International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST218124

Cyber Crime and Children in Digital Era

Madhu Kumari
Department of Journalism and Mass Communication, Banasthali Vidyapith, Rajasthan, India

ABSTRACT

Article Info
Volume 8, Issue 1
Page Number: 151-160

Publication Issue :
January-February-2021

Article History
Accepted : 01 Jan 2021
Published : 06 Jan 2021

Cyberspace is a virtual world or online world. It is an artificial world created by computers or internet enabled devices or components to communicate. It is digital platform where users interact and communicate with one another with the help of internet. The cybercrime is a rapid growing area of crime in the world. It is defined as a crime in which computers or internet enabled devices to commit an offenses which is categorized into two types such as property crimes (hacking, spamming, identity theft, fraud and copyright infringement) and crimes against the person (child pornography, sexual abuse of children, cyber stalking, cyber bullying). Crimes in the virtual world is serious threat to the people as cybercriminals uses computer technology to access the personal and professional information or documents of person or organization for evil or malevolently reasons. The aim of the paper is to render the psychology of child predation and child pornography online in India. This paper will discuss about the different measures which should be taken to protect and educate the children about cyber bullying and cyber stalking in India. It will also highlight the legal intervention, effects on victims, punishment and preventative measures for a broad range of cybercrimes. The study will also understand the psychology behind the cybercrimes such as child sex offences and how such crimes can be prevented. The aim of the study is to discuss the role of government and policy makers for the rehabilitation of victims against cybercrimes. The paper will suggest some measures for the holistic development and security of children.

Keywords : Children, Cyberspace, Cybercrime, Intervention, Psychology

I. INTRODUCTION

In contemporary era, the world is fully dependent on digital space for communication and interaction through social media, financial transaction, mobile transaction etc. As growing dependency on internet is the result of innovation in technological advancement. The present world is widely taking profit of internet for end numbers of activities which is making their lives comfortable and entertaining. The internet or internet enabled devices are fully ruling the every sector such as railway, academics, research, space,

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

telecommunication, health, banking, airport, social media etc. every innovation or technology changes the lives with positivity but it also has some bad effects also.

In the year 1982, William Gibson in his science fiction namely '*Neuromancer*' used the word 'cyberspace' for the first time. He defines *cyberspace* as *"A consensual hallucination experienced daily by billions of legitimate operators,… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light arranged in the nonspace of the mind, clusters and constellations of data."*

Cyberspace is a virtual space constituted by information technologies. It is the combination of a networking and visualization. It is on-line world of computers and internet enabled devices where users communicate. It allows users to disseminate information and interact. It is a digital world where users communicate and discuss, generate ideas for social issues or other activities. It is used to encourage the interaction and discussion through digital platform which can't be sensed or felt as real world. *F. Randall Farmer* and *Chip Morningstar*, IT experts opined that cyberspace has become more popular among users as medium of social interaction and discussion. However, they felt that cyberspace is not so known as its technical execution and implementation.

Cyberspace is a domain which uses electronic and the electromagnetic spectrum with physical infrastructure to store, rectify and disseminate data. With the advancement and innovation in the cyberspace has changed the lives of users. The growing knowledge of cyberspace by individuals has given the birth of the cybercrimes. The cybercrimes has no borders or boundaries and growing at very past pace.

Crime has become inevitable part of our lives and society. We can feel the crime rates are increasing every day in all the societies of the world. The struggle is going in everyone lives between who commit heinous crime and those who want to curb, prevent, detect or punish the criminal activities and tries to strike balance between them. Nowadays people spend their most of the time on digital space for interaction, discussion, debate, pleasure or work. The increasing dependency on digital world for communication, socialization, financial transaction, entertainment or business is becoming matter of concern and struggle. The offences or illegal activities which take place on or using the one or more components or medium of the internet are known as cybercrimes. Any criminal offence on web using the medium of internet such as email, chat, websites, apps etc to conduct unlawful financial transaction, harassment, online child sexual abuses, pornography, cyber terrorism, stealing or leaking personal information, hateful posts for violence or riots.

