructure required to utilise these tools is not typically available without International Companies [2, 5]. In Zimbabwe, Cybercrime legislation has been introduced, but there continues to be limited capacity to enforce this legislation, and investigations into Online Child Sexual Abuse are primarily addressed as part of General Crime Units, without any additional specialised training for those officers [16].

Scholars consistently caution that technological interventions must be embedded within strong ethical, legal, and child rights frameworks to prevent rights violations, surveillance overreach, and secondary harm to victims [3, 12].

3.5. Multisectoral and International Collaboration

Because online child sexual abuse (CSA) is international, coordinated multisectoral and cross-border responses are required. Collaborative efforts, involving government agencies, law enforcement, child protection agencies, educational institutions, civil society organisations and technology companies play crucial roles in prevention, detection and support to survivors [2, 5]. International cooperation provides opportunities to share intelligence, develop harmonised legal frameworks and conduct joint investigations which all play a key role because perpetrators, platforms and victims frequently live in separate jurisdictions [3].

While these benefits have been identified, studies report that countries in the Global South encounter significant structural barriers to collaborating effectively. These include a lack of negotiating power with multinational technology companies, weak regulatory enforcement systems, and limited resources/what is available [7, 9]. In Zimbabwe, collaboration between law enforcement, social service providers, educators, and the civil society sector is still inconsistent, while the response to online child sexual abuse (CSA) remains primarily reactive as opposed to proactive. As such, the literature suggests increased investment in establishing national coordination systems and ongoing development of international working partnerships that prioritise a victim-centred and rights-based approach.

4. Methodology

4.1. Systematic Review Design and Reporting Framework

This study was designed and reported in alignment with established systematic review standards, guided primarily by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. While no quantitative meta-analysis was conducted due to the qualitative and policy-oriented nature of the literature, PRISMA principles were applied to enhance transparency, methodological rigor, and reproducibility. The review followed a structured process encompassing identification, screening, eligibility assessment, and synthesis of relevant literature.

4.2. Search Strategy

A comprehensive and systematic literature search was conducted to identify relevant studies on online child sexual abuse and exploitation. Multiple academic databases were consulted, including Scopus, Web of Science, PubMed, and Google Scholar, to ensure broad disciplinary coverage across child protection, criminology, psychology, social work, and digital studies. In addition, grey literature was systematically searched through the official repositories of international organisations and policy bodies, including UNICEF, UNODC, WeProtect Global Alliance, and other child protection agencies, given their central role in shaping global responses to online CSA.

Search strings were developed using Boolean operators and included combinations of the following key terms: *"online child sexual abuse"*, *"child sexual exploitation"*, *"online grooming"*, *"child sexual abuse material (CSAM)"*, *"digital safety"*, *"cybercrime"*, and *"child protection"*. Reference lists of included studies were also manually screened to identify additional relevant sources.

4.3. Eligibility Criteria

Clear inclusion and exclusion criteria were applied to ensure consistency and relevance. The researcher included the following; Peer-reviewed journal articles, international agency reports, and policy documents, Publications between 2010 and 2024, English-language sources and Studies explicitly addressing online CSA prevention, detection, response, or survivor support. Studies that fell under the following categories were excluded; Studies focusing exclusively on offline CSA without digital components, Opinion pieces lacking empirical or policy grounding and Duplicates and non-accessible full texts. These criteria ensured that only methodologically relevant and substantively focused sources were included in the review.

4.4. Study Selection Process

The study selection process followed PRISMA-recommended stages. Titles and abstracts were first screened for relevance to online CSA. Full-text reviews were then conducted to assess eligibility against the inclusion criteria. Where ambiguity existed, sources were retained to minimise exclusion bias, particularly for policy and practice-oriented documents relevant to low- and middle-income contexts. A final corpus of literature was established following this iterative screening process. The

selection process prioritised methodological transparency and conceptual relevance rather than numerical volume.

