MSI Journal of
Arts, Law and Justice (MSIJALJ)

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

Sameer Haider[1*]

[1*]Director Child Protection at FIKER.

*** Correspondence:** Sameer Haider

The authors declare that no funding was received for this work.

ABSTRACT: Digital communication has led to new opportunities of cross border online exploitation and child trafficking. It is the use of social media sites, chat rooms and online gaming sites where offenders would get in touch, groom and exploit children on a cross-country basis without necessarily crossing a border. This paper will discuss the content of this kind of online harm, children vulnerability, and the difficulty in preventing and investigating such crimes because of the absence of cooperation among nations. It equally discusses the contributions made by states, international institutions and online platforms in establishing safer online spaces. The study identifies scholarly literature, cross-border reports and legal practices that address the issue of child protection and cybercrime using a qualitative and descriptive method. It also examines the major issues such as different country laws, slow cross border investigations, data privacy and lack of technical capability in most countries. The paper further discusses the possibility of utilizing new tools like automated detection systems and faster reporting systems which may be utilized to aid in child protection without going against the privacy privileges. The article talks about how more coordination between countries, the harmonization of cyber laws, and clear policies on platforms

OPEN ACCESS

Received: 01-February-2026
Accepted: 20-March-2026
Published: 25-March-2026

This article is published by **MSI Publishers** in **MSI Journal of Arts, Law and Justice (MSIJALJ)**
ISSN 3049-0839 (Online)

The journal is managed and published by MSI Publishers

Volume: 3, Issue: 3 (March-2026)

of online shopping should be required to protect children against transnational cyber attacks. It concludes with the realistic suggestions of strengthening the prevention, reporting, investigation and support of the victims. It is intended to provoke a common and rights-based resolution to make sure that digital limits serve as a protection rather than a cause of maliciousness.

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

Introduction

Take the example of a 13 year old boy in Lahore who finds himself in the gaming chat after school. In few days, a stranger messages him with promises of virtual coins in exchange of fun pictures. The game becomes horrifying within a short time as the stranger threatens to publish the images unless the boy sends more (Danial, 2025). This is not an isolated case, but a vivid illustration of how serial killers are taking advantage of the naivety of children through the internet. These accounts highlight a pressing fact: children all over the world are more exposed to internet abuse and trafficking, and the digital border, which is the virtual border between secure and unsafe internet spaces, is permeable and poorly patrolled.

Globally, researchers indicate that child sexual abuse over the Internet is increasing at an appalling speed. Criminal networks have been able to plan advanced exploitation plans through new technologies and global connectivity. As an example, analysts observe that harmful activities such as livestreamed abuse, sextortion, and the sale of child abuse material now are run through cross border chains, involving recruiters, facilitators, and anonymous payment processors (Comolli, 2025). By doing so, the internet has virtually eliminated distance: the online exploitation of children in a country can immediately translate to multiple countries. Consequently, a recent Global Threat Assessment concludes that online child sexual exploitation continues to grow across the globe, in both size and approaches (WeProtect Global Alliance, 2023). This international crisis needs an equivalent international reaction.

It is a particularly acute issue in South Asia. In other countries such as India and Pakistan where internet has been bursting in recent years, children have been the

main victims of these crimes. The two countries, Pakistan and its neighbor India, are considered to be at high risk of online exploitation of children (Ali, 2025). Online child sexual exploitation involves grooming and cybersex to streaming of abuse live. These crimes cannot really be combated by conventional legal ways including arrest and trial, since criminals are behind screens, and even beyond borders. As these crimes are now in digital platform and are initiated cross the borders, good solutions also need to be international (Ali, 2025). Otherwise stated, the violence and child trafficking the internet enables does not observe national jurisdictions, but law enforcement and legal systems usually do.

The extent of the issue is chilling in Pakistan. Pakistan is a very young country with a median age of about 22 years, and millions of children under the age of 18 are going to the internet without much supervision. In 2022, the number of children sexually abused material cases was attributed to Pakistani users more than two million (Danial, 2025), although the national Federal Investigation Agency documented just 250 cases that year. This massive disparity is likely not a failure to report, detect, or coordinate, but an issue of problems..

According to Khan et al. (2025), Pakistan, as a major source and destination country, contributes a major percentage to global trafficking. There are approximately 2.3 million modern slavery residents. The technological aspect, which is one of the potent exploitative tools employed by traffickers, allows cross-border exploitation where victims are enticed by promising jobs and social media messages via platforms of Facebook, YouTube, and WhatsApp.

These facts constitute the gist research problem: how can law and policy be adjusted to safeguard children when the perpetrators take advantage of the unregulated borderlessness of the internet? Religionally and internationally, there is an increasing awareness that the current legal frameworks and enforcement tools are inadequate. International conventions (such as the UN Convention on the Rights of the Child and its Protocols) recognize the rights of children, yet jurisdictional and operational flaws in cross border prosecutions are common. Even advanced national legislation, as Ali (2025) notes, is ineffective since criminals operate in technical ways to stay a secret and move around (Ali, 2025). In the Pakistan context, the Prevention of Electronic

Crimes Act (2016) includes provisions of punitive measures to online child exploitation, although the application is disjointed and poorly staffed. In Pakistan, the unreported number of cases is also due to social stigma and mistrust towards the law enforcement agencies (Bashir, 2025). It is against this background that new models of legal cooperation and prevention need to be pursued - metaphorically, to reinforce the digital border that protects children against such harms.