Cybercrime includes a plethora of unlawful activities and growing as threat or problems for modern world. The criminal activities on the web or violation of law on digital world are increasing day by day. The cybercrime can be categorized into two such as 'property crimes' and 'crimes against person'. The property crimes can be illegal transaction, identity theft, scam, fraud and copyright infringement and cyber stalking, cyber bullying, child pornography, leaking private pictures or videos come under crimes against the person.

Cybercrime is rapidly increasing area of crime. Criminals use new and advanced technology against individuals, businesses and governments for cybercrime. It is an act of illegal transaction and trespassing into the computer system for theft or manipulation of data. Because of the speed ease and anonymity of the internet cyber criminals violates the law and commit wide range of criminal activities which is very harmful and dangerous to the users worldwide.

National Crime Record Bureau (NCRB) released the ‘Crime Report-2017’ in 2019. According to the report, the cyber crimes are increasing rapidly and constantly in India. The number of cyber crimes reported were 9,622 in 2014, it amplified in 2016 with 11, 592 cases and the number of cyber crimes goes up in 2016 with 12, 317.

The aim of pure cybercrime is to gain illegal access to the device or deny access to genuine or lawful users. The monetary offences such as financial frauds, online theft or scam and non-monetary illegal act such as cyber bullying, cyber stalking, child pornography, creation and distribution of viruses on personal, corporate and government computers or leaking and viral secret, confidential and important business and private data or information on the cyber world.

Cybercrime in Indian context defined as a voluntary and willful or deletion that badly affects an individual or finances or one’s computer system and liable to penal consequences under the IT Act 2000 (Information Technology Act) mentioned in the Indian Penal Code.

II. Cybercrimes: Different types/forms

1. Cyberstalking

Oxford dictionary defined stalking as “pursuing stealthily”. Cyberstalking means when a person is continuously followed harassed online. It is a type of harassment and can invade the privacy of an individual and leave them petrifying and lonely. It can be both online and offline. Offline stalking means tracing the physical location of the victim and follows them. Distribution of offensive online messages to the public, false accusation about the victim, gathering information, sending direct or indirect messages, attempting to meet the victim are the some of the common behaviours of cyberstalking.

2. Cyberbullying

The use of electronic medium for converted psychological bullying by sending or posting threatening or scary messages. It is willful and repeated act of sending offensive and vulgar messages through the electronic devices such as mobile phones, computers, laptops etc.

3. Child Pornography

Child Pornography is a criminal offence that constitutes the internet-related sex crimes and visual presentation of minor in sexually explicit activity. It is offence which involves the electronic devices such as i-pad, mobile phones, i-phones, digital cameras, photo editing software and web camera for the development of naked and semi-naked pictures of minors and dissemination through social networking sites. With the advancement in technology, the vulgar videos or images of minor can be developed and circulated with less expense and in higher quality and it can be duplicated and distributed easily. Due online nature of offence, the culprit has a false sense of ambiguity.

4. Cyber terrorism

Cyber terrorism is the act of Internet terrorism in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses

5. Continuous and unwanted exposure and reach to sexually explicit content or material

The increasing exposures of Internet pornography have harmful effect not only on adolescents but youth and society as whole as it arouses sex desire. The regular exposures of online sexually explicit material have certain vulnerabilities such as delinquent tendencies, depression, interpersonal victimization, Posttraumatic Stress Disorder etc.

6. Hacking

The process of unauthorized access of an information system or network to evade the privacy is called Hacking. Hacker is someone who gains authorized or unauthorized access to modify or threaten the system.

7. Intellectual Property Crimes

The creations of the mind such as literary and artistic works, design, symbols, images, inventions etc is known as Intellectual Property. There are four types of Intellectual property are Trade Secrets, Trademarks, Copyrights, and Patents.

Intellectual property theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. It is crime committed when someone uses an intellectual property right without the permission of its owner. Intellectual Property Rights infringement is Counterfeiting and Piracy.