4.5. Data Extraction

A structured data extraction approach was employed. Key information was systematically recorded from each included source. This included author(s) and year of publication, geographic and institutional context, study design or document type, identified risk factors and vulnerabilities, prevention strategies, law enforcement and technological responses as well as gaps and limitations identified by authors. This key information ensured comparability across diverse sources and facilitated coherent synthesis.

4.6. Quality Appraisal

Given the heterogeneity of included sources—spanning empirical studies, policy reports, and global assessments—a narrative quality appraisal approach was adopted. Peer-reviewed studies were prioritised for theoretical and empirical robustness, while institutional reports were assessed based on organisational credibility, methodological transparency, and policy relevance. This approach aligns with accepted systematic review practices in social policy and interdisciplinary research where traditional risk-of-bias tools are not always applicable.

4.7. Data Synthesis and Analysis

Data synthesis followed a thematic synthesis approach, consistent with qualitative systematic review standards. Extracted data were coded inductively and deductively to identify recurrent themes across the literature. These themes informed the analytical structure of the findings. The major themes included; Patterns of online CSA and pathways to exploitation, Risk factors and vulnerable populations, Preventive education and digital literacy strategies, Law enforcement and technological interventions, Multisectoral and international collaboration and Gaps in survivor support systems. Thematic synthesis enabled integration of empirical findings with policy insights, ensuring analytical depth and practical relevance.

4.8. Strengthening the Findings and Discussion (Systematic Review Framing)

Several factors were considered to the integrity of the systematic review. These include presenting findings as synthesized evidence, not standalone claims, ensuring that discussion explicitly linked findings back to patterns across studies and framing limitations as systemic gaps in the literature, not weaknesses of individual studies.

5. Findings

This systematic review identified six interrelated thematic findings across the reviewed literature: (1) pathways to online CSA, (2) risk factors and vulnerable populations, (3) preventive education and digital literacy, (4) law enforcement and technological responses, (5) multisectoral and international collaboration, and (6) gaps in survivor support systems.

5.1. Patterns of Online CSA and Pathways to Exploitation

Online child sexual abuse (CSA) is most often carried out by grooming processes on social media, messaging apps, online gaming, and livestreaming platforms [2, 4]. Grooming typically occurs in identifiable stages: building trust with the child, exploiting their emotional vulnerabilities, desensitising the child to sexual activity, and finally coercing them to produce child sexual abuse material (CSAM) or to engage in offline abuse of that child [5]. Pathways to exploitation in the African context and other countries in the Global South may also be facilitated through mobile access to the internet, poor content moderation, and ineffective reporting mechanisms [6, 7].

The findings of Zimbabwean studies and agency reports indicate that perpetrators typically use WhatsApp and Facebook to perpetrate online child sexual exploitation, perpetrating their exploitation through promises of financial support or educational opportunities to prey upon the children they're exploiting [17].

According to research, the way grooming occurs in an online environment can lead to delays in reporting or not reporting what occurred to them. Adolescents who are being groomed online often will not see what has happened to them as abuse when they first experience this type of interaction. The research has also shown that emotional manipulation and a gradual sexualisation are ways that offenders blur the line between coercion and perceived consent with their victims. This can make it difficult for some children to identify when something has harmed them, and perpetrators foster feelings of shame and self-blame in children [4]. When these cases occur on social media or through messaging, they become even more difficult for outside observers to see due to these platforms being a part of everyday life for most people [2].

5.2. Risk Factors and Vulnerable Populations

It is widely acknowledged that unsupervised internet access presents a risk to children across all contexts. Those children with low digital literacy are at risk because they may not be able to identify grooming behaviours, or may lack the confidence to report, resulting in higher rates of exploitation. Poverty and social exclusion further contribute to the increased risk of exploitation for children in the Global South, especially those who do not have private access to a device and when there is an absence of adult supervision.