The paper represents a qualitative doctrinal research approach, which relies on the examination of international legal tools, scholarly literature, official reports, and documented case studies. Also, it applies comparative jurisprudential analysis to look at how various jurisdictions respond to cross-border online exploitation and trafficking.

This study therefore answers the following questions:

1. What do you think are the most important legal and policy issues related to combating transnational in the exploitation and trafficking of children online?
2. What does the current international conventionions and domestic legislation (in Pakistan and other countries) have to play in the protection of children on the internet?
3. How would enhanced protection be enhanced with what best practices or new models of digital cooperation?

The study objectives are:

-Visualize the extent of cross border internet child exploitation and trafficking based on international statistics and case studies.

- Evaluate and appraise existing legal tools and implementation policies at the international, regional and Pakistani levels.

- Uncover loopholes and suggest practical recommendations on legal intervention, technological protection, and intersectoral cooperation to help avert cyber-crimes against children.

Through these questions and aims the paper will shine some light on how to redefine the digital world as a haven of predators to a less harmful place to the children in Pakistan and also globally.

Understanding Cross Border Online Child Exploitation and Trafficking

Cross border online child exploitation and trafficking is one of the most dynamic and complicated crimes in the digital era. The crimes include digital platform grooming, coercing, exploiting, or trafficking children between jurisdictions with sexual or other exploitative motives. Since online communications have no national borders, perpetrators have an opportunity to assault kids in other countries without revealing their identities and whereabouts. This has changed the localised social harm of child exploitation into a transnational crime issue that has challenged law enforcement agencies, policy makers, and child protection systems in all parts of the world.

One of the fundamental aspects of online exploitation is grooming, meaning the process with the help of which perpetrators create emotional connections with children to control their trust and diminish their willingness to go along with abusive demands. Social media, gaming platforms, or messaging applications often seem as simple conversation beginnings that lead to grooming. Attackers tend to stick to a scenario of evaluating vulnerability, emotional isolation, and the progressive introduction of sexual content (Whittle et al., 2013). Such interactions are usually secret and hidden, and they are harder to detect. This means that a number of children fail to notice that they are being manipulated until the abuse has grown.

Sextortion, where children are threatened to send explicit pictures or videos or face exposure, humiliation, or harm, is another common type of exploitation. Sextortion is a world phenomenon because offenders are able to collect, copy and spread content with ease. In the recent years, online sextortion offenses have grown enormously, and the offenders living in various regions victimize minors who can hardly resist or report such a threat (Wolak and Finkelhor, 2018).

Another characteristic of cross border online exploitation is the development and distribution of child sexual abuse material (CSAM). CSAM may contain pictures, videos, or the live abuse of minors. Previously, this kind of material circulated in

underground networks, although offenders are turning to mainstream outlets, encrypted apps, and anonymised search engines where they can exchange and sell content (Quayle, 2020). The growth of digital payment networks and especially cryptocurrencies has also helped offenders in carrying out transactions in ways that cannot be tracked geographically or financially.

There has been an increasing global concern over live streamed child abuse. This entails live streaming of child sexual abuse to audiences who pay anywhere around the globe. Live streamed exploitation is especially dangerous since it enables offenders to control or guide the abuse during the process. The cases reported in the Philippines, India, Indonesia, and other nations indicate that such cases can include cross border clients who demand particular acts remotely when torturing the child in another country (ECPAT International, 2020). This type of exploitation combines digital anonymity, as well as real time violence, with the hottest global child protection problem's.

Online exploitation also overlaps with cross border trafficking. Digital platforms have become increasingly popular in recruiting, advertising or moving children across borders to be sexually exploited. Online advertisements, social media recruitment, or even fake employment opportunities can be used by the offenders to attract the children who are vulnerable. To organize the flow and hide cross-border operations, trafficking networks in South Asia use digital communication extensively to organize the movement (Human Trafficking Front, 2023). After transportation, their photo or mistreatment can be captured and circulated across borders, thus increasing the exploitation network even further.

Criminals are using various hi-tech methods to avoid being caught. Some of them use Virtual Private Networks to conceal their locations, end-to-end encrypted messaging applications to communicate in a secure manner, and anonymizing browsers including Tor to visit dark web markets where CSAM is stored or traded. The dark web boasts a wide variety of groups that deal with the sharing of abuse content and cross border offender networks that are inaccessible to ordinary policing (Lykousas and Patsakis, 2025). Cryptocurrency wallets facilitate financial anonymity,

and in this case, investigators can hardly track the payments related to exploitation or trafficking.

