IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER SAFETY FOR CHILDREN: VISION VIKSIT BHARAT AND THE SDGs

Sanchayeeta Rajkhowa

PHD Scholar

Department of Political Science

Gauhati University, Assam, India

Abstract: The vast internet provides an open vista for children's education in the digital age but assumes awful, remarkable risks, including physical and psychological kid abuse, cyberbullying, data misuse, and online exploitation. For the holistic development of the child, protecting children's rights in the virtual sphere is crucial. In this context of "Child Rights and Cyber Safety," this paper aims at making recommendations for the protection of children's rights within the online realm to promote their holistic development. Such discussions would resonate with the advocacy for the Vision for a Developed India, which envisions an inclusive and developed India by 2047 with a Sustainable Development Goals (SDGs) cohort. This paper portrays itself as advocating for a secure and inclusive digital environment as a critical protective mechanism for the child's development that aligns itself with "SDG 4 (Quality Education), SDG 5 (Gender Equality), SDG 10 (Reduce Inequalities), and SDG 16 (Peace, Justice, and Strong Institutions)." The important areas explored include policy and legal frameworks for online child safety, digital literacy and cyber awareness initiatives, roles of families, schools, and communities in ensuring cyber protection, and technology-enabled advance safeguarding. Thus, the paper posits that the importance of the safe digital ecosystem whereby every other child can thrive safely is paramount for its development into a resilient digitally empowered society.

Keywords: Child Rights, cyber safety, digital literacy, Vision Viksit Bharat, Sustainable Development Goals (SDGs)

I. INTRODUCTION

Protection of children and their holistic development is ensured in a safe digital atmosphere. Cyber safety is analysed from broader perspectives by integrating a right-based approach within Vision Viksit Bharat 2047, which aims to build a technologically sound and secure environment in India (NITI Aayog, 2022). Education, entertainment, and everything else are increasingly becoming dependent on the internet. Hence, safety and awareness against online exploitation should be encouraged. Digital Platforms create both opportunities and challenges like cyberbullying, online exploitation, and invasion of privacy, which operate as impediments to children's safety and security (Livingstone & Third, 2017). Therefore, the utmost need is to protect children from cyber exploitation. This article makes an attempt to weave Sustainable Development Goals (SDGs), which encompass "SDG4 (Quality Education), SDG5 (Gender Equality), SDG10 (Reduced Inequalities), and SDG16 (Peace, Justice, and Strong Institutions)"-into the roadmap of ensuring a safe digital environment for holistic development.

Dependence on digital platforms increased after the COVID 19 pandemic resulting in more online exploitations and cybercrimes (UNSDG 2020). Digital platform enhances learning opportunities, but it creates challenges and vulnerabilities. So, there is need for robust policy frameworks, awareness programs, and technological interventions to ensure safe and secure digital environment (UNICEF, 2021). According to OECD, there are four main risk categories for children in the digital environment: content, contact, consumer and conduct risks (OECD 2020). Advanced technology, privacy, and health and well-being risks are also identified as cross-cutting risks (OECD, 2020). The first focus of any online safety strategy must be to protect the educational and health benefits of digital technologies, since the risks that have to be addressed include exposure to violence, exploitation, and abuse, as well as privacy attitudinal breaches (UNICEF).

"The UN Convention on the Rights of the Child (UNCRC) is a constitutionally binding treaty ratified by 196 states, including India, which speaks of the acceptance of fundamental rights conferred upon each child, irrespective of their race, religion or disability" (United Nations, 1989). Article 17 explains how UNCRC should aim at the development of adequate guidelines for the protection of the child from such information or materials that are injurious to his or her well-being. Whereas Article 19 emphasises the need for all appropriate legislative, administrative, social, and educational measures to protect the child from any kind of injury, neglect or negligent treatment, maltreatment, physical or mental violence, abuse or exploitation (OHCHR, 1989). Parents and care takers should keep track of their child's online activities (United Nations, 1989). The Indian policy framework concerning online exploitation and cyber offences consists of laws such as the Information Technology (IT) Act, 2000; and Protection of Children from Sexual Offences (POCSO) Act.

Digital literacy initiatives complement parental control through the establishment of screening parameters on critical use of technology, responsible use, and comprehending potential threats that may be involved (Oshodi et al., 2024). However, parents, guardians and family members play an important role in securing a sound digital environment for their children. "The recent AI technologies emerge as a

protective instrument, monitoring and analysing online content by filtering harmful content, detecting predatory behaviour, and providing educational resources" (Sahota, 2024). As India is marching towards the bigger goal of "Viksit Bharat" and a global technology powerhouse, it visualises a future where the Internet is inclusive, accessible, and secure for its citizens (Chaturvedi 2025). Digital India has been witnessing dramatic growth with several initiatives like UPI, JAM trinity, Aadhar and so on giving a lot of impetus towards online safety and security (Chaturvedi 2025).

