*Page 1841 - 1858* ***DOI:*** *https://doij.org/10.10000/IJLMH.1110039*

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

## [ISSN 2581-5369]

**Volume 8 | Issue 3**

**2025**

# Global Dimensions of Juvenile Cybercrimes: Balancing Rehabilitation, International Legal Harmonization, and Cybersecurity Education for a Safer Digital Future

SALONI BAHL[1] AND DR. MEENAKSHI PUNIA[2]

## ABSTRACT

*The rapid digitalization of society has created both opportunities and vulnerabilities for children and adolescents, who are increasingly becoming active participants in the digital world. While often perceived as victims of online threats, minors are now also emerging as perpetrators of cybercrimes, including hacking, cyberbullying, identity theft, and ransomware attacks. This research examines the global rise in juvenile cybercrimes, driven by technological accessibility, anonymity, and inadequate digital literacy, especially in underdeveloped regions. Drawing upon international case studies and data from INTERPOL, ENISA, and UNODC, the paper highlights a 37–45% rise in youth cyber offenses over the past decade. Through a comparative legal analysis of India, the European Union, and Commonwealth nations, the paper explores how juvenile justice systems reconcile enforcement with rehabilitation. Cyber Framework, in fostering transnational collaboration. A central focus of the research is on child-centric cybersecurity education as a preventive tool. Programs like India's Cyber Swachhta Kendra, the EU's Better Internet for Kids, and Singapore's Digital Defence campaign are evaluated for their effectiveness. Barriers to implementation—such as the digital divide, curriculum gaps, and lack of trained educators—are also critically examined. The study concludes with policy recommendations emphasizing the integration of cybersecurity education, international legal harmonization, and rehabilitation-focused juvenile justice models. Addressing juvenile cybercrime requires a multi-pronged, globally coordinated approach that protects children while empowering them to be responsible digital citizens.*

***Keywords:*** *Juvenile Cybercrime, Digital Literacy, Rehabilitation, International Legal Frameworks, Cybersecurity Education*

[1] Author is a Research Scholar of Law at Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India.

[2] Author is an Assistant Professor at Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India.

## I. Introduction

The global surge in child-related cybercrimes is an alarming trend fueled by increasing technological access and rapid digitalization. Adolescents often called "digital natives" are not only becoming victims of online exploitation but are also engaging in cybercrimes, sometimes knowingly and at other times due to a lack of awareness. Over the past decade, there has been a marked rise in minors' involvement in cyber offenses such as hacking, identity theft, cyberbullying, and even more serious acts like ransomware attacks. INTERPOL's 2023 report revealed a 37 percent increase in youth cybercrimes over the last five years, with the highest growth observed in underdeveloped countries where digital literacy programs have lagged behind technological progress. This growing issue has prompted both governments and international bodies to address its root causes and mitigate the risks associated with juvenile involvement in cybercrime.

A primary factor driving this tendency is the socio-psychological allure of cybercrimes. Adolescents frequently view digital environments as anonymous realms where acts are devoid of accountability[3]. A multitude are driven by curiosity, the excitement of avoidance, or monetary rewards. In several instances, cybercrimes manifest as a means of retribution, social coercion, or psychological turmoil. Prominent international cases underscore this fact. The 2022 incident involving the "*Lapsus$*" hacking organization demonstrated that a 16-year-old in the UK orchestrated significant attacks on major technology firms such as Microsoft and Nvidia, highlighting the capacity of minors to exploit digital weaknesses for monetary advantage. A 2023 study by the *ENISA* revealed that an increasing proportion of adolescents participate in "*low-level*" hacking operations, including DDoS assaults, frequently without a complete understanding of the legal consequences.

Addressing cybercrimes committed by children poses distinct legal issues. In reference to some of the major international treaties such as the *Budapest Convention on Cybercrime* and the UNCRC, it underscores the significance of rehabilitating juvenile offenders instead of employing punitive approaches. Nonetheless, enforcement remains variable between jurisdictions.[4] The *GDPR* in the European Union imposes stringent regulations on children's online activity; yet, there is a deficiency in global standardization of these regulations. The IT Act of 2000 in India, revised in 2008, contains provisions for penalizing cybercrimes; however, the enforcement concerning adolescents is governed by the JJ Act 2015, which

[3] Ms Geeta Singh Chetry & Uzzal Sharma, *Emerging Technologies as a Tool for Cybercrime Against Women and Children*, (2024), https://papers.ssrn.com/abstract=4765788 (last visited Dec 12, 2024).

[4] *Id.*

emphasizes reformative justice over punitive measures. There have been comparable systems are present in nations such as the United States, where the *CFAA* is augmented by state legislation to tackle juvenile offenders.

In order to address the worldwide aspects of juvenile cybercrimes, international cooperation is essential. Entities such as INTERPOL, Europol, and the Commonwealth Cybercrime Initiative have established systems for instantaneous information exchange, transnational investigations, and capability enhancement. The GFCE has played a crucial role in enhancing information exchange and executing preventive strategies worldwide. Furthermore, bilateral agreements like the *India-U.S. Cyber Framework Agreement* underscore the increasing significance of cooperation in addressing cyber dangers related to children.