8. Phishing

Phishing is technique of deceitfully gaining access to private information. The phisher sends an email from a website claiming to be your bank or Credit Card Company to fill form online requesting ATM Card's PIN, OTP or home address. It is one of the chief ways in which people's identity stolen and a computer filled with viruses.

9. Online Gambling

In India gambling is prohibited under the Public Gambling Act of 1867 which prohibits running or being in charge of a public gambling house. The business of placing, receiving or transmitting a bet or wager through internet is called Internet/Online Gambling.

10. Distribution of pirated software

The illegal copying, distribution or unauthorized reproduction of software without proper license for personal or commercial use is called software piracy. It is profitable business because one can produce number of copies. It can be controlled by awareness programmes and enforcing laws.

11. Cyber Trespass

Trespass means to enter into other's property without prior consent or permission which is ordinarily considered as a civil wrong. Criminal trespass means the trespassing is done with the criminal intention or motive. The cyber trespass is application in cyber world.

12. Cyber extortion

It is a crime by malicious hackers to a website or network, email server, computer system by threat or attack. The hackers demand money or lucrative targets in return for remediating the attack or provide protection. Corporate businesses are more vulnerable to these attacks.

13. Spam

Spam means unwanted and inappropriate messages continuously sent over the internet to large numbers of users which includes junk fax spam, instant message spam, classified ads spam, social media spam, blog spam pop-up ads spam, search engine spam, wiki spam etc.

14. **Identity Theft**

    Identity theft means to refer a fraud to impersonate others (such as their name, address, date of birth) to facilitate crimes which include illegal immigration, espionage, terrorist activities, blackmail etc. Financial Theft, Criminal Theft, Business/Commercial Identity and Identity Cloning Theft are four categories of Identity Theft.

III. Online risks and threats for children

In today's digital era, internet is used as a tool for various types of cybercrimes against children and women. Cyber security has become major concern in contemporary age.

Children are most vulnerable for online abuse and exploitation because of excessive use of ICT (Information and Communication Technology). With the growing digital advancement in ICT and regular use of various social networking sites by children such as Viber, Tumblr, Linkedln, Pinterest, Flickr WhatsApp, Instagram, SnapChat, Facebook, Twitter, Google +, Hike, Tinder exposes them to online abuse, cyber bullying and exploitation. Children are very fond of social networking sites such as YouTube, Instagram and Snapchat as survey conducted by *Pew Research Center* in March-April, 2018. The survey highlighted that 95% adolescents are regular user of smart phone throughout the globe and 45% children are online throughout the day on regular basis.

An Internet & Mobile Association of India (IAMAI) conducted a survey in November, 2015 in 35 Indian cities. The report named '*Internet in India*' highlighted that among 400 m internet users, 28 m users were school children. Telenor & Boston Consulting Group conducted a survey in 2012 and presented report '*Building Digital Resilience*'. The survey also highlighted that children are the most vulnerable in terms of online threat in India as per the survey which was conducted in 12 countries.

IV. Factors responsible for recurring victimization in children

There are many primary factors responsible for child sexual exploitation both online and offline.

They include:

- Gender inequality and poverty
- Racism
- Migration
- Social detachment or loneliness
- Sexual orientation
- Abusive and unstable family
- Lack of efficient legal frameworks, policies and protection mechanisms
- Digital Illiteracy
- General profile and motivations of offenders
- Technological proficiency
- Planned criminal groups

Symptoms of child online threats, abuse and exploitation in India as per report 'Child Online Protection' in India-an Assessment by UNICEF in 2016

Cyberbullying : Emotional harassment, Defamation, Intimidation, Social exclusion

Online Sexual abuse: Sexual harassment, Sexual solicitation, Aggressive, Blackmail and Financial extortion

Online Sexual exploitation : Production and consumption of child sexual abuse material, Sexual solicitation and Aggressive, Commercial, Commercial trafficking and sexual exploitation, child prostitution, production and consumption of child pornography, Child sex tourism