This study aims to investigate a human-rights-oriented approach to cyber safety for the child. It contextualises Cyber safety policies concerning the Vision Viksit Bharat and the SDG goals, particularly "SDG 4 (Quality Education), SDG 5 (Gender Equality), SDG 10 (Reduced Inequalities), and SDG 16 (Peace, Justice, and Strong Institutions)."

II. METHODS

Analysing cyber safety for children is done using a qualitative approach through document analysis and thematic analysis. The policy documents, legal frameworks, and scholarly literature were examined to assess the existing protective measures and gaps in the situation of online safety for children. Data from these documents were analysed using a thematic analysis to reveal patterns and salient themes that bring attention to key concerns and possible routes to mitigate them. In this qualitative way, a comprehensive understanding of children's cyber safety (Murray et al., 2024) in the context of Vision Viksit Bharat and the SDGs is generated.

III. THEORETICAL FRAMEWORK

This research is based on the "Child Rights-Based Approach" (CRBA), which stipulates that all policies that are formulated and implemented should have children's rights at its core (Murray et al., 2024). The CRBA finds alignments with "the United Nations Convention on Rights of the Child (UNCRC)" which proclaims that children must be protected from all forms of exploitation including threats from the cyberspace (UNICEF, 2020).

This study is founded on the "Digital Literacy Framework," which stresses the need for digital literacy to create awareness among children about the online exploitations. According to Livingstone and Helsper (2007), minimising the online risks and developing resilience against cyber threats can be promoted by digital literacy as well (Livingstone and Helsper, 2007). On the other hand, the "Digital Competence Framework" of the European Commission (DigComp) established that well-structured digital programs can actually happen.

Building critical thinking among children can help them to identify and counteract online risks (Ferrari, 2013). It will be an additional foundational pillar of the study based on Bronfenbrenner's "Ecological Systems Theory" (1979). This theory holds that every child's experiences in the digital world are shaped by multiple environmental factors-family, school, community, and policymakers.

As per the Social Learning Theory of Bandura (1977), children imitate online behaviour by observing and interacting from their surroundings (Bandura, 1977). It shows that children, where they are exposed to negative influences online, like cyberbullies, may even repeat the behaviour or become the subject of such actions (Patchin & Hinduja, 2010). Such raises the need for the promotion of positive digital citizenship through the educational interventions. Also, a significant framework for analysis into the way through which children view online risks and deal with cyber threats is "Protection Motivation Theory" (PMT) (Rogers, 1975). It is from PMT that one gets to discover the influence of threat appraisal and coping mechanisms on the development of digital resilience among children.

It is thus an argument of the study by putting these theoretical perspectives together, a multi-faceted, rights-based approach would be necessary for ensuring children cyber-safety. Policies should incorporate principles from CRBA, educational institutions should strengthen digital literacy initiatives based on the Digital Literacy Framework and regulatory bodies need to develop insight from ecological and behavioural theories to implement comprehensive cyber safety measures.

IV. IMPORTANCE OF CYBER SAFETY FOR CHILDREN

The fast digitalisation has affected the day-to-day life of children. Using access of internet for educational or other reasons has both positive and negative impacts on children. Cyberbullying is the use of electronic devices to harass or humiliate others. This is gradually increasing due to COVID-19 pandemic because of excessive reliance on online platforms (Oshodi et al., 2024). Cyberbullying is where an individual uses electronic devices to make fun or humiliate another. It has predominantly happened during the pandemic due to heavy reliance on online forms of interaction and connection (Oshodi et al., 2024). "Cyberbullying is bullying with the help of digital technologies such as mobile phones, laptops, cyber cafes, and other online media" (UNICEF), which results in anxiety, depression, and lack of self-dignity (Livingstone & Blum-Ross, 2023; Marsh et al., 2024). Research has shown that approximately 15 percent of all children worldwide use the cyberspace platform quite often for bullying each other. This, thus makes them disturbed in their daily lives.

Inappropriate and offensive content has a wide range of forms from explicit images and violence to bullying online. While surfing the Internet, youngsters and children have the potential to come across hate speech and violence - including those messages that lead to self-inflicted harm as well as even suicide (United Nations). Approximately 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online. Exposure to pornography and sexual content can negatively impact a child's health. Therefore, families should play an active role by tracking down the online activities of their children.

