AMCAP JMCS |
JOURNAL OF MEDIA AND COMMUNICATION STUDIES
Volume 6, Issue 1. January 2026

DOI: 10.5281/zenodo.18937731

Website home: https://jmcs.amcap.net/website
Submission guidelines: https://jmcs.amcap.net/website/page/submission-guidelines

Date of Receiving: 05-08-2025
Date of Publication:10-01-2026

The Digital Border: Protecting Children from Cross Border Online Exploitation and Trafficking

Author(s)

Sameer Haider[1]

[1]Email:sameerofficial309@gmail.com

Abstract

The emergence of digital communication has brought about fresh possibilities of cross border online exploitation and child trafficking. There is the use of social media platforms, messaging application and online gaming areas where offenders would contact, groom and exploit children across countries without ever physically crossing a border. This paper examines the nature of this type of online harm, the vulnerability of children, and how it is challenging to prevent and investigate such crimes due to the lack of cooperation between countries. It also examines the role played by states, international bodies and digital platforms in creating online spaces that are safer. Using a qualitative and descriptive approach, the study reviews academic work, international reports and legal frameworks that deal with child protection and cybercrime. It also analyses the key challenges like varying national laws, sluggish cross border investigations, privacy of data and insufficiency of technical capacity in most countries. The possibility of using modern tools such as automated detection systems and faster reporting mechanisms that can be used to contribute to child protection, without infringing on privacy privileges is also discussed in the paper. The paper discusses that greater cooperation among nations, the alignment of cyber legislation, and explicit guidelines on online shopping platforms should be necessary to shield children against cross-border cyber exploitation. It ends with the practical recommendations of enhancing the prevention, reporting, investigation and support of the victims. It aims to stimulate a shared and rights-based solution to ensure that digital boundaries are used as a source of protection and not a source of mischief.

Keywords: *Child protection, Online child exploitation, Cross border trafficking, Digital border, International cooperation.*

Introduction

Consider the case of a 13-year-old boy in Lahore who joins a gaming chat after school. Within days, a stranger message him with offers of virtual coins in exchange for “fun” pictures. What feels like a game quickly turns into terror when the stranger threatens to expose the images unless the boy sends more (Danial, 2025). This is not a rare incident but a stark example of how predators exploit the innocence of children via the internet. Such stories underscore an urgent reality: children around the world are increasingly vulnerable to online abuse and trafficking, and the **digital border** – the virtual boundary between safe and unsafe online spaces – is porous and inadequately policed.

Worldwide, experts report that online child sexual abuse is rising at an alarming rate. New technologies and global connectivity have enabled criminal networks to organize sophisticated exploitation schemes. For instance, analysts note that sinister practices like livestreamed abuse, sextortion, and the sale of child abuse material now operate through “cross border chains” involving recruiters, facilitators, and anonymous payment handlers (Comolli, 2025). In this way, the internet has effectively erased distance: an exploitative act online in one country can instantly affect children in many others. As a result, a recent Global Threat Assessment concludes that online child sexual exploitation “keeps escalating worldwide, in both scale and methods” (WeProtect Global Alliance, 2023). This global crisis demands a corresponding transnational response.

The problem is especially acute in South Asia. In countries like India and Pakistan, where internet access has exploded in recent years, children have become prime targets for these crimes. Pakistan and its neighbor India are recognized as countries at great risk for online child exploitation (Ali, 2025). Online child sexual exploitation encompasses everything from grooming and cybersex to live-streaming of abuse. These crimes “cannot effectively be fought through traditional legal means” such as arrest and trial, because offenders operate behind screens and across borders. Since these crimes "are now in the digital platform and are committed across the boundaries," effective solutions must likewise be international in scope (Ali, 2025). In other words, the violence and trafficking of children facilitated by the internet do not respect national jurisdictions, yet law enforcement and legal frameworks typically do.

In Pakistan, the scale of the problem is sobering. With a median age around 22, Pakistan has a very young population, and millions of minors access the internet often without supervision. More than two million instances of child sexual abuse material were linked to Pakistani users in 2022 (Danial, 2025), yet the national Federal Investigation Agency officially recorded only 250 such cases that year. This enormous gap likely reflects not

the absence of abuse, but problems in reporting, detection, and coordination.

Khan et al. (2025) notes that Pakistan plays a significant role in global trafficking, being a top source and destination country. An estimated 2.3 million people live in modern slavery there. Traffickers exploit technology, using platforms like Facebook, YouTube, and WhatsApp as powerful tools to lure victims through fake job ads and social media messaging, facilitating cross-border exploitation.

These realities form the core research problem: how can law and policy adapt to protect children when the abusers exploit the borderless nature of the internet? Globally and regionally, there is a growing recognition that existing legal frameworks and enforcement mechanisms are insufficient. International conventions (for example, the UN Convention on the Rights of the Child and its Protocols) affirm children's rights, but jurisdictional gaps and weak implementation often hinder cross border prosecutions. As Ali (2025) emphasizes, even sophisticated national laws fall short because offenders use technical means to remain hidden and mobile (Ali, 2025). In Pakistan's context, the Prevention of Electronic Crimes Act (2016) includes penalties for online child exploitation, yet enforcement remains fragmented and understaffed. Social stigma and lack of trust in law enforcement also mean that many cases in Pakistan go unreported (Bashir, 2025). Against this backdrop, it is imperative to explore new models of legal cooperation and prevention – metaphorically, to strengthen the digital border that shields children from these harms.

This study adopts a qualitative doctrinal approach, based on analysis of international legal instruments, secondary literature, official reports, and documented case studies. In addition, it uses comparative jurisprudential analysis to examine how different jurisdictions address cross-border online exploitation and trafficking.