The literature on children with disabilities demonstrates that children with disabilities are disproportionately at risk as

a result of increased isolation, dependence and lack of effective communication [11]. Adolescents have also been identified as a high risk group due to the developmental stage they are at, peer influence and aggressive experimentation with the internet [12]. Some communities in Zimbabwe, where many caregivers are absent as a result of labour migration and economic hardship, have an exceptionally high level of vulnerability [13].

In addition to the commonly known risk factors, existing literature shows the cumulative and interconnecting disadvantages associated with children's increased vulnerability for online child sexual abuse (CSA) are due to more than one individual event or exposure. Socio-economic marginalisation, caregiver absence and limited access to protective services all combine with a lack of supervised digital access to create increased risk over an extended period of time [8, 9]. In an example from Zimbabwe, the accumulation of these vulnerabilities reduces children's abilities to seek help and limits the ability for adults to intervene, creating continued and extended cycles of abuse that are progressive in nature [13].

5.3. Preventive Education and Digital Literacy

Preventive education and digital literacy interventions are repeatedly identified as effective protective measures. Specific programmes for children that teach about Internet safety, consent and how to report issues have improved children's knowledge regarding risk, and increased their likelihood of seeking help [10, 14]. However, effectiveness will vary based on the integration of these programmes into a more broad-based framework for child protection rather than as independent initiatives.

In many parts of Africa and across the Global South, the ways in which structured digital literacy education is provided remain inconsistent, as there are often programs available only in donor-sponsored or urban environments [7]. Zimbabwean literature has noted a significant gap in teacher training and the lack of curriculum integration for these programs, which ultimately limits the ability to sustain prevention efforts as noted in a report published by the Zimbabwe Ministry of Primary and Secondary.

Furthermore, available literature shows that digital literacy initiatives are more successful when they expand beyond just children's interventions and are also directed toward the educators/caregivers of children. Evidence indicates that parental mediation and the level of confidence that a teacher has about their capabilities to provide safety on the Internet, as well as the level of ability for both parent and teacher to assist with disclosure about online safety, play an essential role; however, there continues to be evidence that adults do not generally possess the skills/knowledge needed to engage meaningfully with children when it comes to children's online activities [8, 12]. Therefore, this lack of knowledge and skills among adults prevents schools from maximising their protective ability via school-based programmes and indicates that schools need to work together on a coordinated prevention strategy at multiple levels [7].

5.4. Law Enforcement and Technological Responses

The most important factor in fighting online Child Sexual Abuse (CSA) is having a specialised law enforcement capacity. Research has shown repeatedly that units with digital forensics expertise have been much more successful at identifying offenders and disrupting exploitation networks [3, 6]. Unfortunately, many units in Africa and other regions of the Global South have substantial capacity gaps that limit their ability to investigate these cases effectively.

Technological innovations have improved global capabilities in identifying CSAM (Child Sexual Abuse Material), including hash-matching tools, AI detection tools, and platform reporting systems [2, 5]. However, in Zimbabwe, the ability to fully utilize these technological tools to help identify CSAM is limited by both technical capacity and inadequate training, leading to both the under-detection of and delayed investigations into CSAM [16].

If investigators cannot identify abuse using technology, have limited exposure to the type/s of trauma experienced by most survivors, or are slow, uncooperative or unproductive during an investigation, then it will diminish reports of abuse from survivors [3.6] through their lack of faith in law enforcement's ability to assist in recovering their stolen property. In Zimbabwe, the inability to employ specialist cybercrime investigative units and reliance on general policing units creates inconsistency in case handling and limits deterrent effect, confirming findings in regional assessments [16].

5.5. Multisectoral and International Collaboration

Multisectoral collaboration results in improved outcomes for both the prevention and response to sexual exploitation and abuse against children through the most effective coordination amongst law enforcement and child protection services, education systems and civil society, as well as technology companies, thus enabling the sharing and continuity of information and care to assist survivors [2].

Due to the globalized nature of online child sexual abuse, international collaboration is essential. Challenges faced by countries in the Global South to cooperate internationally include jurisdictional limits, unequal relationships with technological firms, and lack of opportunity to participate in international enforcement systems [3]. In Zimbabwe, the coordinated approach is still limited because of poor institutional cooperation across various sectors [17].