There are an estimated 500,000 online predators active each day and children between the ages of 12 and 15 are especially manipulated by adults online (Child Crime Prevention and Safety Center). According to Elgersma (2017), predators mostly target kids who post revealing pictures, divulge past sexual abuse, and/or engage in sexual talk online (Elgersma 2017). "In the present era, children spend

more time on the internet after the lockdown, which enhanced risks of online exploitations by predators and hackers" (Hindustan Times, 2020). Such case studies indicate a variety of patterns with grooming and manipulation, with predators forming relationships with children to exploit them sexually or emotionally (Wurtele & Kenny, 2024). Parents and teachers should teach children about online exploitations via digital literacy. It says in the study by Livingstone and Blum-Ross (2023) and Marsh et al. (2024) that the psychological and mental impacts of cyberbullying can adversely affect one's well-being. Anxiety disorders, depression, and low self-esteem can sink in. About 15 percent of the children are cyberbullied occasionally enough to affect their lives in the study by Kowalski et al. (2024). Therefore, acts against the perpetrators would be beneficial to the children involved.

Most of the things said and done in this context of cyberbullying are indecently offensive and sometimes involve secret videos, hate messages, obscene pictures, or online bullying. Phishing means criminal techniques ranging from ransomware attacks, data breaches, identity theft, to all types of monetary fraud (Sarkar and Shukla, 2023). Victims also may feel ashamed of themselves or may feel that they have been violated due to the infringement of their privacy, which would graze past the level of being looked upon as a mere criminal offense, thereby resulting in financial loss that may psychologically affect them negatively (Cross et al., 2020). The infusion of digital technologies oftentimes adversely impacts the existence of adolescents. The adolescent considers social networking sites as a novel ground to show their pictures, images, and videos on their platform (Khalaf et al., 2023). Though digital technology may hypothetically create forums for social interaction, excess or prolonged use may bring more harm than good (Pandya and Lodha, 2021).

Legal policies and government policies are instrumental in maintaining cyber security for children. There are some legislations by different nations for governing online information, improving protection of privacy, and taking the digital platforms into account. Enforcing such policies and making them stricter can give children a more secure online environment in India. Educational programs should be combined with parental controls which offers a comprehensive approach to addressing these risks (Oshodi et al., 2024). It will provide technical safeguards that limit exposure to harmful content and monitor online activity (Oshodi et al., 2024). Further, building trust so that children are willing to talk about their online activity can avert possible threats from getting out of hand (Wolak et al., 2008). Also, technology firms must engage the governments and children's protective groups to build cross-industry safety guidelines for kids in the digital realm (UNICEF, 2015). Transparency regarding the data collection process and designating a kid-friendly character within the app development can improve safety on the Internet. Cyberspace education must transcend schooling and expand into community-based programs. In spite of the hindrances involved in cyber safety, preventive measures can greatly deter online danger for children. By developing digital literacy, instating effective regulatory guidelines, and inculcating parental participation, society can fashion a safer environment for children to be online.

V. CYBER SAFETY AND THE SDGs

Cyber threats affect critical infrastructures, financials and personal data and are becoming a threat in almost every organisation. Cybercrime has become a global problem that costs the world economy over $6 trillion every year according to the World Economic Forum. The digital divide is still a problem that limits the availability of technology and cybersecurity awareness before the global population. Extreme dependence on the Internet has grown worldwide, yet the gap between the developed and developing nations remains. The International Telecommunication Union publishes a report that 63% of the population has Internet access, with lower rates observed in the least developed nations. The second element of this research aligns with the United Nations Sustainable Development Goals (SDGs), which acknowledge the significance of secure digital spaces for sustainable growth. It is closely linked to SDG 4 concerning quality education as it advises the incorporation of digital literacy into educational frameworks, ensuring that children acquire the necessary skills to use the Internet safely. It has a direct relation with SDG 4 on quality education as it recommends integrating digital literacy in education systems so that children are prepared with the right skills for using the Internet safely. It also relates to SDG 5 on gender equality because it raises the concern of girls' higher probability of being exposed to risk in the online world, including cyberbullying, online harassment, and exploitation. Furthermore, the research also points to its relation to SDG 10 which is inequality reduction through the promotion of inclusive and accessible digital solutions to avoid children from vulnerable groups being marginalised by ignorance or financial constraints. It also has to do with SDG 16 that has to do with peace, justice, and institutions, which stress on the need for appropriate legal and institutional frameworks to combat cyber threats and to provide children with a secure cyber environment.