Accordingly, this research addresses the following questions:

1. What are the key legal and policy challenges in addressing online exploitation and trafficking of children across national borders?
2. How do existing international agreements and domestic laws (in Pakistan and elsewhere) align with the needs of protecting children online?
3. What best practices or new models of digital cooperation can strengthen the protection?

The objectives of the study are to:

1. Map the scope of cross border online child exploitation and trafficking, drawing on

global data and case examples.

2. Review and critique current legal instruments and enforcement strategies at international, regional and Pakistani levels.
3. Identify gaps and propose actionable recommendations for legal reforms, technological safeguards, and multi-stakeholder collaboration to better protect children in cyberspace.

By exploring these questions and objectives, the paper will shed light on how to transform the digital domain from a refuge for predators into a safer space for children, both in Pakistan and around the world.

Understanding Cross Border Online Child Exploitation and Trafficking

Cross border online child exploitation and trafficking represent some of the fastest growing and most complex crimes in the digital age. These crimes involve the use of digital platforms to groom, coerce, exploit, or traffic children across jurisdictions for sexual or other exploitative purposes. Because digital interactions move freely across national boundaries, offenders can target children in different regions while concealing their identities and location. This has transformed child exploitation from a localised social harm into a transnational crime problem that challenges law enforcement agencies, policy makers, and child protection systems worldwide.

A core element of online exploitation is grooming, which refers to the process through which offenders establish emotional bonds with children to manipulate their trust and reduce their resistance to abusive requests. Grooming often begins with seemingly harmless conversations through social media, gaming platforms, or messaging applications. Offenders typically follow a pattern of assessing vulnerabilities, emotional isolation, and the gradual introduction of sexual content (Whittle et al., 2013). These interactions are often private and encrypted, making detection more difficult. As a result, many children do not realise they are being manipulated until the abuse has escalated.

Another widespread form of exploitation is sextortion, in which children are coerced to provide explicit images or videos under threat of exposure, humiliation, or harm. Sextortion has become a global phenomenon due to the ease with which offenders can collect, copy, and distribute content. Online sextortion crimes have increased significantly in recent years, with perpetrators operating from different regions targeting minors who have little capacity to resist or report such threats (Wolak & Finkelhor, 2018).

The creation and circulation of child sexual abuse material (CSAM) is another defining feature of cross border online exploitation. CSAM can include images, videos, or live streamed abuse involving minors. Historically, such material circulated in hidden networks, but offenders are increasingly using mainstream platforms, encrypted apps, and anonymised search tools to exchange and sell content (Quayle, 2020). The expansion of digital payment systems, including cryptocurrencies, has further assisted offenders in conducting transactions without geographical or financial traceability.

Live streamed child abuse is an area of growing international alarm. This involves real time broadcasting of child sexual abuse for paying audiences located anywhere in the world. Live streamed exploitation is particularly harmful because it allows offenders to direct or influence the abuse as it happens. Reports from the Philippines, India, Indonesia, and other countries show that such incidents often involve cross border clients who remotely request specific acts while the child is abused in a different country (ECPAT International, 2020). This form of exploitation merges digital anonymity with real time violence, making it one of the most urgent global child protection challenges.

Cross border trafficking also intersects with online exploitation. Digital platforms are increasingly used to recruit, advertise, or transport children across borders for sexual exploitation. Offenders may use online advertisements, social media recruitment, or fraudulent job offers to lure vulnerable children. Trafficking networks in South Asia rely heavily on digital communication to coordinate movement and conceal transactions across borders (Human Trafficking Front, 2023). Once children are transported, their images or abuse may be recorded and distributed internationally, further expanding the cycle of exploitation.

Offenders exploit a range of advanced technologies to evade detection. Many use Virtual Private Networks to hide their locations, end-to-end encrypted messaging applications to communicate safely, and anonymizing browsers such as Tor to access dark web markets where CSAM is stored or traded. The dark web contains numerous communities dedicated to exchanging abuse material and establishing cross border offender networks beyond the reach of routine policing (Lykousas & Patsakis, 2025). The use of cryptocurrency wallets enables financial anonymity, making it difficult for investigators to trace payments linked to exploitation or trafficking.

Children's vulnerability stems from a confluence of developmental, psychological, and socioeconomic factors. Younger children often lack the understanding to discern online risks, while adolescents can be susceptible to grooming due to emotional insecurity and a desire for validation (Livingstone and Smith, 2014). This is compounded by a general

lack of digital literacy and fears of shame that discourage reporting. Socioeconomically, children from marginalized communities are at higher risk due to reduced parental oversight, limited access to safety education, and financial pressures. Offenders actively target these children, calculating that their families lack the resources or awareness to seek help (Ullah & Bakhsh, 2024).

Real-world incidents underscore the severity of this borderless crime. A 2019 Europol operation dismantling a major cross-border CSAM network spanned multiple continents, revealing the global entrenchment of these digital exploitation rings (Europol, 2019). Similarly, South Asian police operations have disrupted trafficking groups using platforms like WhatsApp and Telegram to coordinate the cross-border movement of minors (Ruellan, 2023), while Pakistan reports a rise in online grooming cases linked to offshore offenders (Iftikhar, 2023).

Cross border online exploitation is therefore not a simple cybercrime but a multifaceted human rights violation that intersects with digital privacy, law enforcement, and global cooperation. Understanding its forms, methods, and root causes is essential for developing legal frameworks that match the scale and complexity of the threat. The next sections will explore how international legal instruments and national laws address these crimes, and what reforms are needed to strengthen the digital border that protects children worldwide.

Legal and Regulatory Frameworks Addressing Cross Border Online Child Exploitation and Trafficking

Cross border online child exploitation has prompted a wide range of legal responses at the international, regional, and national levels. Since digital crimes frequently transcend borders, domestic legislation alone is often insufficient to address the global networks involved in grooming, trafficking, and distribution of child sexual abuse material. Effective regulation therefore requires harmonised legal standards, cross jurisdictional cooperation, and shared procedural frameworks for investigation and prosecution. This section examines the major international and regional legal instruments as well as national frameworks that shape the global response to online child exploitation and trafficking.

