REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 2, 2026, 59-76
https://doi.org/10.71261/rcps/3.3.59.76

Online Child Exploitation and Digital Policing: Challenges, Emerging Trends, and Policy Responses

Syed Rizwan Haider Bukhari[1]

Abstract

Digital technology, such as social media, encrypted messaging, cloud technology and artificial intelligence (AI) has revolutionised communication and opened up new opportunities for children to be exploited online. This exploitation encompasses grooming, sexual extortion (sextortion), child sexual abuse material (CSAM), livestreaming abuse and other cyber-enabled crimes. The lack of a physical border makes it difficult to enforce the law in cyberspace, necessitating the development of more sophisticated digital policing techniques such as Cyber Forensics, international cooperation, Public-Private Partnerships, and the use of Artificial Intelligence in investigations. On a global scale, around 302 million children are victims of some form of online sexual exploitation every year (one in eight). The methodology of this study is qualitative, which involves three methods, namely secondary literature, institutional reports and comparative policy analysis, to explore new trends, technological issues and legal aspects of digital policing. Results show that although technology has improved, policing still has jurisdictional, privacy and capacity issues. Collaborative international action is required; laws need to be harmonized, technology needs to be properly governed, investments must be made in digital policing and child safety education must be proactive and online.

Article History
Received 25 March 2026
Revised 11 June 2026
Accepted 23 June 2026
Published 24 June 2026

OPEN ACCESS

Keywords
Online child exploitation, digital policing, AI investigations, CSAM, international cooperation, cybercrime, encrypted communications, technology governance, child safety.

Introduction

The digital revolution has had an impact upon how children talk, learn, socialize and access information. Internet use figures indicate that children are already on the internet and that everyone is linked together through various digital platforms. Smartphone devices and online games, social media and instant messaging platforms, video-sharing platforms have become part of the everyday lives of children worldwide and offer them learning and social opportunities as well as new ways of being exposed to risk and exploitation. Being digitally connected has many positive aspects for children's learning, socializing and entertainment, but has also exposed children to new and unparalleled vulnerabilities. Criminal networks and individuals use technological anonymity, encrypted communications channels, false identities and cryptocurrency transactions and transnational networks in the Internet targeting vulnerable minors. These techniques have expanded the practice and scale of child exploitation to go beyond the

[1] PhD Political Science (Strategic Studies), Islamia College University Peshawar (Estb : 1913), Khyber Pakhtunkhwa, Pakistan. Email: bukhari@icp.edu.pk; bukharipalmist@gmail.com

traditional offline tools and methods of exploitation and have created new challenges for society, policy makers and law enforcement. (Livingstone & Smith, 2014; UNICEF, 2021; WeProtect Global Alliance, 2025; INTERPOL, 2024).

Internet child exploitation has a wide range of harmful activities. Nowadays it's the perpetrators who are sophisticated groomers who use the words "manipulation" and "coercion" in a digital process. Children and young people are being exploited through the use of AI-generated characters and apps for live streaming and encrypted communications which are increasingly evading the usual means of detection. The production, distribution and commercialization of child sexual abuse material (CSAM) has been made possible through digital platforms which allow for offenders to access global audiences easily and quickly, allowing online exploitation to be a truly transnational phenomenon.(Kokolaki & Fragopoulou, 2025; Ciardha et al., 2025; We Protect Global Alliance, 2025; UNICEF, 2025).

The increasing capabilities of AI and the proliferation of deep fake technology and automated content creation, however, have created further difficulties in detecting and prosecuting online child exploitation. There are new tools that enable hackers to evade content filters, fabricate synthetic baby faces and videos of minors, as well as carry out large-scale psychological manipulation. The changes underscore the need to take a holistic, technologically-savvy and multi-directorial approach to child protection, in the law enforcement, technology, and social sector spaces. Thus in today's society, the practice of digital policing has become a part of child protection policies. Digital policing isn't just about “boots on the ground” and “eyes on the street” like in the days of old, it also relies on cyber intelligence, digital forensics, artificial intelligence, big data analysis, investigations of block-chain and other information-sharing mechanisms across the world. The tools will be used to detect, monitor and investigate cyber crime against children when it occurs and to allow the police to respond to fast moving and cross-border cyber crime (UNICEF, 2021; We Protect Global Alliance, 2025; INTERPOL 2024).

However, there are more issues when it comes to digital policing; it's not just about the tech. Jurisdictional barriers and legal fragmentation, lack of institutional capacity and privacy constraints often mean that enforcement is ineffective. Many countries do not have coordinated laws to comprehensively criminalize OCC; and there is not a uniform approach to cooperation among countries both technically and in terms of laws and legislation and countries are not receiving the same priority as regards action to combat OCC. Also, regulations and law enforcement responses tend to lag behind digital technology development, requiring frequent and continuous adaptation and special investigator training. Law Enforcement is not the only one with a responsibility for children's online safety. Social media, messaging and video companies which are developing the technology have a critical role to play in implementing measures to fight exploitation, including security features, content moderation and reporting. The governments are more interested in policies to ensure the accountability of companies, e.g. child safety functions, age verification, use of algorithm-based moderation, as well as automated recognition of CSAM. There are also other actors (e.g. education providers, mothers, civil society organizations and international agents) who contribute to raise awareness, digital literacy and preventive actions in order to reduce risks. (Mitchell et al., 2025; We Protect Global Alliance, 2025; INTERPOL, 2024; UNICEF Innocenti et al., 2025).