SDG 4 (Quality Education)- Cyber security is importance in achieving many of the SDGs, particularly "SDG 4," which focuses on inclusive and equitable quality education and the promotion of lifelong learning opportunities (UNSDG, 2017). Digital learning has become a critical component of contemporary education, as virtual classrooms, e-learning courses, and online platforms offer educational opportunities to different socio-economic communities (UNESCO, 2024). The increasing dependence on digital platforms has created the urgency for effective cybersecurity interventions against some of the cyber threats that corrupt the education process. There is an evident correlation between "Cyber safety" and "Sustainable Development Goal 4" (SDG 4). First of all, the safety of children from online threats assures attendance and concentration at online classes without the fear of cyberbullying and exploitation. Research suggests that bullying by electronic means has a negative impact on academic learning and mental health, with increased absenteeism and less motivation for attending classes (Hinduja and Patchin, 2020). Hence shielding children against online threats directly supports their right to quality education and helps in supporting the key goals of SDG 4. Moreover, digital literacy is another role that plays the most significant part in education systems around the world. Cyber safety through digital literacy programs helps children and recognizes digital threats while encouraging them to develop critical thinking skills and show responsible online behaviour among themselves. Countries that have

included digital literacy in their instructional curriculum have seen increased awareness of cyber safety among learners and a decrease in cybercrime (Livingstone & Stoilova, 2021). Therefore, considering cyber safety within the educational framework in India will help lay a foundation such that SDG 4 objectives are propounded towards improvement in digital skills and facilitating a safer environment for learning. Hence protection of children from online threats basically fortifies their right to quality education and makes that even more attainable.

SDG 5 (Gender Equality)- "SDG 5" focuses on eliminating not only discrimination but also crimes against girls and ensuring equal opportunities for girls in all life aspects, developing more access in breaking across the digital divide (UN Women). Most girls undergo online harassment, stalking, and abuse, which restricts them from pursuing learning, socialising, and career opportunities. Gender-sensitive policies apply for this situation, in which the cybersecurity response must be among them. Cyber safety is further a gender-sensitive area with its stringent cyber laws to prevent harassment; creating reporting mechanisms for complaints; or more generally, conducting awareness campaigns to educate girls about their digital rights, how to stay safe, and how to report abuses. The contribution of schools and educational institutions is huge towards ensuring cyber safety education in their curriculum so that children, especially the girl child, can learn how to identify threats in cyberspace and how to report them. Promoting female involvement in cybersecurity jobs can begin creating an inclusive environment on the digital front, where policies and technology solutions would benefit from integrating gender perspectives.

SDG 10 (Reduced Inequalities)- Digital inequality is prevalent in India. SDG 10 highlights all forms of discrimination faced in the digital world and emphasises the need for reducing inequalities in the present digital era. Very few rural or economically disadvantaged children have exposure to digital literacy programs, thus putting them at risk of cyber threats, which include online scams, misinformation, and cyberbullying (Singh, 2010). Children with disabilities experience accessibility barriers to online platforms, thus denying them their full chance to participate in online learning and socialisation. Such a rights-based cyber safety framework ensures that all policies and programs address the inclusion of all children, irrespective of their socio-economic background, disability, or gender (UNESCO, 2007). Cyber threats are pronounced against the marginalised spaces, thus further deepening digital inequalities. Children from low-income families often lack parental guidance in matters of online safety, as caregivers lack digital literacy, thus exposing them to cyber threats, such as grooming, cyber harassment, and data privacy violations (Livingstone et al., 2017). A multi-stakeholder approach will be vital to actualising equitable cyber safety for children. Government policies should include public-private partnerships toward developing child-friendly digital platforms. Schools must also enforce the incorporation of cyber safety education in their curriculum. NGOs and community organisations have a major role to play in achieving awareness in the context of cyber safety, mainly for those marginalized children who do not enjoy formal digital education (UNICEF, 2021). Amendments in cyber laws along with better enforcement mechanisms will contribute towards curtailing cybercrime against children and

ensuring accountability in online platforms to protect minors (Bajpai, 2017). "Vision Viksit Bharat 2047" shows a picture of India where digital inclusion is the birthright of every child and an equitable and safe participation in cyberspace. Alignment of cyber safety initiatives with SDG 10 would protect marginalised children from online vulnerabilities, while also enabling their equal participation in the digitised opportunities. Reducing digital inequalities and ensuring a safe digital future for all children in India could thus be achieved by improving digital literacy, strengthening cyber law enforcement, and promoting inclusive digital policy.