One of the most foundational instruments is the United Nations Convention on the Rights of the Child, which obligates states to protect children from all forms of sexual exploitation and abuse. Article 34 requires states to prevent the inducement or coercion of children into unlawful sexual activity and participation in pornographic performances. Later, the Optional Protocol on the Sale of Children, Child Prostitution

and Child Pornography strengthened global commitments by requiring criminalisation of the production, distribution, dissemination, and possession of child pornography, now legally referred to as child sexual abuse material (UNGA, 2000). Although drafted before the explosion of digital technologies, its provisions have been widely interpreted to include online exploitation, giving states a legal basis for criminalising internet related abuse.

The Council of Europe Convention on Cybercrime, widely known as the Budapest Convention, is the most comprehensive international treaty dedicated to cyber offences. It requires states to criminalise offences involving child pornography, illegal access, online grooming, and related abuse material. Importantly, it establishes procedures for digital evidence sharing and mutual legal assistance between states, which are essential for cross border investigations (Gercke, 2012). Although Pakistan is not a party to the Convention, many of its provisions have indirectly shaped domestic reforms through global policy diffusion.

Complementing this, the Council of Europe Lanzarote Convention provides detailed obligations for the criminalisation of online grooming, solicitation, and live streamed exploitation. It requires states to adopt preventive and protective mechanisms, including internet safety education and specialised training for investigators (Council of Europe, 2007). The Convention is widely regarded as a modern instrument because it directly addresses new forms of online exploitation, including technology facilitated grooming. The Lanzarote Convention fills gaps left by earlier treaties that did not anticipate the scale of digital abuse (Davidson & Gottschalk, 2011).

At the regional level, the European Union has developed an extensive legislative framework aimed at combating online child exploitation. The EU Directive on Combating Sexual Abuse and Sexual Exploitation of Children sets minimum criminal law standards and requires member states to criminalise grooming, CSAM distribution, and live streamed abuse. The Directive also requires service providers to cooperate with authorities in removal of illegal material (Chatzinikolaou & Lievens, 2019). The European Union has also invested in cross border operations coordinated by Europol, which frequently identifies networks operating simultaneously in Europe, Asia, and Africa.

The ASEAN region adopted the ASEAN Convention Against Trafficking in Persons, particularly Women and Children, which criminalises trafficking and obligates states to strengthen cross border coordination. Although it does not focus solely on digital exploitation, its provisions are increasingly interpreted to include online recruitment

and abuse (Yusran, 2018). ASEAN member states have recently acknowledged the rise of digital trafficking and have begun updating national laws to reflect these trends.

Global organisations have contributed significantly to developing legal and policy frameworks that address online exploitation. Global organisations like UNICEF, ECPAT, and INTERPOL provide crucial guidelines and operational support. INTERPOL's International Child Sexual Exploitation database is widely used by police agencies to identify victims and offenders across borders. The cross border operations supported by INTERPOL have resulted in the rescue of hundreds of children and the arrest of traffickers operating in online networks (Popa, 2024).

At the national level, many countries have modernised their criminal codes, cybercrime laws, and child protection statutes to align with global standards. The United Kingdom's Sexual Offences Act, Australia's Criminal Code, and Canada's Criminal Code contain comprehensive offences covering grooming, CSAM, exploitation through digital communication, and possession of illegal material. The United States has enacted the PROTECT Act and related legislation enabling federal jurisdiction in cases involving international online exploitation. These domestic reforms demonstrate how states incorporate international obligations into national frameworks.

Developing countries, including those in South Asia, have also made progress. In Pakistan, the Prevention of Electronic Crimes Act provides the legal basis for criminalising online child abuse material, exploitation, and recruitment for trafficking. However, implementation challenges, lack of specialised training, and limited digital forensic capacity continue to undermine the effectiveness of these laws (Bokhari, 2023). Courts often face delays in obtaining evidence from foreign service providers, and mutual legal assistance processes remain slow. As a result, many cross border offenders remain beyond the reach of domestic prosecution.

Despite notable advances, the global legal landscape still contains significant gaps. Definitions of child sexual abuse material vary across jurisdictions, leading to inconsistencies in prosecution standards. Some states criminalise possession of CSAM, while others only criminalise its production or distribution. Legal responses to live streamed abuse remain uneven, and many countries lack laws specifically addressing online grooming. Without harmonised definitions and processes, offenders can exploit legal loopholes by operating from states with weaker frameworks (Westlake & Bouchard, 2015).

Another major challenge is the lack of effective cooperation between states and private

technology companies. Although many companies have reporting obligations, the removal of illegal material remains inconsistent, and some platforms do not comply quickly with foreign legal requests (Livingstone & Third, 2017). Jurisdictional conflicts also arise when servers, offenders, and victims are located in different countries, complicating evidence collection under domestic law.

Overall, international and regional legal frameworks have created strong foundations for combating cross border online child exploitation. Treaties such as the CRC, the Optional Protocol, the Budapest Convention, and the Lanzarote Convention provide the normative basis for criminalisation and cooperation. Regional instruments and national laws complement these obligations, though enforcement and harmonisation remain critical challenges. As online exploitation evolves, legal frameworks must continually adapt to ensure that children can be protected in an increasingly borderless digital environment.

Role of Technology in Facilitating and Preventing Online Child Exploitation

Technology plays a dual role in the modern landscape of child protection. On one hand, digital platforms, encrypted communication tools, and anonymising technologies have enabled offenders to reach children across borders with unprecedented ease. On the other hand, technological innovations have also strengthened the capacity of law enforcement agencies, civil society organisations, and governments to detect, prevent, and investigate crimes involving online exploitation. Understanding this duality is essential for building an effective digital border that safeguards children in a globally interconnected environment.