Recent research shows that approaches to address the situation for digital child protection must be done with a holistic framework involving both legal, technological and social solutions. Timely interruptions, identification of offenders and deterrence of trafficking networks is thought to be facilitated by multi-stakeholder collaboration, including with the private sector. It is also crucial, for the current opportunities for shared action, training and framework for data exchange, to have international organisations such as INTERPOL, International Centre for Missing and Exploited Children (ICMEC), UNICEF etc., which have the capacity of coordinating a global response to child exploitation online. AI and machine learning have empowered law enforcement to investigate and take action on the enormous amount of information that can be captured to find patterns in grooming and exploitation, and predict potential danger. Digital forensics may also be useful at obtaining a recreation of the online interaction and recovering files that have been deleted or finding out information on any money transactions that might have taken place in relation to the exploitation. Nowadays, block chain analytic become more prevalent when it comes to sextortion or trafficking cases to trace payments made using cryptocurrencies between those involved servicing law enforcement to link the hat with the victim, without jeopardizing the evidence in court. Despite technology, there are still many gaps, which have not been closed yet. Monitoring is restricted to privacy and human rights aspects; knowledge and facilities are lacking to apply advanced analytical tools in many places. Constantly, investigators face the challenge of new (encrypted) messaging applications, temporary browser content and anonymity. Good child protection practices, therefore, need to be a balance of surveillance and enforcement with ethics looking to communities, education and technology providers to minimize vulnerabilities.(INTERPOL, 2024; Kale et al., 2026; UNICEF, 2026)

Policy frameworks are also significant pieces of counteracting against online child exploitation. In order to effectively address cyber crime, legislation must be harmonized, there will be mandatory reporting requirements, and cross-border judicial cooperation will be needed. Policymakers have been encouraged to prioritize the development of digital policing units; train police; and create awareness among the public about the new system. Enforcement measures are supported by prevention-oriented interventions, such as providing children with training on digital safety, digital literacy, and approaches to educating parents about child protection (Adel & Norouzifard, 2024).

The threats emerging are problems that need to be addressed in advance. There are now other types of risk including AI-generated material to abuse, the deep fake technology and finally how that abuse is monetized online through cryptocurrencies. New forms of abuse are emerging and law enforcement needs to be adaptive, investing in new and advanced detection tools, and more international cooperation, to stay ahead of abuse. Additionally, giving digital literacy, awareness campaign and psycho-social support to the victims of child trafficking is important to ensure their protection on a long-term basis (Arumugham & Thangaiah, 2026).

Finally, the digital economy has revealed the need to do research in support of policy making. Comparative analysis of the effectiveness of digital policing, technological interventions and collaboration with foreign jurisdictions can be an occasion to learn about good practice and new approaches. This then allows players such as governments, NGOs

and technology providers to develop policy and strategies, in different jurisdictions, for effective resource use, proactive prevention to protect children online, and evidence of impacts of such measures. The digital landscape is in a continual state of evolution, and the child exploitation sector has evolved; therefore, advanced policing in the digital sector is needed. As such, the threats that children face today are more and more borderless, platform- and technology-based, making it harder to tackle by traditional law enforcement strategies. Children need to be safeguarded by incorporating all aspects from law enforcement competencies to technological innovation, through legal harmonisation, public-private partnership and awareness campaigns. The study results provide a robust basis for the development of integrated policies and international cooperation mechanisms to combat the rising phenomenon of online child exploitation as well as for a more effective policing approach (Boutier, 2026).

Literature Review

Evolution of Online Child Exploitation

With the advances in digital technologies like the Internet and social media Child Exploitation has come a long way and has raised serious questions of child brain health in recent times . Early exploitation forms were mainly in the form of forews, forums and personal websites; however with the development and growth of social media, mobile application, games, livestreaming and Cloud now the scale and sophistication of exploitation is growing far more. Bad guys are using the anonymity of the internet, encrypted messaging, assumed online identities, and new AI technology to groom and exploit children around the world. Researchers categorize online child exploitation as: grooming, child sexual abuse material (CSAM), sextortion, live-streamed abuse, online trafficking, sexual coercion, deepfake abuse and digital money-making schemes. Taking a closer look, current global estimates suggest that more than 300 million children fall victim to any form of online sexual exploitation every year, indicating the scale of a complex cyber crime (Clark et al., 2025).

Online Grooming

Online grooming is a deliberate and manipulative technique used by an offender to gain the child's willingness, confidence and trust prior to engaging in sexual exploitation. Generally, the stages include the identification of the victim, building of relationship, dependency upon the abuser, sexualisation of the situation, the process of isolation, and the use of coercion. Today, in a digital world which includes the social media algorithms, multiplayer online games, livestreaming platforms, and messaging apps, the cases accessible for grooming are highly expanded, making it difficult to detect. Grooming is frequently a multi-platform, cross-jurisdictional interaction, which increases the difficulty of law enforcement intervention, as revealed by the research. Research highlights the importance of detecting early signs and preventing the incidents from escalating into abuse by leveraging algorithmic monitoring, behavioral analysis, and awareness campaigns to discourage students and encourage reporting (Demeocq et al., 2026).

Child Sexual Abuse Material (CSAM)

Online exploitation in general, but particularly the existence of Child Sexual Abuse Material, is one of the most pervasive and rapidly growing types of exploitation on the

Internet. Digital CSAM can be reproduced at will, unlike traditional crimes being offered endless potential of victimization when these images are shared or accessed. The complexity of CSAM production and distribution material has expanded with technological innovations, such as encrypted private messaging, peer-to-peer social networks, dark website illegal cyber market places, cloud storage, and payments via cryptocurrencies and blockchain technology has made even financial investigations more complex and time consuming due to vpn usages. The use of digital forensics, AI support in detecting joint international operations are highlighted as key components in the identification of offenders and the rescue of victims is more complexed. CSAM is expanding so quickly that it is difficult for traditional policing structures and mechanisms to keep up, requiring new techniques for evidence collection and enforcement of the law (Engelmann et al., 2025).