SDG 16 (Peace, Justice, and Strong Institutions)- SDG Goal 16 is all about building peaceful and inclusive societies, access to justice, and building effective and accountable institutions (UNSDG, 2017). The Internet has become a determinant space, especially in education and socialisation for children; because of its unregulated and unsafe nature which poses serious danger (Livingstone & Third, 2017). Most children are suffering cyberbullying, online exploitation, and exposure to harmful content; consequently, digital governance and legal protection become essential (UNICEF, 2021). A rights-based cyber safety approach matches with SDG 16 in improving laws, strengthening child protection policies, and improving ethical digital governance. Effective policies and solid legal frameworks make secure cyberspaces where children are protected from cyber threats. In India, the Information Technology (IT) Act, 2000 and the Protection of Children from Sexual Offences (POCSO) Act, 2012, deal with cybercrimes against minors, but loopholes in enforcement and awareness persist. Cyber safety awareness should be implemented in schools and colleges. Digital literacy programs should be arranged which will make children aware about different types of online harms and threats. The last thing that needs to be done is to make digital spaces friendly for children in compliance with safety and privacy regulations. Such work needs the joint participation of the government, the technology companies, and the civil society organisations (Singh, 2020).

A rights-based approach would ensure that the digital platforms create and comply with ethical and child-safety standards. It ought to be for social media, internet service, and online education to carry out child-friendly privacy, tougher content moderation, and real-time monitoring of cyber threats regarding transmitting data from outside. There must be availability of facilities for children through which convenient reporting mechanisms could be made as well as access to legal assistance to victims dealing with cyber threats, so that fast justice and institutional accountability could be built in. Ensuring children have a safe and rights-compliant digital ecosystem is crucial to the development story of India in the context of Vision Viksit Bharat 2047. Tailoring the cyber safety initiatives with SDG 16 strengthens the cyber laws as well as institutional accountability and promotes ethical digital governance. It promotes cyberspace which is peaceful, secure, and just; in this way, India would be protecting the children from cyber threats while allowing the safe rights-based digital participation for its children.

VI. LEGAL AND POLICY FRAMEWORK FOR CYBER SAFETY IN INDIA

India has acknowledged the mouth for the importance of cyber safety among children by various legal and policy initiatives. The National Cyber Security Policy (2013) elaborates further towards strengthening the cyber safety measures for children and creating awareness regarding cyber hygiene (Adopted by the "Ministry of Electronics & Information Technology, India," 2013). Still, there is a necessity for more child-specific cyber safety regulations, which will meet the expectations of emerging threats in the digital world. Countries such as the United Kingdom and Australia have specific laws regarding it. The UK Online Safety Act (2023) requests social media platforms to merge child protection mechanisms (UK Parliment, 2023); India needs to find a way towards adopting such regulatory frameworks as a further step in its fight of protection online children towards promoting compliance within the objectives of Vision Viksit Bharat 2047.

Cybercrime has repercussions regarding the economic stability and growth of a country. This includes loss in various forms, like frauds pertaining to finances, theft of intellectual property, or cyber espionage disrupting businesses and leading the investors to lose confidence. European Union Agency for Cybersecurity issued a report in 2023, which indicates that 60% of the SMEs hit by cyberattacks are forced to close their businesses within six months. Data misuse and deception through false news are directly threatening democratic governance and public trust. Misinformation can be dangerous, as seen by COVID-19 where false treatment and vaccine claims run wild in digital spaces. The role of governments, as well as of international organisations in ensuring cyber safety, is full of significance. Policies and regulations must grow with emerging cyber threats. Educational initiatives on cybersecurity and workforce development underpin a secure digital future. There is a severe dearth of cybersecurity professionals, which results in a highly skill-gap and threatens organisations. Cybersecurity Ventures (2023) predicts that by 2025, there will be 3.5 million unfilled jobs in the cybersecurity sector. Digital age sustainability requires a careful balance between development and security. The Open-Ended Working Group at the United Nations on Cybersecurity aims to establish new global standards while increasing capacity-building in cybersecurity in accordance with Sustainable Development Goal 17 on global partnerships. This raises the stature of the new normal regarding the setting of the ground for harmonising future technological progress and security considerations. Cyber safety is a factor in environmental sustainability as well. The escalating digital footprint from data centers to electronic waste is pressing environmental problems. Greener IT initiatives such as energy-efficient data centers and e-waste recycling programs can reduce the adverse environment impacts of digital growth.