Digital communication technologies have significantly expanded offenders' reach. Social media platforms, gaming environments, and messaging applications enable direct communication between strangers and children, often without parental oversight (Whittle et al., 2013). The interactive nature of these platforms creates opportunities for prolonged manipulation, which can escalate into coercion or abuse. The cross border nature of these communications makes intervention difficult, since offenders and victims may live under entirely different legal systems.

Anonymity is one of the most powerful enablers of digital exploitation. End to end encrypted messaging applications such as WhatsApp, Telegram, and Signal prevent third parties from accessing communication content, including platform owners themselves. While encryption is vital for privacy, it also complicates the detection of grooming, sextortion, and distribution of harmful content. Europol has repeatedly emphasised that

offenders exploit encryption to avoid surveillance and to coordinate international CSAM networks (Europol, 2019). Similarly, anonymising tools such as Tor enable offenders to access the dark web, where CSAM is distributed through hidden forums and marketplaces

Digital financial technologies further support transnational exploitation by enabling anonymous payments. Cryptocurrencies such as Bitcoin are widely used in the purchase of live streamed abuse, the exchange of CSAM, and the coordination of trafficking activities (Westlake and Bouchard, 2015). These financial technologies reduce traceability and make it more difficult for investigators to follow payment trails that would otherwise expose networks. Because cryptocurrency transactions require no central authority and operate across borders, they complicate jurisdictional questions and slow down international cooperation.

Despite these challenges, technology also plays an essential role in preventing child exploitation. Artificial intelligence tools have become central to detecting CSAM at scale. Companies such as Microsoft developed PhotoDNA, which uses image hashing to identify known CSAM even when modified or edited (Quayle, 2020). Cloud service providers and major social media platforms rely on these tools to monitor large volumes of user generated content. Although not perfect, these detection technologies have significantly increased the identification of abusive material globally.

Law enforcement agencies also use technology to strengthen cross border investigations. INTERPOL's International Child Sexual Exploitation Database stores visual material from investigations worldwide and uses image comparison software to identify victims across jurisdictions. This database has facilitated the identification of hundreds of victims by matching digital clues from different countries (Ludik, 2020). DNA analysis, digital forensics, and geolocation tools contribute to reconstructing offender behaviour patterns and supporting prosecutions in transnational cases.

Artificial intelligence has expanded beyond simple content detection to behavioural analysis. Machine learning models are used to flag suspicious communications in real time, particularly in chat rooms or gaming platforms where grooming often begins. Advanced analytics can identify grooming patterns based on language, timing, and communication frequency (Davidson & Gottschalk, 2011). Although these systems must operate carefully to avoid privacy violations, they offer promising support to moderation teams and law enforcement.

Technology is also essential in prevention efforts. Educational campaigns rely on digital

platforms to raise awareness among children, parents, and educators about online risks. UNICEF and ECPAT International have developed interactive tools, child friendly guidelines, and online safety curricula that help children recognise manipulation and report suspicious behaviour. Digital literacy programs significantly reduce vulnerability by empowering minors to understand risks and make informed choices (Livingstone & Third, 2017). In developing countries such as Pakistan, these tools are increasingly necessary due to rapid digital adoption and limited offline awareness.

Social media companies also have legal and policy responsibilities. Under the European Union's Directive on Combating the Sexual Abuse and Sexual Exploitation of Children, platforms must remove illegal content promptly and cooperate with law enforcement (Casagran, & Vermeulen, 2021). Meta, Google, and TikTok have adopted internal safety protocols, age verification tools, and reporting mechanisms to reduce exposure to abusive content; however, enforcement is often inconsistent as platforms struggle to balance privacy, profit incentives, and child safety obligations (Livingstone and Third, 2017). This challenge is compounded when platforms operating in multiple countries face conflicting legal requirements, slowing down cooperation with authorities in cross-border cases.

Although technology provides valuable tools for detection and prevention, its effectiveness depends on governance. Without clear regulatory frameworks, monitoring mechanisms, and cross border data sharing, even the most advanced technologies cannot meaningfully reduce online exploitation. Technological solutions must be paired with strong laws, trained investigators, and international partnerships to create a comprehensive digital border capable of protecting children (Gercke, 2012).

In summary, technology simultaneously facilitates and combats online child exploitation. Offenders exploit anonymity, encryption, global connectivity, and financial innovations to avoid detection and operate across borders. At the same time, governments and organisations increasingly use artificial intelligence, digital forensics, and global databases to prevent abuse and identify offenders. Understanding both aspects is essential for designing legal and policy responses that strengthen digital safeguards for children worldwide.

Challenges in Protecting Children Across Digital Borders

Despite significant advancements in law, technology, and international cooperation, protecting children from cross border online exploitation remains one of the most complex global challenges. The digital environment is borderless, while legal systems

are not. Offenders exploit inconsistencies between national laws, gaps in enforcement capacity, and delays in cross jurisdictional cooperation. This section examines the major challenges that hinder effective protection of children in a world where abuse, evidence, and perpetrators often move between countries with ease.

A central challenge is the difficulty of establishing jurisdiction, as offenders, victims, servers, and digital intermediaries are often located in different countries. This multi-jurisdictional nature of online child exploitation networks makes it difficult for any single state to assert authority (Bouchard & Westlake, 2016). Even when a state can claim jurisdiction, prosecuting an offender abroad requires international cooperation, which can be hampered by differing legal standards or limited capacity. This complexity allows offenders to exploit shifting digital locations and weak enforcement zones.

Another major challenge is the lack of timely cross border cooperation. Mutual legal assistance treaties are traditionally used to request data, evidence, or cooperation from foreign authorities, but these processes are slow and not suited to fast moving digital crimes. Europol's Internet Organised Crime Threat Assessment highlights that delays in data access severely weaken investigations into international CSAM networks (Europol, 2019). Offenders often delete accounts or destroy digital traces long before the requested information reaches investigators. In the context of child exploitation, where rapid intervention can prevent ongoing harm, these delays have serious consequences.