### A. Emerging Trends in Juvenile Cybercrimes Across the Globe

As technology has advanced and youth's use of the internet has increased, juvenile cybercrimes have grown in complexity and scope, making them a serious worldwide concern. Adolescents and youngsters, hitherto viewed only as vulnerable consumers in the digital landscape, are suddenly emerging as offenders of cyber-crimes[5]. This transition indicates the increasing sophistication of digital tools and the accessibility of technology, which has diminished the barriers to entry for illicit online activity. A 2023 report by the UNODC indicates that teenage cybercrimes have increased by around 45 percent worldwide over the last decade. This concerning trend has elicited significant apprehension among policymakers, educators, and law enforcement on the enduring consequences of unregulated youth participation in cybercrimes.

A notable trend in juvenile cybercrime is the rising incidence of hacking and data breaches perpetrated by children. Adolescents frequently exploit vulnerabilities in websites, networks, and applications for many goals, including financial profit and social acclaim[6]. The 2022 incident with the "*Lapsus$*" hacking group exemplifies a 16-year-old from the United Kingdom orchestrating a cybercriminal organization that targeted global firms such as Microsoft, Samsung, and Nvidia. This case highlighted how adolescents, equipped with fundamental programming skills and access to sophisticated hacking tools, can execute extensive cyberattacks resulting in considerable financial and reputational harm. The participation of minors in ransomware attacks has increased. A research by Kaspersky

[5] Cecelia Horan & Hossein Saiedian, *Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions*, 1 Journal of Cybersecurity and Privacy 580 (2021).

[6] Steven Furnell & Samantha Dowling, *Cyber Crime: A Portrait of the Landscape*, 5 Journal of Criminological Research, Policy and Practice 13 (2019).

indicates that more than 25 percent of worldwide traceable ransomware incidents involved juveniles, underscoring a concerning trend of kids being enlisted into organized criminal syndicates.

Addressing juvenile cybercrimes poses special legal problems that call for striking a balance between enforcement and rehabilitation. International legal frameworks are informed by agreements like the *Budapest Convention on Cybercrime*, which aims to standardize legislation across jurisdictions and promote international collaboration in addressing cyber offenses. The UNCRC underscores the necessity of rehabilitative strategies for juvenile offenders, asserting that punitive actions should be utilized just as a last choice. Nonetheless, enforcement procedures differ significantly among countries. The JJ Act, 2015, in India emphasizes reformative methods, safeguarding juveniles from the severe penal repercussions imposed on adult criminals. Conversely, the United States has a more rigorous framework under its CFAA, permitting the prosecution of children based on the gravity of the offense, while some states have diversion programs focused on rehabilitation[7].

In order to combat the growing number of adolescent cybercrimes, international conventions and accords have promoted international collaboration and capacity-building programs[8]. The Global Cybercrime Treaty, established as a consensual framework in 2023, underscores the necessity for countries to provide standardized legal definitions for cyber crimes and to adopt measures to deter the recruitment of minors into cybercriminal activities. Likewise, programs such as the INTERPOL Cybercrime Directorate and the Commonwealth Cybercrime Initiative emphasize information exchange, transnational investigations, and the formulation of child-centric treatments to tackle the underlying causes of these offenses. Notwithstanding these endeavours, enforcement is inconsistent, as numerous countries lack the requisite resources and ability to counter the advanced methods utilized by youthful cybercriminals[9].

In the battle against juvenile cybercrimes, education and awareness campaigns have become essential elements. Governments and international organizations acknowledge the significance of digital literacy initiatives designed to provide children and adolescents with the skills to navigate the online environment safely. The European Commission's Better Internet for Kids program and India's Cyber Swachhta Kendra initiative prioritize safe online practices and the ethical utilization of technology. Nonetheless, obstacles remain in the efficient implementation of these initiatives, especially in under-resourced areas where access to

[7] Kavita Rani, *Cybercrime and Legal Responses in the Indian Jurisdiction*, 1 Indian Journal of Law 35 (2023).

[8] Huong Thi Ngoc Ho & Hai Thanh Luong, *Research Trends in Cybercrime Victimization during 2010–2020: A Bibliometric Analysis*, 2 SN Soc Sci 4 (2022)

[9] *Id.*

education and technology is constrained. Furthermore, the rapid advancement of technology frequently surpasses the ability of educational systems to mitigate developing threats, resulting in awareness deficiencies that cybercriminals might exploit[10].

The rising trends in juvenile cybercrimes also pose considerable ethical and moral dilemmas. The extensive utilization of artificial intelligence and machine learning technologies has facilitated minors in acquiring sophisticated hacking skills with little difficulty[11]. The increasing accessibility of encrypted communication platforms exacerbates the challenges in monitoring and preventing cybercrimes affecting minors. Conversely, these technologies possess the potential for prevention and intervention[12]. AI-driven monitoring systems and blockchain-based identity verification technologies can significantly mitigate the danger of juvenile cybercrimes while safeguarding the privacy and rights of minors.