A well-grounded policy and legal framework are essential to ensure the safety of children in cyberspace while securing their rights in the digital world (Holmarsdottir, Seland, Hyggen, & Roth, 2024). Governments in the world over have employed various legal instruments and policies to mitigate the online threats which children are vulnerable to (OECD, 2020). In India, measures such as the enactment of several legal provisions and regulatory schemes have been introduced to respond to this menace which include, among others, the Information Technology (IT) Act of 2000, the Protection of

Children from Sexual Offences Act, and the National Cyber Security Policy (Romaniuk & Manjikian, 2021). The core of this regulatory framework is the IT Act of 2000, which provides for the recognition of electronic transactions and prevention of cybercrime in India (Ministry of Law, Justice and Company, India, 2000). The "Section 67B" of the IT Act provides that the publication and distribution of child sexual abuse material (CSAM) is an offense, thereby providing further/greater protection to children in the digital environment (Ministry of Law and Justice, 2000). The "POCSO Act" complements the provisions for protection against online exploitation of children with severe penalties for offenses against minors committed online (Ministry of Women and Child Development, 2021). Internationally, the UN Convention on the Rights of the Child asserts that children have the right to receive information but should also be protected against harmful information. Article 17 of UNCRC underlines the need for the intervention of the state to safeguard children against online harm, and Article 19 expands on measures to protect from abuse and exploitation in cyberspace (United Nations, 1989). Nevertheless, notwithstanding these laws, the implementation of safety measures for children is beset with challenges. Law enforcement authorities suffer limitations of jurisdiction, deficiency with respect to the collection of digital evidence, and slow reaction to the technological innovation that is outrunning the legal framework. Besides, low levels of awareness on the existence of the cyber laws among parents, educators, and the children themselves aggravate vulnerability (UNICEF, 2021).

Consequently, adopting a methodology involving all stakeholders, including government, technological firms, and civil societies, for the advancement of cyber safety is essential. For enhancing online child safety, public-private partnerships should therefore harness technical interventions such as artificial intelligence content moderation, age-appropriate digital access controls, and secure communication platforms. In addition, global cooperation can make cyber law enforcement easier to achieve to address cross-border problems of child exploitation on the internet (World Economic Forum). Cyberlaw and regulatory setup for child protection in the cyber environment will become crucial as India progresses towards Vision Viksit Bharat 2047. Policymaking needs to be centered around children at the national cybersecurity level, and education on digital rights must become a part of school curriculums in order to help children navigate safely and responsibly within the online universe (UNICEF, 2022).

VII. CONCLUSION

This research study has brought home the importance of placing principles for the protection of children in digital governance frameworks. This would ensure safety, security, and an overall safe online environment for all children. To strengthen the existing legal and policy frameworks is absolutely crucial to tackling the emerging threats in cyberspace, as the currently existing regulations often lack the specificity and agility required to counter evolving online risks (Livingstone & Third, 2017).

It is also important to note that there exists the importance that is placed by digital literacy programmes for children on which they are concerned about empowerment with knowledge and skills for navigating cyberspace in the safest possible manner. Initiative with awareness or knowledge regarding online risks can be mainstreamed into the school curriculum, thereby ensuring that all socio-economic groups can benefit from structured cyber safety training at the school level (Grey, 2011). The suggestion of a multi-stakeholder approach is that of parents, schools, policymakers, and technology companies in trying to create a safe digital ecosystem. The active surveillance of children's online activities should include parents and caregivers as active partners.

Structured digital safety education programs must be designed by schools, and a shared responsibility for technology companies would be to design platforms emphasising child safety with enhanced privacy settings, content moderated by AI, and proactive risk mitigation strategy (UNICEF). Improved cross-sector collaboration in cyber safety may also find greater synergies in national and international child protection, thereby defining a more holistic context of country-specific capability (ITU). These safety efforts in cyberspace correspond to Vision Viksit Bharat 2047; thus, India remains committed to the creation of an inclusive digital society in which children's rights are respected.

These policies on cyber safety can further be incorporated in correlation to all the Sustainable Development Goals (SDGs) applicable to integrated child development in the digital world, especially SDG 4 (Quality Education), SDG 5 (Gender Equality), SDG 10 (Reduced Inequalities), and SDG 16 (Peace, Justice, and Strong Institutions) (UNDG 2017). Thus, cyber safety not only protects children from online harms, but also empowers them to use the digital medium to fullest possible for learning purposes, in terms of growth, within a resilient and digitally empowered society.