Sextortion and Live-Streamed Exploitation

Modality of online child exploitation is emerging, such as sextortion and live-streamed abuse. Sextortion is the practice of forcing children to produce sexual content under threat, usually by recording or threatening to release sexual images and videos over the internet that, if not paid, will lead to the child being disclosed on such websites. Real-time sexual abuse of children is happening via live-streamed sex, and recordings are frequently shared illegally and have long-term consequences. The literature points to the fact that these forms capitalize on the following features of digital platforms: immmediacy, worldwide reach and anonymity. Livestreamed abuse is emerging as a significant form of online abuse and poses high risks to children, and the lack of investigative action and responses due to the nature of the conversation (encrypted, jurisdictional, anonymous online medium) is a matter of concern(Fair et al., 2026).

Artificial Intelligence and Emerging Threats

In the realm of CSAM, AI has brought about latest challenges which are promising avenue for investigation. AI technologies currently exist which can be used for the production of synthetic abuse imagery, automated deep fake content, automated grooming and for the prediction of potential victim targets. These technologies make up the art of getting more difficult to identify forensically, load more work onto investigators and need constant change in detection algorithms. It has been debated that there is a need to create policies, AI governance frameworks, and state-of-the-art policing protocols that are coordinated across sectors, taking account of AI exploitation and misuse of abuse material and its automation. Preventing new forms of child exploitation, and overseeing such activities in an ethical manner, also depends on continuous technological adaptation and monitoring(Fortunato et al., 2025).

Digital Policing Strategies

Digital policing comprises cyber intelligence, digital forensics, open-source intelligence (OSINT), artificial intelligence (AI), machine learning, investigations in blockchain and metadata, cloud monitoring and international cooperation in order to detect, prevent and prosecute cyber-enabled crimes against children. There is also an improvement in police and security services with predictive analytics, automated image classification, image face detection (legally permitted), and behaviour profiling. Literature also stresses that implementing digital policing through public-private partnerships, multi-agency efforts, and standardized international procedures is most effective. These

technological tools can help agencies predict offender behavior, prioritize criminal investigations, and disrupt criminal exploitation networks, while also preserving privacy and civil liberties(Gaitis et al., 2025).

Challenges in Digital Policing

Digital policing is still struggling with major operational issues against the backdrop of progressing technological development. The effects of jurisdiction squabble on a transborder enforcement, privacy legislations on surveillance, and the quick development of the communication structures is not followed by the quick changes in the law enforcement techniques. Additionally poor technical skills, lack of training and poor provision of resources are barriers to effective interventions. The literature highlights the use of encryption, anonymization tools, and the growing use of new AI which facilitates avoidance techniques, serving as extra hurdles for investigators. Experts recommend that both capacity building and public-private partnerships (P3P) be pursued alongside legal harmonisation and international cooperation in the event that all obstacles need to be overcome(Giles et al., 2024).

Legal Frameworks and International Cooperation

The protection of children online is underpinned by international, regional and national legislation. Harmonized cybercrime laws, MLATs, and cooperation between the different courts is essential for effective enforcement to enable cross-border investigations. Global organizations such as INTERPOL, the International Centre for Missing and Exploited Children (ICMEC), the UN Office on Drugs and Crime (UNODC) all provides support for training, operationalised coordination and policy guidance on the subject. Where as as we know that there are still gaps in laws and capacities among different countries, for standardizing protocols, building investigating capacities for convergence in relavent policies to advance international protection processes (Green et al., 2026).

Public-Private Collaboration

Private Sector is a crucial actor for addressing Online child protection challenges. Social media tech companies have institute monitoring, content moderation, and reporting systems to work in conjunction with law enforcement. By collaborating with public-private partnerships, companies can contribute to the data sharing, while boosting their ability to create joint AI tools that can more effectively identify an exploitation incident and working together, preparing for the governmental response. Literature has also confirmed that the collaborative working supports effective investigations, effective interventions are timely, proportionate and comprehensive and there is a balance between technological innovation and child protection (Henry et al., 2026).

Education, Awareness, and Prevention

Measures of prevention are crucial to curb online exploitation of children. Children's, parent, teacher and community education programs develops children's resistant attitudes, behaviours online and awareness of risk.Child, parent, teacher and community education builds up Digital Competence, Risk Awareness, Online Behaviours and Becoming Resilient. Empirical research demonstrates that if people know what to look for and are provided with awareness-building resources, and if another individual engages in outreach or awareness building through school programs and/or social media exposure, the likelihood of encountering CSAM and being targeted for grooming and sextortion

decreases significantly. Giving more emphasis to the children that encourage children to report, social and psychological support, and having measures within the community to help children protect themselves online (Holt et al., 2020).

Integration of Emerging Technologies

The unscientific available literature emphasizes the importance of incorporating of new technologies in child protection systems which need seriouse attention. AI-powered content detection tools, soft wares, automated content recognition and detection, blockchain tracking of exploitation via cryptocurrencies, analytic on the cloud improve detection drives, evidence collection and prosecutors' efficiency are most important. Scholars have emphasized the true need of time for technology to be complementary. This is also true the it is not substitute for legal and policy structures and to be effective and ethical, but to ensure the effective digital policing in an ever-changing cyber world of modren age of AI, there is a need for ongoing investment in research, training, and capacity building(Jamaludin et al., 2026).

Above mentioned literature has made is evedent that online child exploitation is complex, ever changing, which requires multidimensional and multidisciplinary correct responses. Key actions involve the use of law enforcement and artificial intelligence powered technology, international collaboration, public-private partnerships, legal harmonisation, and educational initiatives. There is still a lack of enforcement, coordination of jurisdictions, technological adaptation, and preventive measures. These results highlight the need for comprehensive, integrated strategies to protecting children online, lays out a foundation for evidence-based policy making, and improve the effectiveness of digital policing tools(Jang & Suh, 2024).