The difficulties in combating teenage cybercrimes are brought to light by case laws from different jurisdictions. The case of *United States v. Drew*[13] established a precedent in the United States for the prosecution of adolescents engaged in cyberbullying under the CFAA. The *Aarushi Talwar*[14] murder case in India, highlighted concerns around cyber evidence and the use of internet platforms by juveniles, leading to demands for more stringent legislation. Simultaneously, the 2023 incident involving a 15-year-old in Australia who devised a phishing scheme aimed at a government institution highlighted the necessity for international cooperation to combat transnational cybercrimes[15].

### B. Comparative Analysis between India, Europe and other Commonwealth Nations

As technology and internet access proliferate worldwide, children and teenagers are increasingly confronted with the opportunities and hazards of the digital realm. This exposure has resulted in a concerning increase in juvenile cybercrimes, requiring strong legislative frameworks, preventive strategies, and international collaboration to properly tackle the problem.

The increase of adolescent cybercrimes in India is characterized by occurrences such as

[10] Yuanrong Hu, Xi Chen & Indranil Bose, *Cybercrime Enforcement Around the Globe*, 9 Journal of Information Privacy and Security 34 (2013).

[11] Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-crime*, 29 Policing: An International Journal of Police Strategies & Management 408 (2006).

[12] *Id.*

[13] United States v. Drew 259 F.R.D. 449 (C.D. Cal. 2009)

[14] Dr. Rajesh Talwar and Another v. Central Bureau Of Investigation 2013 (82) ACC 303

[15] Joana Neto, *Social Network Analysis and Organised Crime Investigation: Adequacy to Networks, Organised Cybercrime, Portuguese Framework, in* Cybercrime, Organized Crime, and Societal Responses: International Approaches 179 (Emilio C. Viano ed., 2017), https://doi.org/10.1007/978-3-319-44501-4_8 (last visited Dec 12, 2024).

hacking, identity theft, cyberbullying, and financial fraud. The IT Act 2000, revised in 2008, constitutes the principal legislative framework for addressing cyber offenses, especially those pertaining to children[16]. However, in cases involving juvenile offenders, the JJ Act, 2015, prevails, prioritizing reformative over punitive measures. A significant incident from 2022 featured a 15-year-old in Jaipur who infiltrated a school's database to modify academic records. Despite the severity of the offense, the judicial reaction under the JJ Act 2015 emphasized counselling and rehabilitation, illustrating India's dedication to reconciling accountability with the developmental requirements of juveniles. Notwithstanding these initiatives, obstacles remain in law enforcement owing to insufficient digital literacy and limited infrastructure, especially in rural regions[17]. Initiatives such as Cyber Swachhta Kendra, introduced by the Ministry of Electronics and Information Technology, seek to enhance awareness and foster cyber resilience among young users; nevertheless, their impact is constrained.

In Europe, the strategy for addressing adolescent cybercrimes is based on a blend of strong legal frameworks and advanced rehabilitative programs. The Budapest Convention on Cybercrime, the inaugural international convention targeting internet and computer-related offenses, has played a crucial role in standardizing legislation among European countries. The GDPR has measures for the safeguarding of minors in digital environments, assuring responsible management of personal data. In nations such as Germany, adolescent cyber offenders are frequently addressed under the Youth Court Act, which emphasizes education and social reintegration rather than punitive measures. In 2023, a significant case featured a 16-year-old from Berlin who devised a phishing scheme aimed at small enterprises. The perpetrator received a sentence of community service and was required to participate in cybersecurity awareness programs, underscoring Europe's emphasis on rehabilitative measures. Moreover, entities such as the ENISA are essential in promoting cooperation among member states to address cybercrimes affecting minors. ENISA's 2022 report indicated that more than 30 percent of cyber incidents reported in Europe involved minors, leading to demands for enhanced educational and awareness initiatives aimed at young users[18].

The Commonwealth nations exhibit a varied approach to juvenile cybercrimes, indicative of the differing degrees of technology progress and legal frameworks among member states.

[16] Sanika Fegade, *Juvenile Justice System: A Medium for Welfare of Children*, 3 Indian J.L. & Legal Rsch. 1 (2021).

[17] Haripriya Rangan, Marcus B. Lane, *Indigenous Peoples and Forest Management: Comparative Analysis of Institutional Approaches in Australia and India*, 14 Society & Natural Resources 145 (2001).

[18] William K. Cummings, The Institutions of Education: A Comparative Study of Educational Development in the Six Core Nations (2003).

Developed nations like as Australia and Canada have established thorough legislative frameworks and proactive initiatives to address the issue. The Enhancing Online Safety Act of 2015 in Australia, overseen by the eSafety Commissioner, establishes measures to combat cyberbullying and other offenses perpetrated by juveniles. A 2023 incident in Sydney involved a 14-year-old use social engineering tactics to illicitly enter a school's financial system. The legal approach used restorative justice procedures, including victim-offender mediation, to establish accountability and mitigate recidivism. Canada's PIPEDA imposes rigorous regulations for safeguarding minors' data, alongside provincial legislation targeting cybercrimes.