There is a combination of developmental, psychological, and socioeconomic factors that contribute to the vulnerability of children. Children who are still young do not always understand how to recognize the dangers of the Internet, and adolescents can be easily groomed because of the sense of insecurity and the need to be validated (Livingstone and Smith, 2014). This is further exacerbated by the overall lack of digital literacy and shame-based fears that do not encourage reporting. Children in disadvantaged groups have an increased risk socioeconomically due to a lack of parental care, access to safety education, and financial constraints. Criminals target these children actively and calculate that their families are neither able nor aware of seeking assistance (Ullah and Bakhsh, 2024).

The seriousness of this borderless crime is reinforced by real-life incidences. In 2019, a major cross-continental CSAM ring that was dismantled by a 2019 Europol operation demonstrated the international nature of such digital rings of exploitation (Europol, 2019). Likewise, South Asian law enforcement efforts have interfered with trafficking organizations that mobilize cross-border trafficking of minors with the help of such platforms as WhatsApp and Telegram (Ruellan, 2023), and Pakistan records an increase in online grooming incidents associated with offshore perpetrators (Iftikhar, 2023).

Cross border online exploitation is by no means a simple cybercrime but a complex human rights infringement that borders in digital privacy, law enforcement, and international collaboration. This is critical in creating legal mechanisms that resonate with the magnitude and intensity of the threat based on its forms, methods and the root causes. The following paragraphs will dwell upon how international law instruments and domestic legislations tackle these offenses, and what changes should be introduced in order to enhance the digital boundary that secures children across the globe.

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

Cross border online child exploitation has resulted in a broad spectrum of legal action, on the international, regional and national levels. Because digital crimes often cross borders, domestic laws are often not enough to combat the international networks of grooming, trafficking and distribution of child sexual abuse material. Good regulation then must be through harmonised legal standards, cross-jurisdictional cooperation and common procedural approaches to investigation and prosecution. This section discusses the key international and regional legal tools along with the national frameworks which influence the response to online child exploitation and trafficking in the world arena.

The United Nations Convention on the Rights of the Child is one of the most fundamental tools that requires states to defend children against sexual exploitation and abuse of any kind. Article 34 mandates states to ensure that they do not induce or coerce children into illegal sexual intercourse and pornographic performances. Subsequently, the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography intensified the international commitments by obligating criminalisation of the production, distribution, dissemination and possession of child pornography, which is now legally known as child sexual abuse material (UNGA, 2000). Though it was written earlier on when digital technologies had not bursted, its clauses have been broadly construed to embrace internet exploitation at the expense of states having a legal foundation to criminalise internet related exploitation.

The most extensive international convention in the area of cyber offences is the Council of Europe Convention on Cybercrime generally referred to as the Budapest Convention. It also obligates states to criminalise child pornography, illicit access, internet grooming, and abuse content of such kind. Notably, it defines the digital evidence sharing and mutual legal assistance inter-state procedures which are critical to multi-national investigations (Gercke, 2012). Most of the provisions of the Convention have, although not directly, influenced domestic reforms in Pakistan, as the Convention is not binding on it but has propagated global policy through the process of global policy diffusion.

In addition to this, the Council of Europe Lanzarote Convention offers specific requirements on the criminalisation of internet grooming, solicitation, and live streamed exploitation. It asks states to implement preventive and protective measures, such as education on internet safety and specific training of investigators (Council of Europe, 2007). The Convention is generally discussed as a contemporary tool since it specifically tackles contemporary manifestations of online exploitation such as technology facilitated grooming. Lanzarote Convention bridges existing gaps in the past treaties that failed to foresee the magnitude of digital abuse (Davidson and Gottschalk, 2011).

The European Union has formulated a comprehensive legislative framework to address the exploitation of children on the internet at the regional level. The EU Directive on the Fight against Sexual Abuse and Sexual Exploitation of children establishes the minimum criminal law standards and obliges member states to criminalize grooming, CSAM distribution, and live streamed abuse. The Directive also mandates service providers to collaborate with the authorities in taking down illegal material (Chatzinikolaou & Lievens, 2019). The European Union has as well invested in cross border operations through coordination of these activities by the Europol which often mentions networks that are running concurrently in Europe, Asia and Africa.

The ASEAN region also embraced the ASEAN Convention against Trafficking in Persons, especially Women and Children, which criminalises trafficking and places the requirement of states to enhance cross border coordination. Even though it does not specifically address the issue of digital exploitation, its provisions are also being viewed through the lens of online recruitment and abuse (Yusran, 2018). The recent recognition of the emergence of digital trafficking by the member states of ASEAN has now resulted in changes in the national laws to accommodate the trends.

International organisations have also played a great role in formulation of legislative and policy frameworks to curb online exploitation. International agencies such as UNICEF, ECPAT, and INTERPOL give valuable recommendations and operational assistance. The International Child Sexual Exploitation database by INTERPOL is highly utilized in police agencies to identify victims and perpetrators that cross

national boundaries. Hundreds of children were rescued, and traffickers acting in the online networks were arrested following the cross border operations eased by INTERPOL (Popa, 2024).