Differences in national legal frameworks also hinder effective protection. While many countries criminalise CSAM production and distribution, fewer have explicit offences for online grooming, live streamed abuse, or technology-facilitated trafficking. This legal fragmentation allows offenders to exploit jurisdictions with weaker or outdated laws, creating safe havens for those who operate across borders (Quayle, 2020).

Technological disparities between countries intensify these problems. High income countries often have access to advanced forensic tools, specialised cyber units, and international databases. In contrast, many developing countries lack digital forensic resources, trained investigators, and child protection units capable of handling sophisticated online crime. Low capacity environments allow organised trafficking networks to flourish because authorities cannot match the speed and sophistication of digital offenders (Garner, 2025). These capacity gaps are especially concerning in regions with large youth populations and rapid internet expansion, such as South Asia and Africa.

Another major challenge is the role of private technology companies. Although platforms

host much of the digital communication where grooming begins, many are reluctant or slow to cooperate with foreign law enforcement requests. This is often due to conflicting legal obligations, such as stringent data protection regimes like the GDPR, which clash with cross-border child protection investigations (Livingstone & Third, 2017). This tension slows evidence disclosure and frustrates efforts to identify offenders exploiting anonymity across borders.

Encryption further complicates efforts to protect children. End to end encryption prevents third party access to messages, meaning that neither law enforcement nor platforms can monitor potentially harmful conversations. While encryption is essential for privacy and security, it also restricts the detection of grooming, sextortion, and live streamed abuse. Europol (2019) warns that the rise of encrypted platforms has significantly expanded offender capabilities, allowing them to coordinate internationally without fear of interception. Law enforcement agencies must therefore navigate the delicate balance between protecting privacy and enabling access to vital evidence in child protection cases.

Another serious challenge is the persistence of the dark web, where anonymous networks enable the distribution of CSAM beyond the reach of traditional monitoring systemsDark web forums remain active hubs for offenders seeking to exchange material or connect with others involved in cross border abuse (Westlake & Bouchard, 2015). Dark web anonymity makes tracking offenders difficult, as IP addresses, payment trails, and communication logs are often concealed. Even when law enforcement infiltrates these networks, investigations may require coordination among dozens of countries, each with different investigative thresholds.

Victim identification is also hindered by the global movement of digital content. Once abusive material is uploaded, it can be copied, edited, and redistributed indefinitely across platforms and jurisdictions. Despite the aid of databases like INTERPOL's ICSE, thousands of child victims in CSAM remain unidentified due to a lack of international evidence sharing and technical challenges (Quayle, 2020). Without coordinated global strategies, these victims continue to suffer in silence while their images circulate.

Social stigma, cultural barriers, and lack of reporting mechanisms also undermine child protection efforts. In many countries, including Pakistan, families are reluctant to report online sexual exploitation due to fear of shame, community judgment, or retaliation. Underreporting is widespread in South Asia because victims often blame themselves or fear criminalisation under morality based laws (Banerjee, 2016). As a result, authorities struggle to gather accurate data and to intervene early in cases involving cross border

offenders.

Finally, the rapid evolution of technology continues to outpace legal and policy responses. Offenders adopt new tools, platforms, and communication methods faster than governments can regulate them. Emerging technologies such as the metaverse, AI-generated imagery, and deepfakes present new challenges for distinguishing real victims from synthetic content and for ensuring legal clarity. Laws must be flexible enough to adapt to new forms of exploitation while maintaining strong procedural safeguards for child protection (Gercke, 2012).

In summary, protecting children across digital borders requires more than strong national laws. Jurisdictional conflict, slow international cooperation, technological disparities, encryption, weak corporate compliance, dark web activity, and social stigma all contribute to a complex environment where offenders often remain ahead of regulators. Addressing these challenges requires harmonised international laws, specialised investigative capacity, stronger cross border collaboration, and proactive engagement with technology companies. Without such measures, the digital border will remain porous, leaving children exposed to exploitation that transcends national boundaries.

Cross Border Cooperation and the Role of International Organisations

Cross border cooperation is at the centre of global efforts to combat online child exploitation and trafficking. Since these crimes involve perpetrators, victims, servers, and financial systems that often span multiple jurisdictions, no single state can respond effectively on its own. International organisations therefore play a vital role in harmonising legal standards, facilitating information exchange, supporting investigations, and strengthening the global response through coordinated action. This section examines the key mechanisms of international cooperation and highlights the contributions of major organisations including INTERPOL, Europol, UNICEF, ECPAT International, and the WeProtect Global Alliance.

INTERPOL and Europol are pivotal in facilitating cross-border investigations. INTERPOL's International Child Sexual Exploitation (ICSE) database uses image comparison software to identify victims and offenders across jurisdictions. Europol's European Cybercrime Centre provides similar support, coordinating multinational operations that often involve offenders in Europe and victims in other regions (Europol, 2019). Its annual Internet Organised Crime Threat Assessment is also instrumental in shaping global policy awareness (Baines, 2019).

The United Nations also plays a significant role in setting global standards. The United Nations Office on Drugs and Crime supports member states in implementing the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, and provides technical assistance to harmonise national laws. UNODC has published guidelines on the investigation and prosecution of technology facilitated trafficking, urging stronger digital evidence frameworks and international cooperation (UNODC, 2008). These guidelines recognise that trafficking networks increasingly use online recruitment and encrypted communication, requiring states to adapt investigative techniques beyond traditional trafficking paradigms.