Research Methodology

The methodology used in this study is a qualitative and exploratory approach, particularly a secondary data analysis to explore the nature of the interplay of the two concepts: on-line child exploitation and on-line digital policing. The research method is descriptive and analytical, with the objectives to understand the nature, scope and technological picture of online child exploitation and to analyse the effectiveness of the digital policing mechanisms.

Based on key experts and across multiple authoritative secondary sources of data such as peer-reviewed journal articles, government publications, reports from international police, child protection agencies, reports on cyber-crime, academic books and global statistical databases, data were selected and collated systemically. For these triangular solution can become reality and enable a holistic analysis of technological and policy aspects. This can help to recognize new trends and weaknesses in response.

The analytical framework focuses on pertinent themes: forms & dynamics of online child exploitation, AI-driven real threats, digital policing strategies issues. These legal & regulatory frameworks, international cooperation, impact of policies and real future challenges of the society. The study recognize had limitations within secondary research such as under reporting fallout, hidden online networks, jurisdictional differences. These statistics may assists in the underestimating the actual scale of child exploitation online.

Discussion

Scale and Magnitude of Online Child Exploitation

For children, the phenomenon of online child exploitation is one of the most significant public safety and cybercrime issues of today's digital world. Internet access, social media platforms, encrypted communications and digital technologies have now replaced the old-fashioned notion of a fenced garden, opening up new avenues of opportunity for offenders to access children in different countries. It is estimated that each year, about 302 million children endure all forms of online sexual exploitation and abuse, while almost one in eight children in the world suffers the ravages of online image-based sexual exploitation and abuse (OISE). Moreover, online sexual solicitation and grooming and other technology-facilitated exploitation of hundreds of millions of children have occurred. It is clear that the issues of child exploitation on the Internet are borderless and have become a global problem, according to these disturbing statistics. This challenge calls for coordinated international responses, coordinated action across national borders in the implementation of applicable laws and practice to build cross-border cooperation through law enforcement in dealing with exploitation of children in the online world and the sharing of information and the harmonisation of laws, as well as collaboration between governments, technology companies, international organisations and civil society to ensure children are safe in the digital environment (Khan, 2024).

The high rate of online exploitation is indicative of technology penetration and the adaptability of offenders. Children are exposed to potential online threats as internet access and digital literacy are higher in countries with more internet access. For instance, areas with low to no digital monitoring and those lacking comprehensive legal protections are more likely to have high rates of child exploitation. These trends suggest that fighting online abuse isn't just a matter of risking policing, it's also about prevention, which involves education opportunities within digital literacy, awareness initiatives within community and international cooperation(Knipschild et al., 2025).

Drivers of Online Child Exploitation

Increased Internet Access

Children are being exposed to online risk from their increasingly fast and adapting use of digital technologies. Children are surrounded by useful tools such as smartphones, tablets, educational platforms, and gaming consoles, which provide access to virtual environments with which they spend a significant amount of their day. These technologies allow children to learn, interact socially and be creative, but offenders also have access to victims, allowing them to groom, coerce and access harmful content(Lahtinen et al., 2025).

Social Media and Gaming Platforms

Social media and multiplayer gaming worlds serve two functions. Many of their functions are designed to allow users to message people anonymously, request to be friends with others, be promoted by the platform's algorithms, and live stream, but all these design options invite predatory actions. Bad actors use deception, aloft trimmed fake identities or AI-generated avatars, to capitalize on children's needs for validation, online popularity and to feel valued and included (Lannier, 2026).

Encrypted Communication and Privacy Tools

End-to-end encryption, a key part of the privacy and security of users' communications, has made investigations more complex. These encrypted messaging services make it harder for investigators to access the communications without lawful powers and may lead to a delay of intervention or jurisdiction issues. Encryption guarantees security for users, but also permits cyber offenders to be safe as they schedule their illegal business.Encryption not only secures users but also opens the way for cyber criminals to carry out exploitation activities safely(Manoj et al., 2025).

Artificial Intelligence and Emerging Threats

The scarcity of online information about the extent of child exploitation has changed dramatically with the introduction of AI. Artificial Intelligence is increasingly being leveraged to create deepfakes images, synthetic child abuse material, voice cloning and to automate grooming. Along with those technological stunts, they also make life harder for law enforcement investigators. In the context of this, AI-generated content becomes harder to detect with the help of specialized forensic expertise, emphasizing the urgent need for capacity building in digital policing(Martin et al., 2025).

Cryptocurrency and Anonymous Transactions

Cryptocurrencies are being used to make anonymous payments, which help fund internet child exploitation and illicit networks or marketplaces. Offenders use anonymous payments to convert profits from CSAM, sextortion, and trafficking into cash and evade detection or prosecution using the traditional banking system(Wortley et al., 2024).

Digital Policing Strategies

Cyber Patrol and Surveillance

Proactive police patrols on digital platforms are now used to keep an eye on risky activity on publicly accessible platforms. Cyber patrol combines state of the art automated detection algorithms with human intelligence to find indications of early stages of grooming, distribution of CSAM, and traffic in networks. Operational procedures guarantee adherence to national laws and international human rights standards, taking into account child protection and privacy implications.

Digital Forensics and Evidence Recovery

Digital forensic approaches have become a core strategy to prosecute online child exploitation. Investigators has the technology to reconstruct deleted files, investigate metadata is also possible, explore cloud data is difficult but not impossible, review network logs and timeline histories of devices are easily carried out. There is need for investing on technological infrastructure, inter-agency collaboration, and specialized training. Digital Evidence Extraction and Authentication are significant in securing convictions and decimation of crime networks in new era of AI tech world which is further capacity for emergence of advanced forensics highlights.