At the national level, most countries have revised their criminal laws, cybercrime and child protection laws to be in line with international standards. The Sexual Offences Act of the United Kingdom, the Criminal Code of Australia and the Criminal Code of Canada have broad offences in relation to grooming, CSAM, exploitation via digital communication and possessing illegal material. The US has passed the PROTECT Act and associated laws that allow federal jurisdiction over cases on international online exploitation. These domestic reforms show the ways states integrate international commitments into national systems..

South Asian countries that are developing have also improved. Pakistan The Prevention of Electronic Crimes Act of Pakistan has created the legal framework upon which criminal prosecution of online child abuse material, exploitation and recruitment to be trafficked can occur. Nevertheless, the effectiveness of these laws is still hampered by the implementation issues, the absence of specialised training, and insufficient digital forensic capabilities (Bokhari, 2023). The delays in courts getting evidence of foreign service providers are common and mutual legal assistance procedures are also slow. This has made numerous cross border criminals evade local prosecution.

Even though the global legal environment has come a long way, it still has serious gaps. There are different standards of prosecution due to the differences in definitions of child sexual abuse material across jurisdictions. Certain states make collaborating with CSAM a crime and other criminalize only its production or selling. The legal reaction to live streamed abuse is disproportionate and most countries do not have laws that specifically combat online grooming. Lack of harmonised definitions and processes means that offenders can take advantage of legal loopholes by functioning in states with weaker structures (Westlake and Bouchard, 2015).

The second one is a significant limitation of efficient collaboration between states and privately owned technology firms. Even though most companies have reporting

requirements, the deletion of unlawful content is not consistent, and some websites are not fast to respond to foreign court orders (Livingstone & Third, 2017). The jurisdiction also becomes a problem where the server, offender and victim are in various countries and it is no longer straightforward to collect evidence using the domestic law.

In general, both international and regional legal frameworks have established powerful platforms against cross border online child exploitation. Criminalisation and cooperation have their normative basis in the form of treaties like the CRC, the Optional Protocol, the Budapest Convention, and the Lanzarote Convention. These obligations are supplemented by regional instruments and national laws, but enforcement and harmonisation are still very important issues. With the changing nature of online exploitation, the law will continually change to provide an opportunity to protect children in a more globalized digital space.

Role of Technology in Facilitating and Preventing Online Child Exploitation

Technology has a two-fold role in the contemporary child protection environment. On the one hand, online platforms, encrypted tools of communication, and anonymising technologies have made offenders able to find children across borders with ease never before seen. Conversely, the technological advancements have also enhanced the ability of law enforcement agencies, civil society organisations as well as governments to identify, stop as well as examine offenses that involve online exploitation. This duality is critical in developing a successful digital border that protects children in the world of global interactions.

Electronic communication media have greatly increased the reach of offenders. Social networks, games, and conversations allow real-time contact between strangers and children, frequently without the parental control (Whittle et al., 2013). The interactive quality of these websites provides a possibility of long-term manipulation, which can develop into coercion or abuse. Cross border character of such communications complicates intervention, as both criminals and victims might be subject to completely different laws.

One of the strongest enablers of digital exploitation is anonymity. WhatsApp, Telegram, and Signal are end to end encrypted messaging apps that ensure the content of communication stays confidential to third parties, including the owners of the platform. Although encryption is crucial to privacy, it makes grooming, sextortion and distribution of harmful content harder to detect. Europol has already stressed on several occasions that criminals use encryption to escape surveillance and to organize international CSAM networks (Europol, 2019). On the same note, anonymisation software like Tor allows criminals to browse the dark web, where CSAM is sold via secret forums and markets.

New technologies Digital financial technologies also facilitate transnational exploitation through anonymity of payments. Bitcoin and other cryptocurrencies are commonly used to buy live streamed abuse, trade with CSAM and organize trafficking (Westlake and Bouchard, 2015). These monetary technologies decrease traceability and complicate the process of the investigator to track payment trails which would otherwise uncover networks. Since cryptocurrency transactions do not involve any central authority and operate internationally, they make jurisdictional issues more complex and make international collaboration slower.

Nonetheless, technology is also crucial in stopping the exploitation of children. The use of artificial intelligence tools has risen to the forefront in the detection of CSAM at scale. Firms like Microsoft were able to come up with PhotoDNA, a system based on image hashing to recognize familiar CSAM even after editing or editing it (Quayle, 2020). These tools are used by cloud service providers as well as major social media platforms to screen high rates of user-generated content. These detection tools have not proved to be flawless but have greatly enhanced the detection of abusive content around the world.

Technology is also employed by law enforcement agencies in enhancing cross border investigations. The International Child Sexual Exploitation Database of INTERPOL contains visual evidence of all investigations of this type in the world and compares images with the software to find victims across the borders. This database has helped single out hundreds of victims based on digital hints across various nations (Ludik, 2020). DNA analysis, digital forensics, and geolocation tools would assist in

rebuilding offender behavioural pattern and carrying prosecutions in transnational offences.