UNICEF contributes by developing child rights frameworks, advocating for better legal protections, and supporting national action plans against online abuse. Through initiatives such as the Global Partnership to End Violence Against Children, it collaborates with states to build child-safe digital ecosystems, promoting age-appropriate design, reporting mechanisms, and awareness programs. UNICEF's collaborations in South Asia have encouraged states like Pakistan to strengthen online safety education and update their child protection strategies (Livingstone and Third, 2017).

ECPAT International, one of the oldest global child protection networks, plays a research and advocacy role by monitoring trends, supporting survivor centred policies, and assisting national coalitions that combat sexual exploitation. ECPAT's country reports provide detailed assessments of legal frameworks, enforcement gaps, and emerging online threats in low and middle income countries. These reports have influenced legislative reforms and guided governments in modernising their responses to online grooming, CSAM, and trafficking (ECPAT International, 2020). ECPAT is frequently recognised for bridging gaps between civil society and government, allowing coordination that would otherwise be difficult in resource constrained environments.

The WeProtect Global Alliance unites over one hundred countries, tech companies, and civil society groups. Its Model National Response provides a benchmark framework for states to strengthen law enforcement, victim support, and industry cooperation (Baines, 2019). The Alliance also facilitates crucial dialogue between governments and technology companies to resolve tensions regarding data access and child protection.

Technology companies themselves are now recognised as essential partners in international cooperation. Platforms such as Meta, Google, and Microsoft collaborate with global law enforcement through industry networks like the Technology Coalition, which develops tools to detect CSAM and coordinates responses to emerging threats.

Microsoft's PhotoDNA, which creates digital hashes of known abuse material, has been widely adopted by companies and supported law enforcement investigations around the world. Partnerships between technology companies and international organisations significantly increase detection capacity and contribute to faster identification and removal of CSAM (Quayle, 2020).

Despite these advances, significant challenges remain. Variations in privacy laws and national procedures complicate cross-border evidence sharing, while mutual legal assistance is often slow. Cooperation with technology companies can be hampered by conflicting legal obligations and a reliance on voluntary compliance (Livingstone & Third, 2017). Furthermore, many developing countries lack the technical infrastructure to participate effectively in multinational investigations.

In sum, international organisations play an indispensable role in building legal and operational bridges between national systems. Their contributions range from setting global standards and conducting multinational investigations to supporting capacity building and industry cooperation. However, these mechanisms require continuous strengthening to keep pace with evolving technologies and increasingly sophisticated offender networks. Without sustained global collaboration, the digital border will remain vulnerable, allowing cross border exploitation to thrive in the gaps between national jurisdictions.

Pakistan's Response: Laws, Challenges, and Opportunities

Pakistan, like many developing countries, faces considerable challenges in responding to cross border online child exploitation. The rapid expansion of internet access, widespread use of smartphones, and limited digital literacy among children have created new vulnerabilities. While Pakistan has introduced important legislative and institutional measures, gaps in implementation, enforcement capacity, and international cooperation continue to constrain the effectiveness of its response. This section evaluates Pakistan's legal framework, operational structures, and ongoing challenges, while highlighting opportunities for strengthening child protection in the digital environment.

The primary legislative instrument addressing online child exploitation in Pakistan is the Prevention of Electronic Crimes Act (PECA) 2016. PECA criminalises offences such as the production, distribution, and possession of child sexual abuse material, recruitment or inducement for sexual exploitation, and the use of information systems for trafficking. PECA marked an important shift by recognising offences that take place entirely within

digital spaces and by empowering the Federal Investigation Agency to investigate cybercrimes (Iftikhar, 2023). However, PECA's provisions do not comprehensively address emerging forms of abuse such as live streamed exploitation, sophisticated grooming through encrypted platforms, or transnational sextortion networks.

Pakistan has additional legal protections under the Zainab Alert, Response and Recovery Act 2020, which established a national alert system for missing and abducted children. Although the Act enhances coordination between law enforcement agencies, it focuses primarily on physical abduction rather than online exploitation. Furthermore, the Pakistan Penal Code criminalises sexual exploitation and trafficking, while the Prevention of Trafficking in Persons Act 2018 provides procedures for prosecuting traffickers. Yet these laws are still grounded in traditional understandings of trafficking and do not fully incorporate contemporary patterns of digital recruitment and online facilitation (Khan et al., 2025).

Institutionally, the Federal Investigation Agency's Cyber Crime Wing is responsible for investigating online child exploitation. The Wing has expanded its forensic laboratories, reporting mechanisms, and digital investigation units in recent years. However, limited staffing, high case volume, and outdated equipment remain major obstacles. Most cybercrime investigators lack specialised training in CSAM investigations, digital forensics, and dark web monitoring, reducing their ability to address cross border networks effectively (Haque et al., 2023). These capacity constraints are exacerbated by limited cooperation with foreign authorities and technology companies, which often delays access to crucial digital evidence.

Pakistan's ability to respond effectively is also hindered by social and cultural barriers. Underreporting is widespread due to stigma, fear of social backlash, and distrust in law enforcement. Families often avoid reporting online sexual offences because they fear reputational harm, and victims may be reluctant to disclose abuse due to shame or fear of being blamed. Pakistan's cultural context, combined with insufficient awareness of online risks, results in very few cases being reported compared to the growing scale of digital exploitation (Mehmood, 2025).

Another challenge arises from jurisdictional conflicts between federal and provincial authorities. While PECA authorises federal investigation of cybercrimes, child protection is primarily a provincial responsibility under Pakistan's devolved governance structure. This division creates institutional fragmentation that complicates coordinated responses. Child protection units in provinces such as Punjab, Sindh, and Khyber Pakhtunkhwa often lack mechanisms for sharing information with federal cybercrime

investigators, limiting their ability to intervene in cases involving both online and offline exploitation.