VIII. REFERENCES

1. Bajpai, A. (2017). Child Rights in India. Oxford University Press.
2. Bandura, A. (1977). Social learning theory. Prentice-Hall.
3. Bon, A., Saa-Dittoh, F., and Akkermans, H. (2023). Bridging the Digital Divide. In book: Introduction to Digital Humanism, 283-298. http://dx.doi.org/10.1007/978-3-031-45304-5_19
4. Bronfenbrenner, U. (1979). The Ecology of Human Development. Harvard University Press.
5. Chaturvedi, S. 2025. Safer Internet Day: Building resilient and cyber-secure ecosystem to empower India's digital nagriks. The Economic Times, February 11. https://government.economictimes.indiatimes.com/news/secure-india/safer-internet-day-building-resilient-and-cyber-secure-ecosystem-to-empower-indias-digital-nagriks/118136283
6. Children and Grooming / Online Predators. https://childsafety.losangelescriminallawyer.pro/children-and-grooming-online-predators.html

7. Cross C, Richards K, Smith RG (2016) The reporting experiences and support needs of victims of online fraud. Trends and Issues in Crime and Criminal Justice 518: 1–14.
8. Cyril, G. (2020). Digital age: Keep your children safe from online predators and hackers. Hindustan Times, May 8. https://www.hindustantimes.com/more-lifestyle/digital-age-keep-your-children-safe-from-online-predators-and-hackers/story-L5cKAVVgJlRRNowyxmt8MP.html
9. Elgersma, C. (2017). Facts about online predators every parent should know. Commonsense Media. https://www.commonsensemedia.org/articles/the-facts-about-online-predators-every-parent-should-know
10. Federal Trade Commission. (2021). Children's Online Privacy Protection Rule ("COPPA"). Retrieved from https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
11. Ferrari, A. (2013). DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. European Commission. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC83167/lb-na-26035-enn.pdf
12. Government of India, Ministry of Electronics and Information Technology. (2024). National Cyber Security Policy [Unstarred Question No. 3789, Lok Sabha]
13. Grey, A. (2011). Cyber Safety in Early Childhood Education. Australian Journal of Early Childhood, 36(2), 77-81. https://doi.org/10.1177/183693911103600210
14. Holmarsdottir, H., Seland, I., Hyggen, C., & Roth, M. (Eds.). (2024). Understanding The Everyday Digital Lives of Children and Young People.
15. Hinduja, S. & Patchin, J. W. (2020). Cyberbullying Identification, Prevention, and Response. Cyberbullying Research Center. https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2020.pdf
16. International Telecommunication Union. Child Online Protection Guidelines. https://www.itu-cop-guidelines.com/
17. Khalaf et al. (2023). The Impact of Social Media on the Mental Health of Adolescents and Young Adults: A Systematic Review.
18. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4). http://dx.doi.org/10.1037/a0035618
19. Livingstone, S., & Helsper, E. J. (2007). Gradations in Digital Inclusion: Children, Young People, and the Digital Divide. New Media & Society, 9(4), 671–696. http://dx.doi.org/10.1177/1461444807080335
20. Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für

Medienforschung | Hans-Bredow-Institut (HBI); CO:RE- Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

21. 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
22. Meda, K. 2024. Identity theft is being fueled by AI & cyber-attacks. Fraud Prevention Manager & SME / Deseret First Credit Union, May 3.
23. Ministry of Education, India. NEP Regulations/Guidelines/Framework. https://www.education.gov.in/nep/regulations-guidelines-framework?shs_term_node_tid_depth=511
24. Ministry of Electronics &Information Technology, India. (2013). National Cyber Security Policy 2013. https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
25. Ministry of Law, Justice and Company, India. (2000). The Information Technology Act, 2000. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C
26. Ministry of Women and Child Development, India. (2021). Steps to tackle Cyber Crime against Children. https://pib.gov.in/PressReleasePage.aspx?PRID=1706002
27. Murray, J., Swadener, B. B., & Smith, K. (Eds.). (2024). The Routledge international handbook of young children's rights. Routledge.
28. NITI Aayog. (2022). Vision Viksit Bharat 2047: A roadmap for India's future. Government of India.
29. OECD. (2020). Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and policies. https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/protecting-children-online_0c385619/9e0e49a9-en.pdf
30. Office of the United Nations High Commissioner for Human Rights. (1989). Convention on the Rights of the Child. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
31. Oshodi et al. (2024). Combining parental controls and educational programs to enhance child safety online effectively. Vol 6, no. 9.
32. Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and Self-Esteem. Journal of School Health, 80(12), 614–621. https://doi.org/10.1111/j.1746-1561.2010.00548.x