AI has gone past the content detection to behavioural analysis. Machine learning algorithms are employed to label suspicious messages as soon as they happen, specifically in chat rooms or video games where grooming frequently starts. Effective analytics are able to detect grooming habit according to the language, timetable and frequency of communication (Davidson and Gottschalk, 2011). Even though such systems should be used with caution to prevent privacy breaches, they can successfully aid moderation teams and the police.

Prevention efforts also require technology. The educational campaigns are based on online platforms to sensitize children, parents, and teachers on online dangers. UNICEF and ECPAT International have created interactive tools, child friendly guidelines, and online safety curricula that aid children to identify manipulation and report suspicious actions. Digital literacy initiatives cut vulnerability down to size by giving the minors the power to navigate risks and make informed decisions (Livingstone and Third, 2017). In emerging market like Pakistan, these devices are becoming a necessity because of high rate of digital adoption and little offline awareness.

Companies in the social media sector too have legal and policy responsibility. According to the Directive on Combating the Sexual Abuse and Sexual Exploitation of Children under the European Union, the platforms have to delete the illegal content as soon as possible and cooperate with law enforcement (Casagran, & Vermeulen, 2021). Internal safety measures, age checks, and reporting features have been implemented at Meta, Google, and Tik Tok in order to decline access to abusive content, but these measures are not consistently enforced because the companies have to manage privacy, profit motives, and child protection duties (Livingstone and Third, 2017). This issue is exacerbated when such platforms with operations in more than one country have to comply with conflicting laws, which hinders collaboration with law enforcement in cross-border cases.

Though technology holds useful resources to detect and block it, the success of technology requires governance. Even the most sophisticated technologies cannot help in any meaningful way to reduce online exploitation unless there are clear regulatory frameworks, monitoring mechanisms, and the exchange of data across borders. The technological solutions should be accompanied by powerful laws, trained investigators, and intercontinental relationships to establish an integrated digital border that can safeguard children (Gercke, 2012).

To conclude, technology is both perpetrating and fighting online child exploitation. Criminals take advantage of anonymity, encryption, world connectivity, and financial innovations to cross-border and escape capture. Simultaneously, the role of artificial intelligence, digital forensics, and international databases in preventing abuse and locating criminals becomes more and more popular among governments and organisations. Both views are critical to the development of legal, policy solutions that would enhance digital protection of children across the world.

Challenges in Protecting Children Across Digital Borders

Although it has made great progress in the law, technology, and international collaboration, child defense against cross border online exploitation is one of the most complicated problems worldwide. The online world is borderless whereas law systems are not. Offenders take advantage of differences in national laws, inadequacies in enforcement capabilities, and cross jurisdictional lag times. This section discusses some of the key challenges that impede effective protection of children in a world where abuse, evidence, and perpetrators are free to move across countries with relative ease.

One of the main issues is that it can be hard to determine the jurisdiction because sometimes the offenders, victims, servers and digital intermediaries may be in different states. This transnational quality of online child exploitation networks renders it challenging to make any single state take control (Bouchard and Westlake, 2016). Prosecuting a criminal in a foreign state despite the ability of a state to exercise its jurisdiction is a matter of international collaboration, which can be

hindered by legal differences or insufficient ability. This dynamism enables offenders to take advantage of changing digital places and lax enforcing areas.

The second issue of concern is the absence of timely cross border cooperation. The standard ways to seek data, evidence, or cooperation with foreign authorities are through mutual legal assistance treaties, which are slow and inappropriate to fast moving digital crimes. According to the Internet Organised Crime Threat Assessment released by Europol, any delay in data access devastates the investigations of international CSAM networks (Europol, 2019). Criminals have a habit of deleting accounts or erasing digital footprint well before the information being requested is delivered to the investigators. These delays are severe in the context of child exploitation when time can be used to avoid future damage.

The variation in national legal settings is also an impediment to successful protection. Although most countries have criminalised the production and distribution of CSAM, fewer of them explicitly criminalise online grooming, live streamed abuse, or technology-facilitated trafficking. Such legal fragmentation enables criminals to seek the jurisdictions that have less effective or out of date laws, providing safe havens to those who manipulate cross-border activities (Quayle, 2020).

The problems are exacerbated by technological differences among nations. Advanced forensic tools, specialised cyber units, and international databases are often available to high income countries. Conversely, most developing nations do not have digital forensic tools, trained investigators, and child protection departments that can deal with complex cybercrime. The existence of low capacity environments enables the activity of organised trafficking networks, since law enforcement is unable to keep up with the pace and complexity of online criminals (Garner, 2025). Such capacity gaps are particularly noteworthy in areas that have a high number of youth and a high rate of internet growth like South Asia and Africa.

The other significant obstacle is the role of the private technology companies. Though platforms are the main arena of much of the digital communication in which grooming starts, many are unwilling or slow to comply with foreign law enforcement

requests. This is usually because of competing legal requirements, including some of the strictest data protection laws, including the GDPR, which do not align with cross-border child protection inquiry (Livingstone and Third, 2017). Such tension makes evidence disclosure slow and frustrating to track down offenders who are taking advantage of anonymity beyond their borders.