Artificial Intelligence in Investigations

AI can support investigation for the detection of known CSAM, prioritization of investigation leads, identification of repeat offenders and surveillance of suspected activity. Automated classification systems and image recognition technology improve the process, but it is important to remember that human oversight is needed to ensure accuracy and

compliant with the law. AI can also assist in intelligence-led policing, helping to allocate resources strategically and stopping exploitation from escalating.

International Cooperation

Because online child exploitation is trans-border, it requires strong cooperation across the borders. Cybercrime units facilitate the exchange of intelligence, collaborative investigations, mutual legal assistance, extradition activities and the integration of databases. International and regional agencies like INTERPOL, Europol and ICMEC also assist in transnational operations by offering operational guidance, best practices, and technical training to digital policing agencies around the world .

Legal and Regulatory Challenges

There are a number of legal limitations to effective intervention. It is difficult to gather evidence, due to jurisdiction issues, conflicting privacy laws, data localization requirements and poor mutual legal assistance practices. We have additional difficulties such as encrypted communications, anonymization tools, and a number of authorities with different jurisdictions, which affect the investigations and prosecution. Both scholars emphasize the requirement for a harmonized law, international treaties and a cybercrime protocol of sorts to fill the legal gaps.

Capacity and Resource Constraints

Many countries have huge shortage of Cyber investigators, Digital forensics labs, AI expertise instead of any, specialized prosecutors, financial resources to operate a cyber investigation team. As technology advances, often at a much faster pace than institutions can keep up, the volume of investigations rapidly piles up, interventions are slow and the victims are left vulnerable to ongoing abuse. For establish sustainable approaches to digital policing there is a need of essential capacity-building efforts to build readiness, bolster technical skills.

Public-Private Partnerships

Cooperation is a key element in the work of ensuring the protection of children in the digital space, and the cooperation of public authorities with the private sector is particularly crucial in this context. Social media and messaging services, cloud and other digital service providers and online games increasingly play a role in child protection by implementing reporting mechanisms, content moderation, or AI-based detection tools, and/or exchanges with relevant authorities. The relationship between children's safety, users' rights to privacy and the legal responsibilities are considerations that need to be carefully balanced to form effective partnerships. With the right regulatory frameworks in place and mutual cooperation these partnerships play a vital role in building capacity, identifying offenders, ensuring investigations can be conducted in a timely manner and helping to strengthen childhood-focused prosecutions of technology-facilitated child abuse crimes.

Education, Awareness, and Prevention

To minimise vulnerabilities to online exploitation, there is a need for prevention. Children, parents, schools and community members are made aware of online risks, how to act in a safe manner and how to report concerns through digital literacy programs. Measurable decreases in exposure to grooming, sextortion and CSAM as well as strengthening child psychosocial resilience and empowering children personally to protect

themselves has been identified through school-based interventions, community workshops and public awareness campaigns.

Ethical Considerations and Technology Governance

The focus is on the ethical application of AI, automated surveillance and predicting abuse in policing. It is important to uphold public confidence that the investigative tools do not infringe upon privacy, human rights or due process. Guidelines for ethical implementation, responsible handling of data, and accountability for all stakeholders – both public and private – using technology for digital child protection are beneficial within technology governance frameworks .

Integration of Emerging Technologies

AI-powered monitoring, blockchain-cryptocurrency tracing of transactions, automatic content recognition, and cloud-based analytic platforms have great promise for improving child protection. These technologies enable to speedily identify the victims, gather court admissible evidence and disrupt the offender networks. The study emphasizes the importance of persistent investment, technical training, and legal harmonization to effectively enhance the use of technology as a tool to complement and not replace effective policing.

Policy Implications and Future Directions

Literature is pointing towards the need of an integrated approach towards the effective mitigation in the domain of online child exploitation. These include ensuring harmonised international legal frameworks, creating clearer digital policing infrastructure, using AI to help detect crimes, public/private partnerships and taking active steps of education. Key factors are the ongoing technology uptake, sustainable capacity building, and ethical oversight and the engagement of communities. Future perspectives as highlighted in literature review: taking into account the impact of the AI regulation, the data privacy legislation and development of new digital platforms' in child protection and the variation of enforcement mechanisms and available resources across different regions. Online exploitation of children is a borderless, complex and ever changing type of cybercrime. This entails multi-disciplinary protection approaches that include: Digital policing, Technological innovations, International cooperation, Legal harmonisation, Public-private cooperation and Education-based prevention. Practice guidance indicates that addressing the issues of jurisdiction, capacity shortages, emerging AI-powered risks and ethical concerns are all significant in safeguarding children online. Policy guidance on design and reform, law enforcement and guidance for stakeholders who want to improve child protection systems in countries can be taken from different evidence-based insights.

Findings / Results

Global Scale of Online Child Exploitation

The research highlights that child on-line exploitation is one of the fastest growing, and most pervasive, cybercrime incidents in the world. Every year it is estimated that over 300 million children are affected by some type of online sexual exploitation: online grooming, image exploitation, sextortion, and live-streamed exploitation. Offenders can target vulnerable children that are located in multiple jurisdictions with a borderless cyberspace, whilst often using tools to make it harder to be identified and encrypted networks to prevent being tracked. This type of crime is a very prime example of how vital

it is to have relevant digital policing, collaboration between countries and public-private partnerships to try and protect children all over the world.