Conversely, Commonwealth members in Africa and South Asia encounter distinct issues stemming from resource scarcity and irregular enforcement of cyber legislation. The CMCA 2018 in Kenya criminalizes certain cyber offenses; nevertheless, enforcement is hindered by insufficient technological skills and equipment[19]. In 2022, a 17-year-old from Nairobi was apprehended for planning a ransomware attack on a local financial institution. The case underscored the growing sophistication of adolescent cyber criminals in the region and revealed deficiencies in the legal system's capacity to address such instances effectively.[20] The Commonwealth Cybercrime Initiative aims to enhance capacity and promote knowledge exchange among member states, concentrating on the specific requirements of poor countries.

A shared characteristic among these jurisdictions is the focus on international collaboration to tackle the transnational aspect of cybercrimes. The Budapest Convention on Cybercrime has been fundamental in promoting cooperation, allowing nations to exchange information, undertake joint investigations, and extradite offenders when required. The INTERPOL Cybercrime Directorate has played a crucial role in coordinating initiatives to address adolescent cyber transgressions, especially in instances with cross-border implications. A 2021 operation conducted by INTERPOL revealed a network of minors from India, the UK, and Australia engaged in a global phishing scheme, highlighting the necessity for cohesive international collaboration.

In every jurisdiction, education and awareness are still vital parts of the battle against adolescent cybercrimes. Although Europe has led in the execution of extensive digital literacy initiatives, other regions are progressing rapidly. In India, programs such as the National Cybersecurity Awareness Month seek to inform young people regarding internet safety and

[19] Alfred Stepan, Juan J. Linz & Yogendra Yadav, Crafting State-Nations: India and Other Multinational Democracies (2011).

[20] *Id.*

the ethical utilization of technology. Likewise, Commonwealth countries such as South Africa have implemented school-based initiatives to educate pupils on the dangers linked to digital environments[21]. The efficacy of these programs significantly varies, frequently impeded by socioeconomic inequality and cultural variances.

The environment of juvenile cybercrimes has also been shaped by technological breakthroughs in two ways. On one hand, technologies such as artificial intelligence and blockchain have facilitated enhanced surveillance and deterrence of cybercrimes. AI-powered content moderation systems are progressively employed to identify and eliminate detrimental online actions involving kids. The rise of encrypted communication platforms and the dark web has afforded adolescents additional opportunities to engage in cybercrimes, hence complicating enforcement efforts[22]. The involvement of technology businesses in tackling these difficulties is essential. Corporations like as *Google* and *Meta* have implemented features like parental controls and age-appropriate material filters to safeguard minors; yet, their execution frequently prompts ethical and privacy dilemmas.

As technology advances, the techniques and motivations of adolescent cyber criminals will likewise progress. Policymakers, educators, and law enforcement agencies must stay alert and flexible, utilizing worldwide best practices to establish a more secure digital environment for everyone. Through the promotion of collaboration, the improvement of education, and the resolution of systemic issues, countries may alleviate the threats associated with juvenile cybercrimes and create a future in which technology functions as a beneficial force rather than an instrument of damage.

## II. International legal and strategic frameworks to combat juvenile cybercrime

The foundation of international legal frameworks for combating cybercrimes is the 2001 Budapest Convention on Cybercrime. Originally devised for Europe, its impact has proliferated worldwide, with nations such as the United States, Japan, and Australia actively adopting its stipulations. The Convention explicitly addresses crimes including unauthorized access, data interference, and child exploitation, highlighting the necessity of international cooperation in investigations. India, although not being a party, has harmonized certain domestic cyber legislation, particularly the IT Act 2000, with the objectives of the

[21] André Blais, Louis Massicotte & Antoine Yoshinaka, *Deciding Who Has the Right to Vote: A Comparative Analysis of Election Laws*, 20 Electoral Studies 41 (2001).

[22] Philipp Dann & Arun K. Thiruvengadam, *Comparing Constitutional Democracy in the European Union and India: An Introduction, in* Democratic Constitutionalism in India and the European Union 1 (2021).

Convention. The Second Additional Protocol, enacted in 2021, fortifies this pact by improving cross-border access to electronic evidence, tackling a critical obstacle in transnational cybercrime investigations concerning young offenders[23].

The international approach to cybercrimes affecting minors has also been significantly shaped by the UN. The General Assembly's 2021 Resolution on Countering the Utilization of ICTs for Criminal Purposes emphasizes the necessity of multilateral collaboration to successfully address cybercrimes[24]. This resolution is vital as cyber risks involving minors have surged, with INTERPOL's 2023 Global Crime Trends report revealing a 70 percent rise in juvenile cybercrimes over the last decade. These charges frequently encompass actions such as phishing, cyberbullying, and digital fraud, illustrating the concerning trend of adolescents being enticed into cybercrime due to access to advanced technology and insufficient awareness of legal repercussions.