The literature also notes that formalised coordination mechanisms rather than ad-hoc partnerships will yield more effective collaboration. With this type of collaboration when there are established pathways for referral, and protocols for sharing

information, and clearly defined roles of the various institutions involved, there will be fewer gaps related to the prevention and response efforts [2, 6]. In Zimbabwe, the lack of consistent coordinated platforms allows for limited sharing of information between sectors resulting in reactive responses rather than a comprehensive prevention approach [17].

5.6. Gaps in Survivor Support Systems

According to the literature, Survivor Support is frequently cited as the weakest area of Online Child Sexual Abuse response. Psychosocial service provision, Legal Assistance, and long term rehabilitation are also noted as generally underdeveloped globally (with an emphasis on low-resource settings [7, 8]. Survivor support for survivors of online child sexual abuse exists in the unique context of the 24/7 nature of the Internet whereby CSAM will always exist and continue to circulate indefinitely. Support services typically do not account for the Digital aspects of these unique harms. In Zimbabwe, the vast majority of services available to survivors of online child sexual abuse are provided through NGO channels, with little-to-no integration with the state, creating challenges regarding equal access and sustainable service delivery [18].

There is a clear pattern across research studies showing that the lack of sufficient support for survivors has a negative impact on both recovery and justice results. In addition to recovering from their experience, survivors of online child sexual abuse typically require continuous psychosocial support because the damage caused by digital abuse has far-reaching consequences. However, psychosocial care services that specifically address the impact of online child sexual abuse are not only limited in availability but also vary by location within resource-poor countries [7, 8]. As seen in Zimbabwe, when services provided by NGOs are provided without systematic integration into the states' resources, this creates a barrier to continuous care while reinforcing the inequities in access, according to the child protection community there [18].

6. Discussion and Analysis

The complexity of child sexual abuse and exploitation (CSA) online have increased, resulting in a larger continuum of services that must be adaptive, collaborative and responsive to children's reality; therefore, a systems-based response is required. The evidence from this systematic review shows that addressing online CSA is not possible through isolated intervention, but that prevention, enforcement and survivor support must be coordinated in order to achieve sustainable outcomes for children. This coordinated approach aligns with existing global best practice frameworks (e.g., WeProtect Global Alliance Model National Response) that identify policy, education, law enforcement and victim support as interdependent elements for achieving sustainable outcomes for the protection of children online [2].

In contrast to the United Kingdom and Australia's child protection systems adapting to create an explicit link between on and offline risks, grooming and mobile-based exploitation pathways highlight the limitations of traditional child protection models that rely heavily on a physical place and offline risks to protect children; however, as mobile connectivity is generally established as an available means for communication before a country's ability to regulate the internet, the speed at which children are exposed digitally exceeds the speed at which protective mechanisms are put in place. The result is a growing number of environments in which the potential for exploitative activity exists with little oversight. Conversely, countries such as the United Kingdom and Australia have modified their respective child protection systems to explicitly incorporate online risk environments. The UK is represented by the Child Exploitation and Online Protection (CEOP) Command, which integrates intelligence regarding online groomed children with safeguarding responses associated with offline grooming. In contrast, Australia's eSafety Commissioner integrates an authority to regulate with public education, along with a capacity to provide rapid removal of harmful content from the internet [19, 20]. While there is not yet a visible basis for the successful combination of digital realities with institutional child protection mandates in most parts of Africa, these examples serve as an indication that there are effective strategies in place in other parts of the world that could be employed by African policymakers.