Impact of Technological Advancements

Technological advances have impacted the risks and responses to online child exploitation. Offenders can easily access online platforms (social media, gaming spaces, livestreaming and messaging applications etc.) that increase opportunities for online access and grooming. Meanwhile, technology has enhanced the police by making them more competent. These tools—such as the digital forensics, AI-assisted monitoring, predictive analytics and automated content detection—can help investigators respond much more quickly and accurately than conventional reports can be produced, potentially identifying suspicious activity and filling some gaps in global child protection efforts.

Artificial Intelligence: Dual-Edged Impact

The use of AI in combating online child exploitation has a double-edged sword since AI models use surveillance, risk stratification, and disclosed data to classify child abuse and establish probable cause. On the other hand, AI allows for the automation of identification of known CSAM, behavioural analytics, image recognition and prioritisation of investigative leads. Criminals however are also employing AI technologies to generate synthetic abuse content, an abundance of deepfakes, automated grooming bots and voice synthesis systems, further complicating the process of identifying and digitally investigating abuse. The study also calls attention, however, to the fact that using AI will mean constant fine-tuning and a delicate balance between human oversight and computer-assisted investigations to ensure accuracy, ethical consideration, and timely response from policing agencies.

Encrypted Communications, Anonymity, and Cryptocurrency

Encrypted messaging, anonymous network and cryptocurrencies are all a hindrance of investigations. There are possibilities to make non-traceable payments with cryptocurrencies, and using end-to-end encryption, communications cannot even be accessed if there is a legal authorization. Those tools allow the perpetrators to plan their activities across the border in a way less likely to be noticed. Based on the results, it can be concluded that cybercrime needs specific legislation, harmonization of international cybercrime protocols and collaborative monitoring mechanisms to be able to effectively counteract these changing crimes.

Dependence on International Cooperation

Crossing of national boundaries with regard to online child exploitation is commonplace and international cooperation is necessary. Intelligence sharing, joint investigations, mutual legal assistance and extraditions are a major part of effective digital policing, along with databases. Organizations such as INTERPOL, Europol, and International Centre for Missing and Exploited Children (ICMEC) provide valuable support in officers' operations, training and data co-ordination. The study highlights the need for national action to be complemented by the action of global partnerships in order to break exploitation networks at the international level.

Multidisciplinary Investigative Approach

When discussing interventions, it is important to also have a multidisciplinary collaboration. Cybercrime Units, Digital Forensic Analysts, Psychologists, educators, Child

Protection agencies, Technology companies and policy makers. These views combine to enable comprehensive responses in the area of victim assistance, evidence collection, perpetrator apprehension and policy development. Long-term prevention and prosecution can be brought about in a collaborative model through education, rehabilitation and public awareness raising activities while enjoying support for child protection.

Limitations of Legal Frameworks

With law that is not technology related, comes enforcement. Jurisdictional issues, inconsistencies in privacy laws and difficulties with trans-border assistance are slow down investigations and prosecutions. Existing cybercrime legislation isn't designed to combat AI-driven exploitation, deep fake materials and encrypted communication. Results illustrate the importance of restoring legal harmonization and standardizing procedures, and of regular monitoring of the law to avoid becoming outdated and ineffective in the fast-moving technology arena.

Prevention and Digital Literacy

When it comes to preventing online exploitation, preventive measures are also important. Through training and awareness initiatives on digital literacy and guiding children, parents and schools can help children stand up to grooming and sextus and develop a resistance to CSAM. It states that "reshape data education notions and give it a technological protection umbrella with reporting tools and secure online platforms to create the broader protection umbrella. Within the education sector, awareness campaigns can be conducted to educate children and parents/carers about the risks, where and how to ask for support, and what to do in a safe online environment.

Technological Integration and Ethical Considerations

The emergence of technology enhances investigative capability with a need for attention to conduct. Monitoring with AI support, blockchain tracing of cryptocurrency exploitation and automated content recognition systems enhance detection and collection of evidence. The considerations, however, have to be balanced with privacy protection, civil liberties and ethical aspects would have to be considered. -Scholars focus that an excellent system of governance of technologies ensures public trust, law and the security of the children and other lawful internet users and effectiveness of policing.

Policy Implications

They have important consequences for policy makers. In order to achieve efficient child protection, there is a need for coordinated legislation, investments in digital infrastructure of police investigative process, the exchange with foreign partners, the use of Artificial Intelligence for investigations, cooperation with the public and private sectors, and large-scale awareness campaigns. However, policy-makers must address issues pertaining to the cooperation between countries on matters of encryption, anonymisation, cybercrime, as well as resource allocation for specific cybercrime units and learning and technological adaptation. Education and awareness creation for children and carers is key in order to encourage and foster safe online behaviour and resilience. On-line child exploitation is a threat with many dimensions, which demands an integrated approach. The technological advancements, the tools for investigations, the collaborative work between different police units, the integration of public and private sectors, and the educational and

preventive measures make for a comprehensive child protection strategy. Even with the constraints of resources, scope of the intervention, territorial boundaries and the presence of a new group of actors that could pose a high risk to children with well-developed AI capabilities, a strategic and coordinated, and collaborative, approach can have a significant impact on reducing risk and providing protection for children in digital environments.