One of the most important international frameworks for addressing children's rights and protection in the digital age is the CRC, which was adopted by the UN in 1989. According to Articles 16 and 34 of the CRC specifically protect minors from abuse, exploitation, and privacy infringement, including in the digital domain. The *Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography (2000)* enhances these rights by mandating states to prohibit and address these violations. The CRC has motivated other regional measures, including the Council of Europe's Lanzarote Convention, which tackles the online sexual exploitation of children and safeguards their rights inside court proceedings[25].

As critical components of international endeavours to combat juvenile cybercrimes, education and awareness programs have emerged. Initiatives such as the WePROTECT Global Alliance have united governments, technology firms, and civil society to combat online child exploitation. The 2022 worldwide Threat Assessment released by the alliance indicated a remarkable 60 percent rise in online abuse reports during the pandemic, underscoring the necessity for ongoing worldwide initiatives[26]. Initiatives that promote understanding of digital rights, cyber hygiene, and the legal ramifications of online behaviour have proven pivotal in decreasing youth participation in cybercrimes while equipping them to engage with the digital

[23] Dina I. Oddis, *Combating Child Pornography on the Internet: The Council of Europe's Convention on Cybercrime*, 16 Temp. Int'l & Comp. L.J. 477 (2002).

[24] *Id.*

[25] Ellen S. Podgor, *Cybercrime: National, Transnational, or International*, 50 Wayne L. Rev. 97 (2004).

[26] WeProtect, *Global Threat Assessment 2023*, https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf (last visited Dec 12, 2024).

realm responsibly[27].

With particular protections for children's privacy, the GDPR, which was implemented in 2018, establishes strict guidelines for the protection of personal data in the European Union. These restrictions safeguard minors from online exploitation and ensure organizations are accountable for the responsible processing of their data. According to some cases such as *Schrems II*[28], which addressed data transfer between the EU and the United States, highlight the significance of these policies in upholding international standards for data privacy and security.

The significance of international organizations such as INTERPOL in addressing cybercrimes affecting minors is undeniable[29]. INTERPOL has improved worldwide collaboration in detecting and combating cybercrimes through programs such as the *Global Cybercrime Strategy (2022–2025)*. The strategy prioritizes adolescent offenders and victims, highlighting capacity enhancement, intelligence dissemination, and cooperative investigations. This approach demonstrates the increasing acknowledgment that tackling juvenile cybercrimes necessitates a comprehensive strategy incorporating legal, social, and technological measures.

The struggle against cybercrime has underscored the importance of bilateral and multilateral agreements in promoting international collaboration. Agreements such as the US-India Cyber Framework, established in 2016, promote information exchange, collaborative investigations, and capacity enhancement, enabling nations to effectively tackle the transnational aspects of cybercrimes involving minors. The trilateral cybersecurity collaboration among Australia, the UK, and the US, established in 2021, aims to strengthen collaborative capacities to combat new cyber threats, particularly those involving juvenile offenders[30].

The conversation around digital rights is still influenced by international human rights treaties like the UDHR. The principles of the UDHR are embodied in the *UN Guiding Principles on Business and Human Rights (2011),* which mandate that technology companies are responsible for preventing the misuse of their platforms for criminal activities. In instances concerning minors, these principles underscore the obligation of enterprises to protect children's rights while facilitating access to secure digital environments.

Another significant step in international initiatives to encourage responsible behaviour in the

[27] *Id.*

[28] Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ECLI:EU:C:2015:650

[29] Lucia Pizzato, *Institutional Change in International Organisations: The Case of Interpol*, Institutional change in International Organisations: the case of Interpol (2019), http://dspace.unive.it/handle/10579/15307 (last visited Dec 12, 2024).

[30] *Id.*

digital sphere is the 2018 Paris Call for Trust and Security in Cyberspace in 2018. Endorsed by more than 80 nations, the appeal emphasizes the necessity of safeguarding at-risk groups, particularly children, from cyber-attacks[31]. It aims to establish a safer and more inclusive digital ecosystem through the promotion of multi-stakeholder collaboration.

## III. Global programs on cybersecurity education for children

### A. India's Approach to Raising Awareness and Promoting Digital Literacy

In the digital age, ensuring children's cybersecurity education has become a global imperative. Countries worldwide have initiated programs to equip young minds with the knowledge and skills necessary to navigate the online world safely.[32] In the United States, the CISA offers resources tailored for grades K-5, introducing basic cybersecurity concepts to help children develop skills to protect themselves from digital dangers.[33] Similarly, the "*Be Internet Awesome*" program empowers kids with tools and education to confidently and safely explore the internet. In the United Kingdom, initiatives like the Cyber Security Challenge UK have developed games such as Cyphinx to inspire interest in cybersecurity careers among young individuals. These programs aim to build a foundation of cyber awareness from an early age, fostering a generation of digitally literate and secure individuals.