Encryption also makes it hard to protect children. End to end encryption does not allow any third party to access messages, and thus, law enforcement or platforms can not keep track of potentially harmful conversations. Although encryption is vital to privacy and security, it limits grooming, sextortion, and live streamed abuse. Europol (2019) cautions that the emergence of encrypted platforms has greatly enhanced the powers of offenders who are now able to organize at the international level without the fear of interruption. The law enforcement agencies are thus forced to balance between privacy protection and access to essential evidence in cases involving child protection..

The existence of the dark web where anonymous networks allow the dissemination of CSAM that cannot be detected through the standard monitoring systems is another major obstacle (Westlake and Bouchard, 2015). Dark web anonymity allows offenders to be hard to track, since IP addresses, payment history, and communication records are usually hidden. Even law enforcement agents who infiltrate these networks can take months of investigation to be coordinated with dozens of countries with varying investigative thresholds.

The international flow of digital information also impedes victim identification. After uploading abusive content, a copy can be endlessly reproduced, altered, and shared across sites and jurisdictions. Even with the help of databases such as the ICSE of INTERPOL, thousands of child victims of CSAM are not identified because of the absence of international evidence sharing and technical issues (Quayle, 2020). These victims are silently robbed of their lives as their pictures keep spreading unless there are coordinated global strategies.

Child protection efforts are also crippled by social stigma, cultural barriers, and absence of reporting mechanisms. Most of the countries, such as Pakistan, can hardly

record online sexual exploitation because of shame, community stigma, or retaliation. In South Asia underreporting is rife due to the tendency of victims to fault themselves or due to the threat of criminalisation in the face of morality based legislation (Banerjee, 2016). Consequently, law enforcers find it difficult to collect precise data and to act early in instances of cross border criminals.

Lastly, the massive advancement in technology is still moving faster than legal and policy adaptation. Criminals use new tools, platforms, and means of communication at a faster rate than the government can keep up. New technologies like the metaverse, AI-generated imagery, and deepfakes pose new challenges to identifying the real victim and synthetic content and enforcing the law. The laws should be dynamic to accommodate emerging exploitation patterns although highly procedural to safeguard child protection (Gercke, 2012).

Conclusively, to safeguard children beyond national boundaries, formidable domestic legislation is not enough. A complex environment where offenders usually stay ahead of regulators is caused by jurisdictional conflict, slow international cooperation, technological differences, encryption, weak corporate compliance, activity on the dark web, and social stigma. The way forward to this involves harmonised international laws, specialised investigative capability, enhanced cross border cooperation, and proactive involvement with technology companies. Without these, the digital border will be permeable, and children will be at risk of being exploited across national boundaries.

Cross Border Cooperation and the Role of International Organisations

Global efforts to fight online child exploitation and trafficking focus on cross border cooperation. No individual state can act well on its own because these are crimes that involve perpetrators, victims, servers, and financial systems that may cut across different jurisdictions. The international organisations thus contribute heavily to the harmonisation of legal standards, exchange of information, aiding of the investigation and enhancing the global response by working together. This part studies the principal processes of global collaboration and the roles of the major

organisations such as INTERPOL, Europol, UNICEF, ECPT International and the WeProtect Global Alliance.

INTERPOL and Europol play a central role in ensuring cross-border investigations. The International Child Sexual Exploitation (ICSE) database by INTERPOL is an image comparison database that assigns victims and offenders across jurisdictions. The same support is offered by the European Cybercrime Centre of Europol, which coordinates multinational efforts and usually the offenders are based in Europe and the victims are found elsewhere (Europol, 2019). Its yearly Internet Organised Crime Threat Assessment is also a factor that influences global policy awareness (Baines, 2019).

The United Nations plays a major role in global standards setting as well. The United Nations Office on Drugs and Crime assists member states in the implementation of the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography and technical assistance in harmonisation of national laws. UNODC has released recommendations on how technology enabled trafficking should be investigated and prosecuted, which recommends enhanced digital evidence structures and collaboration among states (UNODC, 2008). These principles acknowledge that trafficking organisations are increasingly employing web-based recruitment and coded communication, and states now need to revise methods of investigation outside the common paradigm of trafficking.

UNICEF can help by creating child rights models, promoting stronger legal frameworks, and encouraging the use of national action plans against online abuse. It works with states to create child-safe internet environments through programs like the Global Partnership to End Violence Against Children, enhancing age-appropriate design, reporting systems, and awareness campaigns. The partnerships that UNICEF has established with South Asian governments have prompted countries such as Pakistan to intensify the use of IT safety education and refresh their child protection policies (Livingstone and Third, 2017).

ECPAT International, being one of the oldest international child protection networks, has a research and advocacy role, keeping track of trends, promoting survivor

centred policies, and helping national coalitions to combat sexual exploitation. The country reports produced by ECPAT offer precise evaluations of the legal frameworks, areas of ineffective enforcement, and the online threats and threats that have arisen in the low and middle income countries. Such reports have led to legislative change and have informed governments in updating their actions against online grooming, CSAM, and trafficking (ECPAT International, 2020). ECPAT is often credited with closing the divide between the civil society and the government, facilitating coordination that would otherwise be challenging within resource limited spaces.