Conclusion

The Internet poses a significant and complex challenge in the crossover area of cyber security, human rights and child protection. With technological advancement, this study reveals that there has been an augmentation of both exploitation and investigation. The rise of the digital policing has seen the adoption of cyber forensics, artificial intelligence, predictive analytics, inter-agency working and many more across-disciplinary investigative ideas and capabilities introduced to help police respond more effectively to online abuse. Despite this progress, criminals continue to work hard to reduce the potential of being caught using encrypted communications, anonymous web, AI web-based identities, and digital infrastructures around the globe. It is clear that none of the governments or law enforcement agencies can be effective on their own in combating child exploitation on the Internet; the nature of cyberspace does not pay regard to state boundaries. It will require harmonized legislation, coordinated multialternational actions and co-operation, institution of public-private partnerships, ethic management of technologies and jamais-ending investments in specific investigation bodies. The activities should include all these preventive measures as well as the digital literacy programmes, child education, parental guidance, platform safety interventions, etc. to complement the enforcement activities and role in minimising the vulnerabilities. In conclusion, a child-centred, flexible and evidence-based solutions are needed to ensure children's safety online. As technology and digital platforms evolve, policy frameworks need to incorporate technological innovation, multidisciplinary collaboration, international coordination, and take steps to prevent in advance. All of these - together, such as law enforcement, education, awareness, ethical use of technology and cross-border cooperation - will enable stakeholders to decrease risks and protect children from exploitation for safer online spaces for future generations.

Recommendations

Strengthening Specialized Cybercrime Units

Governments should establish special cybercrime and digital policing units providing them with the latest in the field of forensics, safe data centers and powerful computing machines. These units should also be led by staff who have experience or training to undertake the highly sophisticated online investigations that include exploiting networks across different countries, encrypted messages and material generated using AI. Technical capacity building process helps promptly identify emerging threats and respond to them.

Enhance International Legal Cooperation

As online child exploitation is of a transnational nature, cross-border collaboration is vital. States need to have formal arrangements to share evidence, for joint investigations, and for mutual assistance. Ref. agreements at the regional level and global level can facilitate the fastest possible extradition, and ease the harmonization of procedure and

standards involved in investigations and help to ensure real-time communication between law enforcement authorities.

Engage Technology Companies in Child Protection

Age appropriate design, automated content monitoring systems, and robust reporting system are recommended tech interventions to improve child safety settings. Cooperation with the government and civil society can also facilitate in the creation of quick response mechanism which would ensure deletion of illegal content without affecting the privacy and human rights element of the same.

Expand AI-Assisted Investigative Tools

Police can use AI and machine learning (ML) to identify suspicious behavior, categorize abuse content and anticipate high-risk behavior. AI technologies complemented with human intervention can play a crucial role in maintaining ethical standards, avoiding false-positive results, and optimally managing resources.

Integrate Digital Literacy in Schools

The requirement is to have complete digital literacy training in schools to sensitise children against grooming, dangers of being on the internet, sextortion and the control of privacy. The early awareness gives a chance for children to recognize warning signs and take measures to prevent risk in a digital environment.

Support Parental and Guardian Training

Parents/carers should be alerted to methods of monitoring their child's online activity, how to ensure their child's privacy settings and the possibility that their child's behaviour might indicate exploitation. Community awareness events, internet tutorials and awareness sessions can be held to support family's role in child protection.

Modernize Cybercrime Legislation

egislation needs to be modernized to cope with the ongoing digital risks including AI created abuse, deepfakes, virtual reality exploitation, and anonymous cryptocurrency transactions. Clear definitions are needed, as well as other prescriptions and protections in the law to combat new forms of online exploitation, and prosecutions need to be eased.

Promote Public Awareness and Reporting

Free public education to inform communities of the risks associated with the Internet and encourage reporting of suspected Internet abuse and remove stigma of victimization. Access to channels for reporting, in the form of a hotline or internet-only reporting forms, will likely increase the detection rate, and will facilitate access to help-seeking services for survivors.

Implement Victim-Centered Support Systems

Comprehensive psychological, legal and social services should be provided for the survivors during the investigation and recovery. Proper care, counselling and legal assistance are provided to the victims, which includes the approach of trauma informed care, supports the victims wellbeing and increases support of the law enforcement.

Support Evidence-Based Research on Emerging Technologies

Future research should investigate the impact of generative AI, interactive virtual environments, and secure platforms and new online ecosystems on child protection. The results of these studies will inform policy, technological trends, and help ensure interventions are adaptive to changes in threat.

References

Adel, A., & Norouzifard, M. (2024). Weaponization of the growing cybercrimes inside the dark net: The question of detection and application. *Big Data and Cognitive Computing, 8*(8), 91. https://doi.org/10.3390/bdcc8080091

Arumugham, S., & Thangaiah, P. R. J. (2026). Cyberpolicing child sexual exploitative and abuse material. *International Journal of Digital Crime and Forensics, 18*(1). https://doi.org/10.4018/IJDCF.403438

Bailo, P., Sirignano, A., Nittari, G., Visconti, G., Pesel, G., Spasari, T., & Ricci, G. (2026). A review of crime at machine speed: Criminological aspects of artificial intelligence's industrialisation of deception. *Sci, 8*(3), 54. https://doi.org/10.3390/sci8030054

Boutier, I. (2026). *Artificial intelligence and child sexual exploitation: The digitalisation of harm.* https://researchonline.gcu.ac.uk/en/publications/artificial-intelligence-and-child-sexual-exploitation-the-digital/

Clark, A., Coles, C., Lankester, M., Fernandes, D., Blackwood, N., Cavenham, J., & Dickson, H. (2025). Recidivism rates among online child sexual exploitation material offenders: Systematic review and meta-analyses. *The Journal of Forensic Psychiatry & Psychology, 36*(6), 843–868. https://doi.org/10.1080/14789949.2025.2603236

Demeocq, C., Taylor, A., Ross, B., & McFeeters, A. (2026). Generative AI in child sexual exploitation and abuse: Views from UK law enforcement. *AI & Society.* https://doi.org/10.1007/s00146-026-03176-6

Engelmann, L., Weirich, C. A., & May-Chahal, C. (2025). Developing quality standards for community-based online child sexual exploitation and abuse interventions. *Child Abuse & Neglect, 164*, 107444. https://doi.org/10.1016/j.chiabu.2025.107444