India, recognizing the importance of digital literacy, has implemented several initiatives to raise awareness and promote cybersecurity education among children. The National Digital Literacy Mission (NDLM), adopted by the Government of India, aims to ensure that every household has at least one digitally literate person.[34] Programs like "The Kavach" focus on providing technology education to students from primary to senior secondary levels, offering courses in robotics, artificial intelligence, cybersecurity, and coding. These initiatives align with the New Education Policy (NEP) 2024, emphasizing hands-on learning and innovation.

There are efforts at the state level have also been significant. In Telangana, the Cyber Congress initiative trains public school students to identify scams and handle cyberbullying, with over 3,000 students graduating as cyber ambassadors in its first year.[35] Similarly, the Cyber Safe Program in Delhi NCR has raised awareness about cybersecurity threats, including

[31] Emmanouil Billis & Panagiotis Gkaniatsos, *Minors as Victims in the Age of Information and Communication Technologies*, (2019), https://papers.ssrn.com/abstract=2768590 (last visited Dec 12, 2024).

[32] "Empowering young minds to navigate the digital world," *India Today*, 2024 *available at*: https://www.indiatoday.in/education-today/featurephilia/story/empowering-students-raising-cybercrime-awareness-in-schools-2573209-2024-07-29 (last visited Mar. 27, 2025).

[33] "Cybersecurity Education Resources for Grades K-5 | CISA," *available at*: https://www.cisa.gov/resources-tools/programs/cybersecurity-education-career-development/resources-grades-k-5 (last visited Mar. 27, 2025).

[34] "Digital Literacy, Safety & Security Programme," *Digital Empowerment Foundation, DEF available at*: https://www.defindia.org/digital-literacy-safety-security-programme/ (last visited Mar. 27, 2025).

[35] Varsha Bansal, "In the Fight Against Scams, 'Cyber Ambassadors' Enter the Chat" *Wired.*

cyberbullying, by imparting over 6,000 hours of training to students, parents, and teachers.[36] These localized efforts demonstrate the importance of community-based approaches to cybersecurity education. Further, there NGOs who have also played a crucial role in promoting online safety for children in India. The organizations like CRY India are committed to raising awareness about the importance of online safety, helping children focus on their education without digital distractions or risks. The Smile Foundation implements regular cybersecurity awareness and online safety workshops for students, empowering them with essential online safety knowledge and equipping them to navigate the digital world with confidence.

Despite these efforts, challenges remain. The NCRB found that child cybercrime in India has risen by 32 percent in just one year, highlighting the need for increased awareness and education.[37] To address this, projects have been initiated to raise awareness about the safe use of smart devices and the internet for children aged 8-16, focusing on cyber threats, privacy measures, safe mobile usage, and ethical hacking. These initiatives aim to create a culture of safe online practices among the youth.

Internationally, partnerships between governments, educational institutions, and private organizations have been instrumental in promoting cybersecurity education. Fortinet's Education Outreach Program works with global partners to drive change on pressing cybersecurity issues, providing training and certification opportunities to help close the cybersecurity skills gap.[38] Such collaborations are essential in creating a comprehensive approach to cybersecurity education for children. There are global programs on cybersecurity education for children, including India's multifaceted approach, highlight the collective effort required to safeguard the digital future of the younger generation. Through government initiatives, community-based programs, and international collaborations, strides are being made to equip children with the necessary tools to navigate the online world safely and responsibly. Continued investment in and expansion of these programs are vital to address the evolving challenges of the digital age.

### B. Barriers to Effective Implementation of Cyber Education

In the rapidly evolving digital era, cybersecurity education has emerged as a crucial

[36] *Id.* at 59.

[37] A. Davis, "Strengthening Cyber Safety Skills for Children in India," *available at*: https://www.gendigital.com/blog/impact/community/save-the-children-2024 (last visited Mar. 27, 2025).

[38] FTI, "Education Outreach Program," *Fortinet available at*: https://www.fortinet.com/training/education-outreach-program?utm_source=website&utm_medium=pr&utm_campaign=outreach (last visited Mar. 27, 2025).

component of digital literacy, particularly for children who are increasingly active online. According to UNICEF, over 71 percent of youth worldwide are online, with children often encountering the internet at younger ages than ever before. While several nations have initiated cybersecurity awareness programs targeted at minors, implementation gaps remain due to structural, policy-related, infrastructural, and sociocultural challenges.

### a) Global Landscape of Cybersecurity Education for Children

The global landscape of cybersecurity education for children is evolving, yet remains uneven across regions and socioeconomic contexts. According to a 2023 UNESCO report, only 37 percent of countries have formally incorporated digital citizenship or cybersecurity components into their national school curricula. High-income nations such as Finland, Singapore, and South Korea lead the way, integrating structured cyber literacy from primary school onward through public-private initiatives and government mandates. In contrast, many low- and middle-income countries lack national strategies, often relying on ad hoc programs led by NGOs or international bodies like UNICEF. The European Union's Digital Education Action Plan 2021–2027 and the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) K-12 initiative are notable examples of policy-driven approaches. Meanwhile, the African Union's "Digital Transformation Strategy for Africa (2020–2030)" acknowledges cybersecurity education as a critical future priority, though implementation remains in early stages. Despite growing awareness of the need for cyber resilience among children—particularly in the context of increasing online risks like phishing, cyberbullying, and child exploitation—the lack of universal standards, funding disparities, and varying policy commitments result in an inconsistent global approach to cybersecurity education for the next generation.