The WeProtect Global Alliance brings together more than one hundred countries, technology firms, and civil societies. Its Model National Response gives a blueprint model of how states could improve law enforcement, support victims, and industry collaboration (Baines, 2019). The Alliance also supports the essential consultation between the governments and technology corporations to overcome the tensions concerning access to data and child protection.

Technology corporations have come to be identified as key collaborators in global collaboration. To combat such activities, platforms like Meta, Google, and Microsoft partner with law enforcement across the world through industry associations (like the Technology Coalition), which creates tools that identify the presence of CSAM and facilitate responses to new threat types. PhotoDNA, a Microsoft-created system that makes digital hashes of known abuse content, has gained wide acceptance among companies, has been used to aid law enforcement investigations globally. Alliances of technology firms with global organisations can greatly enhance the detection capabilities and help in quicker detection and elimination of CSAM (Quayle, 2020).

The challenges are however still critical despite these advances. Differences in privacy regulations and national practices make sharing evidence across borders difficult, and mutual legal assistance in many cases is slow. Legal contradictions between legal commitments to cooperation and reliance on voluntary regulation may impede cooperation with technology companies (Livingstone and Third, 2017). Moreover, most developing nations do not have the technical infrastructure to be involved effectively in multinational investigations.

To conclude, international organisations are essential in bridging the gaps between national systems in both legal and operative aspects. They contribute to the establishment of global standards and multinational investigations as well as contribute to capacity building and cooperation between industries. Nevertheless, these processes need persistent reinforcement in order to keep up with the changing technologies and more advanced criminal networks. In the absence of a sustained international cooperation, the digital border will be left open, and cross border exploitation will flourish in between national jurisdictions..

Pakistan's Response: Laws, Challenges, and Opportunities

Pakistan, similar to most developing nations, has a significant difficulty in reacting to online child exploitation across borders. New vulnerabilities have been exposed by the fast-growing internet access, use of smartphones, and low levels of digital literacy among children. Although Pakistan has implemented significant legislative and institutional reforms, the response is still limited by the gaps in the implementation process, enforcement capacity and international cooperation. This section reviews the legal framework, operational frameworks, and current challenges faced by Pakistan, including opportunities on how to enhance child protection in the digital space.

The main law relevant to the problems of online child exploitation in Pakistan is the Prevention of Electronic Crimes Act (PECA) 2016. The production, distribution, and possession of child sexual abuse material, recruitment or inducement to engage in a sexual exploitation, and the use of information systems to traffic are all criminalized under PECA. PECA became a significant change because it formally acknowledges offenses that occur when entirely in digital environments and gives the Federal Investigation Agency the authority to investigate cybercrimes (Iftikhar, 2023). Nonetheless, the provisions of PECA are not exhaustive in dealing with forms of abuse emerging in live streamed exploitation, advanced grooming using encrypted systems, or transnational sextortion rings.

Other legal safeguards are the Zainab Alert, Response and Recovery Act 2020 that instituted a national system of alerting in the case of missing and abducted children

in Pakistan. Though the Act can be seen as improving the coordination of law enforcement agencies, it is more concerned by physical abduction and less by online exploitation. Moreover, the Prevention of Trafficking in Persons Act 2018 and the Pakistan Penal Code criminalize sexual exploitation and trafficking, and procedures exist to prosecute traffickers. However, these policies continue to be based on the classical conceptions of trafficking and they fail to capture the modern trends of digital hiring and virtual facilitation (Khan et al., 2025).

On the institutional level, the Cyber Crime Wing of the Federal Investigation Agency is tasked with the investigation of online child exploitation. In recent years, the Wing has been increasing its forensic laboratories, reporting mechanisms, and units of digital investigations. Nevertheless, understaffing, over-casing, and obsolete equipment are significant challenges. A majority of cybercrime investigators do not have specialised training in CSAM investigations, digital forensics, and cross border network monitoring, and this limits their capability to target cross border networks (Haque et al., 2023). Such capacity limitations are compounded by a lack of cooperation with foreign authorities and technology companies, which frequently postpones access to essential digital evidence.

Social and cultural barriers are also an obstacle to effective response in Pakistan. There is underreporting as a result of stigma, fear of social rejection, and mistrust of law enforcement. The reasons why families do not report online sexual offences include not wanting their reputation damaged, and victims themselves might be hesitant to report abuse since they are ashamed or fear being blamed. The cultural background of Pakistan, accompanied by the lack of awareness about online risks, makes the number of cases reported lower than the number of cases of online exploitation (Mehmood, 2025).

The other barrier is the jurisdictional differences between provincial and federal powers. Although PECA empowers federal law enforcement to investigate cybercrimes, child protection is a provincial issue in Pakistan in its devolved form of governance. This departmentalization produces institutional fragmentation that makes coordinated responses difficult. In many provinces such as Punjab, Sindh, and Khyber Pakhtunkhwa, child protection units do not have an information sharing

mechanism with federal cybercrime investigators to help them intervene in cases of online and offline exploitation.