Fair, C. C., Patel, P., & Maheshwari, G. (2026). Looking for individual-level evidence for the ethnic security dilemma revisited: A study of Balochistan. *Studies in Conflict & Terrorism, 49*(6), 1030–1063. https://doi.org/10.1080/1057610X.2024.2330155

Fortunato, E., Slikboer, R., Henshaw, M., & Ogloff, J. R. P. (2025). Females who engage in online child sexual exploitation: A critical narrative review. *Psychology, Crime & Law*, 1–28. https://doi.org/10.1080/1068316X.2025.2540384

Gaitis, K. K., Vermeulen, I., Stevenson, J. G., & Fry, D. (2025). Extended reality environments and child safety: Examining the emerging risks for child sexual exploitation and abuse and discussing prevention and response through a technologised neo-ecological perspective. *International Journal of Law, Crime and Justice, 83*, 100786. https://doi.org/10.1016/j.ijlcj.2025.100786

Giles, S., Alison, L., Humann, M., Tejeiro, R., & Rhodes, H. (2024). Estimating the economic burden attributable to online-only child sexual abuse offenders: Implications for police strategy. *Frontiers in Psychology, 14.* https://doi.org/10.3389/fpsyg.2023.1285132

Green, T., Kosaraju, A., & Soutar, E. (2026). Child-centred policing: Supporting trauma-informed frontline police practices with girls who have lived experiences of child sexual exploitation in the United Kingdom. *Frontiers in Public Health, 14.* https://doi.org/10.3389/fpubh.2026.1697743

Henry, N., Umbach, R., Shelby, R., Beard, G., & Given, L. M. (2026). "It's still abuse": Community attitudes and perceptions on AI-generated image-based sexual abuse.

Information, Communication & Society, 1–21. https://doi.org/10.1080/1369118X.2026.2613437

Holt, T. J., Cale, J., Leclerc, B., & Drew, J. (2020). Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. *Aggression and Violent Behavior, 55*, 101464. https://doi.org/10.1016/j.avb.2020.101464

INTERPOL. (2024). *Beyond illusions: Unmasking the threat of synthetic media for law enforcement.*

Jamaludin, A., Anggraeni, H. Y., Noval, S. M. R., Sari, R. A. W., Sonjaya, S., & Fikri, A. M. (2026). Propagation of AI-generated child sexual abuse material as a cybercrime commodity in Indonesia. *Oñati Socio-Legal Series, 16*(3), 1189–1206. https://doi.org/10.35295/osls.iisl.2579

Jang, Y., & Suh, Y. (2024). Cyber sex crimes targeting children and adolescents in South Korea: Incidents and legal challenges. *Social Sciences, 13*(11), 596. https://doi.org/10.3390/socsci13110596

Khan, A. A. (2024). Reconceptualizing policing for cybercrime: Perspectives from Singapore. *Laws, 13*(4), 44. https://doi.org/10.3390/laws13040044

Knipschild, R., Covers, M., & Bicanic, I. A. E. (2025). From digital harm to recovery: A multidisciplinary framework for first aid after online sexual abuse. *European Journal of Psychotraumatology, 16*(1), 2465083. https://doi.org/10.1080/20008066.2025.2465083

Kokolaki, E., & Fragopoulou, P. (2025). *Unveiling AI's threats to child protection: Regulatory efforts to criminalize AI-generated CSAM and emerging children's rights violations.* arXiv.

Lahtinen, H.-M., Honkalampi, K., Insoll, T., Nurmi, J., Quayle, E., Ovaska, A. K., & Vaaranen-Valkonen, N. (2025). Investigating the disparities among child sexual abuse material users: Anonymous self-reports from both charged and uncharged individuals. *Child Abuse & Neglect, 161*, 107299. https://doi.org/10.1016/j.chiabu.2025.107299

Lannier, S. (2026). Obligations of online service providers to fight against child sexual abuse material: A systematization of EU law. *Victims & Offenders, 21*(3), 506–534. https://doi.org/10.1080/15564886.2025.2557901

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654.

Manoj, D., James, R. I., Kumaran, S., Devnath, G. P., Varughese, B. T., Arakkal, A. L., & Johnson, L. R. (2025). Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation. *Child Protection and Practice, 4*, 100088. https://doi.org/10.1016/j.chipro.2024.100088

Martin, J., Gharabaghi, K., & Donevan, M. (2025). Dismantling silos: Cross-sectoral response to combating child sex trafficking and online child sexual exploitation. *Frontiers in Psychology, 16.* https://doi.org/10.3389/fpsyg.2025.1625975

Mitchell, K. J., Jones, L. M., & Finkelhor, D. (2025). *Trends in arrests and investigative techniques of technology-facilitated child sexual exploitation crimes: The Fourth National Juvenile Online Victimization Study.* Office of Justice Programs.

Nurmi, J., Paju, A., Brumley, B. B., et al. (2024). *Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy.* arXiv.

Ó Ciardha, C., Buckley, J., & Portnoff, R. S. (2025). *AI-generated child sexual abuse material—What's the harm?* arXiv.

UNICEF. (2021). *Ending online child sexual exploitation and abuse: Lessons learned and promising practices in low- and middle-income countries.*

UNICEF, ECPAT International, & INTERPOL. (2025). *Disrupting Harm: Generating evidence on technology-facilitated sexual exploitation and abuse of children.*

WeProtect Global Alliance. (2025). *Global Threat Assessment 2025: A call for prevention.*

Wortley, R., Findlater, D., Bailey, A., & Zuhair, D. (2024). Accessing child sexual abuse material: Pathways to offending and online behaviour. *Child Abuse & Neglect, 154*, 106936. https://doi.org/10.1016/j.chiabu.2024.106936