- Through initiatives like *Better Internet for Kids (BIK)* and *Insafe Network*, the EU emphasizes safe digital behaviour among children across member states. These platforms offer age-appropriate content and cyber-awareness materials in multiple languages.
- The *Cybersecurity & Infrastructure Security Agency (CISA)* supports K-12 cybersecurity through the *CEA* program. The NICE, coordinated by NIST, has developed a framework aligning cybersecurity curricula across school levels.[39]
- Under the *National Cyber Security Policy 2013* and the *Digital India* initiative, efforts such as *Cyber Shikshaa* (NASSCOM and DSCI) and state-level digital literacy campaigns

[39] "NICE Workforce Framework for Cybersecurity (NICE Framework)", NICCS, 2025.

have attempted to engage students, but penetration remains low due to linguistic and infrastructural barriers.

- The *eSafety Commissioner* runs digital safety campaigns and online safety modules integrated into school curricula. Programs such as "The Lost Summer" use gamification to teach cyber ethics and online safety.
- Through its *Basic Act on Cybersecurity*, Japan encourages cyber hygiene from a young age, integrating it into elementary and secondary school curricula with support from government-approved e-learning platforms.

### b) Barriers to Effective Implementation

Despite increasing recognition of the importance of cybersecurity education for children, multiple barriers hinder its effective implementation globally. A significant challenge is the digital divide—millions of children, especially in low-income and rural areas, lack access to digital devices or internet connectivity, as highlighted by the 2023 ITU report. The curriculum gaps persist, with only 22 percent of countries integrating formal cybersecurity education in primary or secondary school syllabi (OECD, 2022), and a shortage of trained educators further compounds the issue. The legal and policy frameworks such as COPPA (U.S.) and GDPR-K (EU) mandate children’s data protection but lack provisions for compulsory cyber education in schools. Additionally, cultural taboos around online risks like cyberbullying and grooming, limited parental awareness, language barriers, and underfunded infrastructure present serious obstacles to large-scale, inclusive cyber education programs.

- As per the *ITU 2023 Global Connectivity Report*, nearly 2.6 billion people remain offline, with a significant proportion being children in low-income or rural areas. Lack of internet access and digital infrastructure hampers the reach of cyber education.
- In India, only 42 percent of urban children and a mere 18 percent of rural children had access to digital devices for learning during the pandemic.[40]
- Globally, only 22 percent of countries have included formal cyber hygiene or data privacy topics in their national K-12 curricula.[41]
- Many schools lack age-appropriate cybersecurity learning materials. The absence of a unified curriculum makes it difficult to track outcomes or assess student preparedness.

[40] ASER, "Annual Status of Education Report (Rural) 2021".

[41] T. Burns and F. Gottschalk, "Educating 21st Century Children Emotional Well-Being In The Digital Age" OECD (2022).

- According to a 2021 ISC² report, there's a global shortage of 3.4 million cybersecurity professionals.[42] Consequently, few trained personnel are available to educate children on cybersecurity principles.
- A survey conducted by *Microsoft's Global Online Safety Survey (2023)* revealed that only 35 percent of parents actively monitor or guide their children's online behaviour, reflecting a gap in parental digital literacy.[43]
- In some cultures, discussions around online threats such as grooming, cyberbullying, or sextortion are considered taboo, further limiting open dialogue.
- While laws like COPPA in the U.S., GDPR-K in the EU (Articles 8 & 12), and India's recently passed DPDP Act, 2023 include clauses for children's data protection, enforcement remains inconsistent.
- Many countries lack dedicated legislation mandating cybersecurity education in school curricula, reducing accountability and priority at the policy level.
- Most cybersecurity education resources are in English. For regions with multilingual populations like Africa or South Asia, this creates significant accessibility barriers. For example, the lack of cybersecurity content in regional languages in India limits reach in Tier II and III cities.

### c) Global Best Practices in Child-Centric Cybersecurity Education

There are several countries provide exemplary models for effective cybersecurity education among children. Estonia's ProgeTiger initiative stands out by embedding digital and cyber skills in early education, reaching over 90 percent of schools with state-supported teacher training.[44] In the UK, the CyberFirst program by the NCSC uses gamified learning, competitions, and scholarships to engage students, especially girls and underrepresented groups, in cybersecurity awareness and careers. According to Singapore's Digital Defence campaign leverages interactive content and simulations to make cyber education engaging and relatable, with over 85 percent of students participating nationwide.[45] These programs succeed due to comprehensive curriculum integration, public-private collaboration, localized content,

[42] "ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap,"*available at*: https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap (last visited Mar. 27, 2025).