Education around digital literacy should not be viewed as the only answer to the ongoing problems facing today's youth. By providing education in digital literacy, we are arming young people with the tools necessary to identify and communicate harm; however, the reality is that many young people's ability to exercise their agency is restricted by a variety of systemic issues, including poverty, lack of caregivers, and disparities in power between adults and young people and among young people themselves. Research in Nordic countries indicates that school-based digital safety education is more effective when incorporated into a larger network of child welfare and protection systems that respond quickly to the needs of child victims of digital abuse or exploitation [3]. By placing the burden on young people to protect themselves without similarly investing in the support systems of their parents, institutional accountability, and regulatory practices for Internet platforms, we may inadvertently put that responsibility on those least capable of shouldering it. To effectively prevent digital abuse, it requires the collaboration of the entire community and must not be relegated to a skill set of individuals [8, 12].

The worldwide inequalities of law enforcement response clearly demonstrate that while high-income nations have established cybercrime investigative units that utilise advanced technology with collaborative international efforts, many areas in Africa lack technical capabilities and operate with responsibility fragmentation. A clear example is Zimbabwe, which has made legislative advancements in cybercrime law,

but these improvements are not mirrored in operational efficiency. Canada and the Netherlands both have established dedicated reporting and investigative agencies that address the growing number of cybercrime incidents, including Cybertip.ca and the Dutch National Rapporteur on Trafficking. Both have public reporting programs, digital forensic investigative techniques, and victim assistance referral pathways [3, 21]. As the report indicates, to enhance law enforcement measures directed at child cyber exploitation, there must be substantial long-term commitment to developing the necessary skill sets, infrastructure, and child-sensitive service delivery methodology in terms of law enforcement's response rather than relying solely on short-term technological responses.

The systematic exclusion of services and support for survivors from both the framework of policy and practice highlights a large ethical and practical gap. This emphasis on "finding and punishing" offenders without sufficient emphasis on supporting survivors and assisting in their recovery, will not only continue to do harm but will also decrease the trust and confidence in these systems. It has been evidenced by the international Barnahus model in both Iceland and other parts of Europe that a multi-disciplinary, "onestop" approach to survivor support which provides medical, psychosocial, and legal services to a survivor in a child centred, integrated manner has proven to be successful [22]. The lack of similar institutionalized and accessible survivor support systems in many Global South regions creates a void and prevents the potential for survivors to achieve the best possible recovery outcomes and continue to actively participate in the justice process.

Finally, the review underscores that multisectoral and international collaboration is most effective when grounded in equity, mutual accountability, and national ownership. Successful international initiatives demonstrate that collaboration is most impactful when Global South countries are supported to strengthen domestic coordination rather than relying solely on external actor [2, 3]. For countries such as Zimbabwe, meaningful collaboration depends on investing in national coordination frameworks that link education, law enforcement, social services, and civil society. Without this foundation, international partnerships risk reinforcing dependency rather than resilience. Overall, the evidence calls for holistic, child-centred digital protection strategies that integrate prevention, justice, and care within sustainable national systems.

7. Conclusion and Implications

The digital age has brought about an increasing number of online child sexual abuse (CSA) and exploitation cases, and CSA through digital means is one of the most complex and critical child protection issues for the digital age. Through this systematic review, it has been demonstrated that the rapid growth of digital technology has significantly changed the way that children experience sexual abuse and exploitation and how they are exploited, resulting in an increased number of ways that abuse exists and is perpetrated against children, as well as creating a wide variety of harm based upon geographic location, laws, institutions, etc. The study confirms that the issue of online child sexual abuse is not a standalone or merely technological issue; it is an extensive, broad-based sociocultural, economic, and structural response to exploitative behaviours against children.

The findings of the Study indicate that a comprehensive and coordinated approach focusing on the needs of children is necessary for successful prevention and protection from Child Sexual Abuse (CSA). The need for an integrated approach that includes prevention, detection, enforcement, and survivor support is supported by many studies that conclude that a fragmented or reactive intervention process is ineffective. Although preventative education and digital literacy programs are essential for providing children with the necessary skills to safely navigate their online world, these types of programs must exist within a supportive framework, which includes families, schools, and the community, for them to be effective. When children are left to independently cope with the risk posed by digital technology, especially in environments with significant poverty, lack of supervision from caregivers, and a minimum of regulatory and legislative structure, there is a risk of shifting the responsibility for protecting children from these risks to the individual rather than the systems and institutions that have the primary obligation to protect them.