Despite these challenges, significant opportunities exist. Pakistan's participation in regional organisations like SAARC, combined with its interest in aligning cyber laws with international standards, could enhance collaboration with bodies like INTERPOL and the WeProtect Global Alliance. Strengthening partnerships with global technology companies would also improve access to digital evidence and enable faster removal of CSAM.

Investing in capacity building is another critical opportunity. Training for investigators, prosecutors, and judges in digital forensics and cross-border evidence handling would enhance prosecutions. Concurrently, expanding digital literacy programs in schools, through collaboration with UNICEF and civil society, is crucial for reducing children's vulnerability (Livingstone & Third, 2017).

Overall, while Pakistan has established a legal foundation for addressing online child exploitation, stronger institutional capacity and expanded international cooperation are essential. Modernizing laws, investing in training, and deepening global collaboration are key to enhancing its digital border and protecting its most vulnerable citizens.

Recommendations for Strengthening Digital Borders

Strengthening the digital border demands a multi-layered approach that integrates legislative reform, capacity building, technological innovation, and international cooperation. This framework helps states, including Pakistan, enhance their capacity to prevent, investigate, and respond to cross-border online child exploitation.

1. Legislative Harmonisation and Legal Reform:

A foundational step is harmonising national laws with international standards. Countries must adopt clear legal definitions of online grooming, CSAM, and live-streamed exploitation. Pakistan should update PECA to criminalize AI-generated abuse material and exploitation on encrypted platforms. Aligning domestic laws with frameworks like the Budapest Convention improves legal clarity and cross-border cooperation.

2. Enhancing Cross-Border Investigative Capacity:

Effective response requires robust cross-border mechanisms. States should prioritize expanding participation in INTERPOL's ICSE database and establishing regional information-sharing networks. To overcome slow MLATs, dedicated 24/7 points of

contact between national cybercrime units are essential. Building institutional capacity requires investment in modern digital forensic labs, specialized training in dark web monitoring, and dedicated child protection units.

3. Regulating Technology Platform Accountability:

A "Safety by Design" legal mandate should require platforms to integrate content detection tools, age-verification systems, and accessible reporting mechanisms. Governments must formalise partnerships with industry through frameworks outlining mandatory reporting obligations for detected CSAM, ensuring timely data sharing with law enforcement. Independent audits of platform safety should be mandated.

4. Proactive Prevention through Education and Awareness:

Enhancing digital literacy is a critical pillar of prevention. A structured online safety curriculum must be integrated into national standards, teaching skills to recognize grooming tactics. Parallel awareness campaigns for parents provide guidance on online risks. In Pakistan, community outreach led by trusted local NGOs is vital to combat stigma and encourage reporting.

5. Implementing Survivor-Centred Support Systems:

A victim's journey does not end with an investigation. This involves establishing multi-disciplinary teams that provide crisis intervention, trauma-informed mental health care, and legal advocacy. Child-friendly interview facilities and specialized training for judiciary are crucial to prevent re-victimization during legal proceedings.

6. Fostering Proactive Adaptation to Emerging Technologies:

States must adopt proactive regulatory approaches for frontier threats like the metaverse and deepfakes. Establishing national advisory committees with technologists and child rights advocates can provide ongoing threat assessment. Investing in next-generation detection tools ensures protective measures evolve with the threats.

Conclusion

The rise of digital technologies has created a borderless landscape for child exploitation, challenging traditional legal and institutional frameworks. This paper has detailed how online grooming, sextortion, and live-streamed abuse are facilitated by global connectivity and anonymity. These crimes, driven by offenders who exploit the digital world's lack of borders, demand a response that is equally global, coordinated, and comprehensive.

International organisations have been essential in shaping this response. INTERPOL's databases, UNICEF's child-centred advocacy, and the WeProtect Global Alliance's frameworks highlight that isolation is not an option. Strong cross-border cooperation, harmonised laws, and rapid information sharing are indispensable. However, these global efforts must be matched by robust domestic action. National laws must evolve with emerging technologies, and states must invest in specialised investigative capacity, digital literacy programs, and survivor-centred support.

Pakistan's experience mirrors that of many developing nations, demonstrating that a legal foundation, while crucial, is insufficient without effective implementation, institutional capacity, and societal trust. Ultimately, building an effective digital border is a collective moral responsibility. It requires sustained commitment from governments, international organisations, technology companies, and communities. Only through coordinated action, continuous innovation, and an unwavering child-centred approach can the digital world be made safer for all children.

BIBLOGRAPHY

Baines, V. (2019). Online child sexual exploitation: towards an optimal international response. *Journal of Cyber Policy*, *4*(2), 197–215. https://doi.org/10.1080/23738871.2019.1635178

Bouchard, M., & G. Westlake, B. (2016). Criminal Careers in Cyberspace: Examining Website Failure within Child Exploitation Networks. *Justice Quarterly*, *33*(7), 1154–1181. https://doi.org/10.1080/07418825.2015.1046393

Council of Europe. (2007). *Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse: Lanzarote, 25. X. 2007*. Council of Europe.

Davidson, J., & Gottschalk, P. (2011). Internet Child Abuse. Current Research and Policy, 43. ECPAT International. (2020). Online child sexual exploitation: A summary paper for the World Congress on Justice With Children. ECPAT International. Retrieved from https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf

Europol (2019). Internet Organised Crime Threat Assessment. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

Gercke M. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. International Telecommunications Union.

Chatzinikolaou, A., & Lievens, E. (2019). A legal perspective on trust, control and privacy in the context of sexting among children in Europe. *Journal of Children and Media*, *14*(1), 38–55. https://doi.org/10.1080/17482798.2019.1697320

Livingstone, S. and 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. J Child Psychol Psychiatr, 55: 635-654. https://doi.org/10.1111/jcpp.12197

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, *19*(5), 657-670. https://doi.org/10.1177/1461444816686318

Quayle, E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. *ERA Forum* **21**, 429–447. https://doi.org/10.1007/s12027-020-00625-7

UN General Assembly. 2000. "Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography." https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child.