Irrespective of these issues, there are immense opportunities. Being a member of regional agencies such as SAARC, and the desire of Pakistan to align its cyber laws with international standards may boost cooperation with agencies such as INTERPOL and the WeProtect Global Alliance. Enhancing relationships with international technology would also enhance access to digital evidence and allow quicker elimination of CSAM.

Another important opportunity is investing in capacity building. Prosecutions would be improved by training investigators, prosecutors, and judges on digital forensics and cross border evidence handling. At the same time, digital literacy campaigns in schools, in partnership with UNICEF and civil society, is essential in mitigating children vulnerability (Livingstone and Third, 2017).

All in all, although Pakistan has created a legal framework to combat online child exploitation, further institutional capacity and increased international collaboration is necessary. The key to improving its digital boundary and securing the most vulnerable citizens is modernization of laws, investment in training, and enhancing global cooperation.

Recommendations for Strengthening Digital Borders

The digital border can be strengthened through the multi-layered approach that involves legislative reform, capacity building, technological innovation, and international cooperation. This framework assists states including Pakistan to improve their ability to prevent, investigate and respond to cross-border online child exploitation.

1. **Legislative Harmonisation and Legal Reform:** A the initial step is to harmonise national laws with that of the international law. It is necessary to define specific legal and legal categories of online grooming, CSAM and live-streamed exploitation in countries. Pakistan ought to revise PECA to criminalize AI-generated abusive contents and exploitation on encrypted

networks. The harmonization of domestic laws with such models as the Budapest Convention enhance the legal clarity and the cross-border collaboration.

2. **Enhancing Cross-Border Investigative Capacity:** Proper response needs sturdy interstate mechanisms. States are encouraged to focus on increasing the number of countries that participate in the ICSE database of INTERPOL as well as regional information-sharing networks. Special 24/7 national cybercrime unit-to-unit interfaces will be crucial to overcome slow MLATs. The institutional capacity building needs to invest in the development of modern digital forensic laboratories, training in specific child protection units, and training in dark web monitoring.

3. **Regulating Technology Platform Accountability:** A "The legal requirement of "Safety by Design" must necessitate the incorporation of content detection devices, age-checking systems, and convenient reporting processes into the platforms. Governments should institutionalize collaboration with industry by having frameworks that set out compulsory reporting of identified CSAM, so that such data can be shared in time with the law enforcers. There should be independent audits of the safety of platforms.

4. **Proactive Prevention through Education and Awareness:** The improvement of digital literacy is one of the essential preventive pillars. The online safety curriculum should be a structured online program that has become part of the national standards, which include skills to be taught on how to identify grooming tactics. Parents receive awareness on parallel awareness campaigns on online risks. Community outreach through the local NGOs that the people trust is essential to fight stigma and report.

5. **Implementing Survivor- Centred Support Systems:** A investigation is not the end of the journey of a victim. This is in the form of setting up multi-disciplinary teams that offer crisis intervention, trauma-informed mental health care, and legal advocacy. The facilities of interviews that are kid friendly and

special training of judicial personnel are essential to avoid re- victimization in the course of court proceedings.

6. **Fostering Proactive Adaptation to Emerging Technologies:** States also need to pursue active forms of regulation of frontier threats such as the metaverse and deep fakes. Threat assessment can be done in the form of establishing national advisory committees that involve technologists and child rights advocates. Imposing the next-generation detection tools also guarantees that the protection measures are up to date with the threats.

Conclusion

The emergence of digital technologies has opened up a borderless world of child exploitation that defies the historic legal and institutional organizational paradigms. In this paper, global connectivity and anonymity have enabled online grooming, sextortion, and live-streamed abuse. Certainly, these are the crimes perpetrated under the influence of criminals, who take advantage of the fact that the digital world has no borders, and requires the response equally international, coordinated, and comprehensive.

The international organisations have played a crucial role in developing this response. The databases of INTERPOL and child-toned advocacy of UNICEF, the structures of the WeProtect Global Alliance, emphasize the idea that isolation is not the way to go. Close international collaboration, co-ordinated legislations, and fast information exchange are invaluable. Nevertheless, such international initiatives should be accompanied by strong domestic response. States should invest in specialist investigative capacity, digital literacy initiatives, and survivor-centred care, and national law needs to keep up with new technologies.

The case of Pakistan is similar to many developing countries showing that a legal framework is essential, but it cannot be effective without proper implementation, institutional capability, and popular confidence. Finally, the development of a competent digital border is a shared ethical obligation. It takes commitment over a long period by governments, international organisations, technology firms and

societies. It is a coordinated action, constant innovation, and uncompromising child-centred approach that will result in making the digital world safer to all children.

BIBLOGRAPHY

1. 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

2. 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

3. 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.

4. 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

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

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

7. 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

8. 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

9. 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

10. 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

11. 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.

12. 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

13. 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

14. 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

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

16. 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

17. 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

18. 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

19. 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/

20. 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.

21. 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

22. 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

23. 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

24. 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

25. 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

26. 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

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

28. 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

29. 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

30. 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

31. 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

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

33. 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

34. 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/

35. 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

36. 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