While law enforcement has taken on a prominent role in addressing online child sexual abuse (CSA), the responses provided by law enforcement are sporadic and inconsistent. Although many of the technological tools and cybercrime prevention legislation have been adopted in many parts of the world, the findings of this review highlight huge gaps in capacity for many low and middle-income countries, including Zimbabwe. Therefore, legislative advancements alone will not create a culture of accountability or deterrence without specialised training for personnel, proper infrastructure to support investigations, and use of child-sensitive investigative techniques. The results also demonstrate the necessity of continued investment in specialised cybercrime units, international collaboration, and the utilisation of ethical and trauma-informed methods for all investigations and prosecutions of CSA cases.

The most critical contribution of this study is the recognition of survivor support as the least developed and most under-supported aspect of the existing frameworks for responding to digital abuse. The repetitive and ongoing nature of digital abuse, particularly with regard to the distribution of child sexual abuse materials, leads to significant and enduring psychological and social costs [23]. Many short-term and crisis-based approaches that address abuse do not provide for these long-term costs and effects. Survivor-centered approaches that provide a combination of psychosocial care, legal aid, and protection from re-victimization are critical to supporting children's rights to recover from abuse, maintain their dignity, and be provided access to justice. It is imperative that states develop robust, state-led survivor support systems in partnership

with civil society, to promote this approach to supporting survivors of digital abuse.

This study also emphasises that our response to online CSA must involve collaboration from multiple sectors and countries. Because digital exploitation crosses borders, being effective in responding requires coordinated action from all the stakeholders involved, including government organisations, law enforcement agencies, child protection organisations, educational institutions, and technology companies; however, this collaboration needs to be based upon principles of equity, national ownership, and capacity building. In the Global South, when engaging with the international community, engagement should increase the effectiveness of the existing domestic system and not create a reliance or duplicate the existing system.

8. Implications for Policy, Practice, and Research

In addition to the implications for policymakers in strengthening their national schemes for Child Online Protection by integrating the approaches of Education, Law Enforcement and Support for Survivors with Regulatory Oversight of Digital Platforms; for practitioners, it is evident through the evidence presented in this review, that there needs to be improved collaboration between different disciplines and that an approach that is centred on survivors (i.e. Those affected) will give the best outcomes at every stage of prevention and response.

There are still many gaps in empirical research from low- and middle-income countries; this is especially true for the effectiveness of prevention programs, law enforcement approach, and the models for supporting Survivors. Future empirical research should focus on evaluating within their specific contexts, developing longitudinal studies regarding survivor outcomes, and developing indicators that measure the specific harms of online abuse.

In conclusion, addressing online child sexual abuse and exploitation requires a paradigm shift from fragmented, reactive responses to holistic, child-centered, and system-wide strategies. Only through sustained investment, equitable collaboration, and evidence-informed action can safe and enabling digital environments for children be realized.

Abbreviations

CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
AI	Artificial Intelligence
NGO	Non Govermental Organisation

Author Contributions

Daniel Masungwa: Conceptualization, Project Administration, Resources, Writing – original & draft

Livingson Moyo: Formal Analysis, Supervision, Visualization, Validation

Tafadzwa Zulu: Supervision, Writing – original draft, Writing – review & editing

Dorcas T Hove: Data curation, Methodology, Resources, Software

Nyaradzo Mhizha: Data curation, Investigation, Resources

Elsie Whacha: Data curation, Project Administration, Software

Abel Bohwasi: Formal Analysis, Methodology, Validation

Ketty Chirangwanda: Supervision, Software, Resources

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. Journal of Child Psychology and Psychiatry, 55(6), 635–654. National Institutes of Health (.gov) https://doi.org/10.1111/jcpp.12197

[2] WeProtect Global Alliance (2019) Model National Response to Prevent and Tackle Online Child Sexual Exploitation and Abuse. London: WeProtect Global Alliance.