33. Pokhrel S., Chhetri R. (2021). A literature review on impact of COVID-19 pandemic on teaching and learning. Higher Education for the Future, 8(1), 133–141. 10.1177/2347631120983481
34. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology: Interdisciplinary and Applied, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803
35. Romaniuk, S. N., & Manjikian, M. (Eds.). (2021). Routledge companion to global cyber-security strategy. Routledge.
36. Sahota, N. (2024). AI Shields Kids by Revolutionizing Child Safety And Online Protection. Forbes. https://www.forbes.com/sites/neilsahota/2024/07/20/ai-shields-kids-by-revolutionizing-child-safety-and-online-protection/
37. Sarkar, G., Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, Vol. 2.
38. Singh, S. (2010). Digital Divide in India: Measurement, Determinants and Policy for Addressing the Challenges in Bridging the Digital Divide. International Journal of Innovation in the Digital Economy, 1(2), 1-24. http://dx.doi.org/10.4018/jide.2010040101
39. Staksrud, E., & Olafsson, K. (2013). Does the use of social networking sites increase children's risk of harm? Computers in Human Behavior, 29(1), 40–50. http://dx.doi.org/10.1016/j.chb.2012.05.026
40. Twenge, J. M., Joiner, T. E., Rogers, M. L., & Martin, G. N. (2018). Increases in depressive symptoms, suicide-related outcomes, and suicide rates among U.S. adolescents after 2010 and links to increased new media screen time. Clinical Psychological Science, 6(1), 3-17. https://doi.org/10.1177/2167702617723376
41. UN Sustainable Development Group. (2020). Policy Brief: Education during COVID-19 and beyond. https://unsdg.un.org/resources/policy-brief-education-during-covid-19-and-beyond
42. UN Women. SDG 5: Achieve gender equality and empower all women and girls. https://www.unwomen.org/en/node/36060
43. UNESCO. (2007). A human rights-based approach to education for all: A framework for the realization of children's right to education and rights within education. https://unesdoc.unesco.org/ark:/48223/pf0000154861
44. UNESCO. (2024). Why does UNESCO consider digital innovation in education important? https://www.unesco.org/en/digital-education/need-know
45. UNICEF. (2015). Guidelines for Industry on Child Online Protection. https://www.unicef.org/media/66616/file/industry-guidelines-for-online-childprotection.pdf
46. UNICEF. (2021). The State of the World's Children 2021. https://www.unicef.org/reports/state-worlds-children-2021#:~:text=The%20State%20of%20the%20World's%20Children%202021%20examines%20child%2C%20adolescent,mental%20health%20and%20well%2Dbeing

47. UNICEF. (2022). Child Online Protection in and through Digital Learning. https://www.unicef.org/eca/media/22501/file/Child%20Online%20Protection%20in%20and%20through%20Digital%20Learning.pdf
48. UNICEF. (2022). Child online protection: Keeping children safe in the digital world. from https://www.unicef.org/protection/child-online-protection
49. UNICEF. Children's Rights in the Digital World. https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf
50. UNICEF. Protecting children online. https://www.unicef.org/protection/violence-against-children-online
51. United Nations. (1989). Convention on the Rights of the Child. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
52. United Nations. Sustainable Development Goals. https://unric.org/en/united-nations-sustainable-development-goals/
53. UNSDG. (2017). Goal 16: Promote just, peaceful and inclusive societies. https://www.un.org/sustainabledevelopment/peace-justice/
54. UNSDG. (2017). Goal 4: Ensure inclusive and equitable quality education and promote lifelong learning opportunities for all. https://unstats.un.org/sdgs/report/2017/goal-04/
55. Virmani, A. (2024). Viksit Bharat: Unshackling Job Creators and Empowering Growth Drivers. NITI Aayog. https://www.niti.gov.in/sites/default/files/2024-07/WP_Viksit_Bharat_2024-July-19.pdf
56. Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of young people's vulnerabilities to online grooming. Aggression and Violent Behaviour, 18(1), 135-146. http://dx.doi.org/10.1016/j.avb.2012.11.008
57. Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online "predators" and their victims: Myths, realities, and implications for prevention and treatment. American Psychologist, 63(2), 111-128. https://doi.org/10.1037/0003-066x.63.2.111
58. World Economic Forum. (2023). Global Cybersecurity Outlook 2023. https://www.weforum.org
59. World Economic Forum. Partnership against Cybercrime. https://initiatives.weforum.org/partnership-against-cybercrime/home
60. Wurtele, S. K., & Kenny, M. C. (2024). Online predators and child exploitation: A review of current research and prevention strategies. Child Abuse & Neglect, 128.