[43] C. Gregoire, "New Microsoft research illustrates the online risks and value of safety tools to keep kids safer in the digital environment" *Microsoft On the Issues*, 2023 *available at*: https://blogs.microsoft.com/on-the-issues/2023/02/06/safer-internet-day-global-online-safety-survey-2023/ (last visited Mar. 27, 2025)

[44] E. Toome, "ProgeTiger: How to create interest in technology?" *Education Estonia,* 2021*available at*: https://www.educationestonia.org/progetiger/ (last visited Mar. 27, 2025).

[45] Ibid.

and robust policy backing offering replicable models for other nations seeking to scale cyber literacy for the younger population.

- A global leader in digital governance, Estonia has introduced *ProgeTiger*, an initiative that integrates coding, cybersecurity, and digital ethics into early education. Over 90 percent of schools participate, and teacher training is government-subsidized.[46]
- This includes competitions, scholarships, and classroom resources. It has shown measurable improvements in interest in STEM and cybersecurity careers among girls and underserved communities.
- The *Digital Defence* campaign educates children and families on recognizing cyber threats, with interactive videos and simulation tools used across schools. By 2023, over 85 percent of Singaporean school children had participated in a cybersecurity awareness session.[47]

### d) Recommendations for Overcoming Barriers

To overcome the barriers to effective implementation of cybersecurity education for children, a multi-stakeholder, policy-integrated, and resource-sensitive approach is essential. Governments must prioritize cybersecurity education by embedding it into national curricula through comprehensive digital literacy frameworks, supported by adequate teacher training and infrastructure investment. The PPP should be fostered to leverage expertise, funding, and scalable digital tools, especially in low- and middle-income countries. Further, the Global bodies like UNESCO, UNICEF, and ITU can play a pivotal role by setting universal minimum standards and providing modular, multilingual content that can be locally adapted. Additionally, awareness campaigns targeting parents and guardians must be intensified to create safe digital environments beyond the classroom.

- Governments should introduce compulsory cybersecurity education modules tailored for age groups, integrated with ICT and civic studies.
- Subsidized certifications and workshops in basic cyber hygiene and online safety should be made mandatory for schoolteachers.

[46] *Id.* at 71.

[47] "SG Cyber Safe Students Programme," *Cyber Security Agency of Singaporeavailable at*: https://www.csa.gov.sg/our-programmes/cybersecurity-outreach/sg-cyber-safe-students/ (last visited Mar. 27, 2025).

- Collaboration between governments, NGOs (e.g., *Childnet International*), private companies (e.g., *Google's Be Internet Awesome*), and community-based groups is essential to localize content and increase reach.
- Child-specific cybersecurity laws should include clear educational mandates, enforcement mechanisms, and funding allocations.
- Programs such as "*Interland*" by Google and "*Cyber Legends*" in Canada use storytelling and gamification to boost engagement and retention.
- Translate and culturally adapt cybersecurity materials into regional languages, and offer content for children with disabilities.

The global efforts to educate children about cybersecurity have gained considerable momentum in recent years, reflecting an increasing recognition of children's vulnerability to online threats such as cyberbullying, identity theft, online grooming, and misinformation. Initiatives led by international organizations like UNICEF, ITU, and the World Economic Forum, as well as national education departments, have resulted in the integration of digital literacy and cybersecurity modules in school curricula across several countries. However, the success of these efforts remains uneven and is largely contingent on addressing persistent gaps in access to digital tools, quality of pedagogy, technological infrastructure, and the lack of coherent policy frameworks. In low- and middle-income countries, for instance, only 35 percent of schools have reliable internet connectivity, and fewer than 20 percent of teachers report receiving adequate training in digital safety education.[48]

## IV. Conclusion

To overcome these challenges, there is a critical need for an inclusive, rights-based approach that respects children's privacy, agency, and right to education, while incorporating locally relevant content that resonates with the unique socio-cultural and technological landscape of each region.[49] This approach must also draw upon global best practices, such as the UK's "*Cyber Explorers*" program or Estonia's national digital literacy initiative, and be underpinned by robust legal and regulatory frameworks that mandate safe online environments and enforce accountability from digital platforms. Moreover, active collaboration between governments, educators, parents, civil society, and technology providers is essential to build a resilient digital ecosystem that supports learning and safety in equal measure. Since children are often

[48] A. Haleem et al., "Understanding the role of digital technologies in education: A review," 3 *SOC* 275–85 (2022).

[49] E. Keddell, "Recognising the embedded child in child protection: Children's participation, inequalities and cultural capital," 147 *CYSR* 106815 (2023).

among the earliest adopters of new technologies and digital platforms, equipping them with critical thinking skills, cyber hygiene awareness, and knowledge of their digital rights from an early age is not merely beneficial—it is vital for fostering a secure, inclusive, and future-ready digital society for all.

*****