United Nations Office on Drugs and Crime. (2008). Toolkit to combat trafficking in persons. https://www.unodc.org/documents/human-trafficking/HT-toolkit-en.pdf

G. Westlake, B., & Bouchard, M. (2015). Criminal Careers in Cyberspace: Examining Website Failure within Child Exploitation Networks. *Justice Quarterly*, *33*(7), 1154–1181. https://doi.org/10.1080/07418825.2015.1046393

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and violent behavior*, *18*(1), 62-70. https://doi.org/10.1016/j.avb.2012.09.003

Danial, S. (2025, November 3). *Are we doing enough to protect our children online?* Retrieved from https://www.dawn.com/news/1952821

Comolli, V. (2025, July 3). *Organized child sexual exploitation: Addressing motives and response needs in South East Asia*. Global Initiative Against Transnational Organized Crime. Retrieved from https://globalinitiative.net/analysis/organized-child-sexual-exploitation/#:~:text=Crackdowns%20in%20the%20physical%20realm,more%20sophisticated%2C%20networked%2C%20and%20organized

Ali, M. I. (2025). *Beyond borders: The case for hybrid tribunals in tackling online child sexual exploitation in India and Pakistan.* IUS Law Journal, 4(1). https://www.researchgate.net/publication/393090568_BEYOND_BORDERS_THE_CASE_FOR_HYBRID_TRIBUNALS_IN_TACKLING_ONLINE_CHILD_SEXUAL_EXPLOITATION_IN_INDIA_AND_PAKISTAN

Khan, Z., Kamaluddin, M. R., Manap, J., Rajaratnam, S., Mohd, M., & Chong, I. M. (2025). *Exploring the role of technology in human trafficking in Pakistan: A qualitative study of lived experiences of victims.* PLOS ONE, 20(3). https://doi.org/10.1371/journal.pone.0320088

WeProtect Global Alliance. (2023). The global threat assessment 2023: Analysis of the sexual threats children face online. Retrieved from https://www.weprotect.org/global-threat-assessment-23/analysis-sexual-threats-children-face-online/

Bashir, L. (2025). A Crisis of Enforcement: Corruption, Weak Institutions and the Invisibility of Human Trafficking Victims and Pakistan. *Insights of Pakistan, Iran and the Caucasus Studies*, *4*(2), 86-107.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of minors: Characteristics and dynamics. *Journal of Adolescent Health*, *62*(1), 72-79. https://doi.org/10.1016/j.jadohealth.2017.08.014

Popa, L. (2024). National and international cooperation in investigating crimes of child

sexual abuse or sexual exploitation committed by using information technologies. Agora International Journal of Juridical Sciences, 18(1), 102–111. https://doi.org/10.15837/aijjs.v18i1.6747

Ludik, P. S. (2020). Interpol review papers special edition preface. *Forensic Science International: Synergy*, *2*, 351. https://doi.org/10.1016/j.fsisyn.2020.01.006

Yusran, R. (2018). The ASEAN Convention Against Trafficking in Persons: A Preliminary Assessment. *Asian Journal of International Law*, *8*(1), 258–292. https://doi:10.1017/S2044251317000108

Ullah, H. M. H., & Bakhsh, F. (2024). Socioeconomic and Cultural Factors and Juvenile Delinquency in Pakistan: A Critical Analysis of Structural Theories. *Current Trends in Law and Society*, *4*(1), 101–109. https://doi.org/10.52131/ctls.2024.0401.0037

Iftikhar, B. (2023). Digital Crime Scenes: Protecting Children from Sexual Exploitation in Pakistan. *Available at SSRN 5007631*. https://dx.doi.org/10.2139/ssrn.5007631

BANERJEE, P. (2016). Criminalising the Trafficked: Blaming the Victim. *Economic and Political Weekly*, *51*(44/45), 62–68. http://www.jstor.org/stable/44166669

Khan, Z., Kamaluddin, M. R., Manap, J., Rajaratnam, S., Mohd, M., Chong, I. M., ... & Setiyani Subardjo, R. Y. (2025). Exploring the role of technology in human trafficking in Pakistan: A qualitative study of lived experiences of victims. PloS one, 20(3), e0320088. https://doi.org/10.52131/pjhss.2024.v12i1.2

Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. IEEE Access, 11, 40049-40063. https://doi:10.1109/ACCESS.2023.3268529

Bokhari, S. A. A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social Sciences*, *12*(11), 629. https://doi.org/10.3390/socsci12110629

Lykousas, N., & Patsakis, C. (2025). Just in Plain Sight: Unveiling CSAM Distribution Campaigns on the Clear Web. *arXiv preprint arXiv:2511.03816*. https://arxiv.org/html/2511.03816v1

Garner, D. (2025). Protecting children in the digital age. *Police Chief Magazine*. https://www.policechiefmagazine.org/protecting-children-digital-age

Casagran, C., & Vermeulen, M., (2021). Reflections on the murky legal practices of political micro- targeting from a GDPR perspective. International Data Privacy Law, 11(4), 402. https://doi.org/10.1093/idpl/ipab018

Human Trafficking Front. (2023, July 14). *The Use of the Internet to Recruit Children by Traffickers.* https://humantraffickingfront.org/the-use-of-the-internet-to-recruit-children-by-traffickers/

Ruellan, L. M. (2023). *The sexual exploitation of children in the digital age. An overview of a major phenomenon in Southeast Asia.* Master's Thesis, Università di Pavia. https://unitesi.unipv.it/fragment/handle/20.500.14239/26134

Mehmood, M. (2025). The Role of Cyber Security in Promoting Digital Inclusion: A Case Study of Pakistan. *Annals of Human and Social Sciences*, *6*(1), 35–44. https://doi.org/10.35484/ahss.2025(6-I)04