[3] United Nations Office on Drugs and Crime (UNODC) (2021) Global Study on the Sexual Exploitation of Children. Vienna: UNODC.

[4] Kloess, J. A., Beech, A. R. and Harkins, L. (2014) 'Online child sexual exploitation: Prevalence, process, and offender characteristics', Trauma, Violence & Abuse, 15(2), pp. 126–139. https://doi.org/10.1177/1524838013511543

[5] Seto, M. C., Hanson, R. K., & Babchishin, K. M. (2015). Contact sexual offending by men with online sexual offenses. Sexual Abuse, 23(1), 124-145. https://doi.org/10.1177/1079063210369013

[6] INTERPOL (2020) Global Crime Trend Report: Child Sexual Exploitation. Lyon: INTERPOL.

[7] ECPAT International (2021) Global Threat Assessment: Sexual Exploitation of Children Online. Bangkok: ECPAT International.

[8] UNICEF (2020) Protecting Children from Online Sexual Exploitation and Abuse. New York: UNICEF.

[9] Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2016). Global Kids Online: Research synthesis 2015–2016. UNICEF Office of Research – Innocenti and London School of Economics and Political Science https://doi.org/10.1177/2043610616676035

[10] Jones, L., Bellis, M. A., Wood, S., Hughes, K., McCoy, E., Eckley, L., Bates, G., Mikton, C., Shakespeare, T. and Officer, A. (2012) 'Prevalence and risk of violence against children with disabilities: A systematic review and meta-analysis', The Lancet, 380(9845), pp. 899–907. https://doi.org/10.1016/S0140-6736(12)60692-8

[11] Stalker, K. and McArthur, K. (2012) 'Child abuse, child protection and disabled children: A review of recent research', Child Abuse Review, 21(1), pp. 24–40. https://doi.org/10.1002/car.1154

[12] Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. Journal of Communication, 67(1), 82–105. APA PsycNet https://doi.org/10.1111/jcom.12277

[13] Mudege, N. N., Ezeh, A. C., & Izugbara, C. O. (2017). "But we are not all the same": Towards a nuanced understanding of masculinities and HIV testing among male youth in Malawi and Uganda. Sex Education, 17(1), 1–15. https://doi.org/10.1080/14681811.2016.1213233

[14] Walsh, K., Zwi, K., Woolfenden, S., & Shlonsky, A. (2018). School-Based Education Programs for the Prevention of Child Sexual Abuse. Research on Social Work Practice, 28(1), 33–55. https://doi.org/10.1177/1049731515619705

[15] Ministry of Primary and Secondary Education (2020) Education Sector Strategic Plan 2021–2025. Harare: Government of Zimbabwe.

[16] Chigwada-Bailey, R. (2021) Cybercrime and Law Enforcement Capacity in Zimbabwe. Harare: Zimbabwe Legal Information Institute.

[17] UNICEF Zimbabwe (2021) Child Protection Annual Report. Harare: UNICEF Zimbabwe.

[18] Zimbabwe Child Protection Working Group (2022) National Child Protection Coordination Report. Harare: ZCPWG.

[19] CEOP Command (2020) Child Exploitation and Online Protection Centre: Annual Report. London: National Crime Agency.

[20] Australian eSafety Commissioner (2021) Australia's eSafety Framework: Protecting Children Online. Canberra: Australian Government.

[21] Public Safety Canada (2020) Cybertip.ca Annual Report. Ottawa: Government of Canada.

[22] Council of Europe (2018) Barnahus Quality Standards: Guidance for Multidisciplinary and Interagency Responses to Child Victims of Violence. Strasbourg: Council of Europe.

[23] Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2014). A evaluation of "Intervention in a Box": A brief education intervention to prevent online sexual solicitation of youth. Journal of Child Sexual Abuse, 23(2), 177–197. https://doi.org/10.1080/10538712.2014.868383