Cyber radicalization : Ideological indoctrination and recruitment, Threats or acts of severe violence
Online attacks and fraud: malware infection, Pharming

Identity theft : Privacy breach, Malvertising Enticement to drug trafficking, phishing, hacking
Online enticement: Exposure to inappropriate content, access to alcohol exposure to inappropriate content, and drugs illegal, cheating, plagiarism, gambling, sexting, self-exposure

Cyberbullying: Bullying among children is indication of a disproportionate of power or strength. The children demonstrate their aggression on regular basis through intentionally or unintentionally. India ranked third for high rates of online bullying among 25 countries as per the survey *'Global Youth Online Behaviour'* conducted by Microsoft in 2012. Standing Committee on Information Technology, under Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India presented 52nd report named '*Cybercrime, Cyber Security and Right to Privacy'* in 2014 which highlighted that children are bullied and harassed online by known people or relatives is more common in India.

Online sexual abuse of children: The most common forms of children online sexual abuse in India are display or viral of sexually explicit, violent and aggressive content and sexual torture and harassment. Adolescents are exposed to various online explicit and violent materials on various digital devices due to the lack of safeguards and proper guidance at home, in internet cafes etc.

Online sexual exploitation: The number of webpage and websites showing Child Sexual Abuse Material (CSAM) has amplified by 147 percent from 2012 to 2014, in which children of 10 years or age or younger Child Sexual Abuse Material (CSAM) has amplified by 147 per cent from 2012 to 2014, in which children of 10 years or younger represented in 80 percent of these materials, according to the International Association of Internet Hotlines. The most common and popular form of online child sexual exploitation is the production and usage of CSAM which is known as Child Pornography. Cyberspace provides rich base for children for financial gain because of sexual activity as grooming which means tempting child for sexual talk, enticed etc.

Cyber extremism : Children and young people are most vulnerable for cyber extremism which is potential threat to the security and integrity of nations. The non-state actors propagate and promote radicalized extreme thought processes which are serious threat to global security in terms of terrorism.

Online commercial fraud: Online commercial fraud is growing day by day in manipulating users and gaining illegal finances. Digital natives spend more time on the internet and exposes themselves to the online fraud. According to the survey by the TCS GenY in 2013-2014, there is extreme increase in the number of online shoppers who are primarily teenagers.

Online temptation to illegal behaviours: Online gaming such as PlayerUnknown's Battlegrounds (PUBG), Blue Whale etc are very dreadful and has adverse impact on children. Several Indian psychiatrists have notion that severe addiction of video or online games, interaction and communication to the strangers on social media and Internet surfing among children has disrupted their day to day activity. It makes them violent and aggressive. A Google Trends report in 2017 of the last 12 months highlighted that India bagged the first rank in highest number of searches related to the Blue

Whale Challenge across the globe. Girls are more engaged in 'selfies' and boys are more prone to games.

V. Protection and guidance through education for digital literacy and safety

The role of the Indian Government

1) *Pradhan Mantri Gramin Digital Saksharta Abhiyan* (https://www.pmgdisha.in) started in 2017 aim to make six crore rural people digital literate by 31st March, 2020 under Digital India flagship programme. *'The scheme aims to empower rural citizens with information, knowledge, skills and enable them to actively participate in governance'*, said Shri Ravi Shankar Prasad, Minster of Law & Justice and Minister of Electronics and IT, Government of India.
2) Another programme named *Samagra Shiksha* (http://samagra.mhrd.gov.in/) by Department of School Education and Literacy, Ministry of Human Resource Development, Government of India. It includes the three schemes of *Sarva Shiksha Abhiyan (SSA)*, *Rashtriya Madhyamik Shiksha Abhiyan (RMSA)* and Teacher Education (TE). *Samagra Shiksha* focuses on Digital Education in India. It supports digital boards, smart classrooms and DTH channels from upper primary to higher secondary school education.

The leading Research & Development (R&D) organization of the Ministry of Electronics and Information Technology (MeitY), Government of India called Centre for Development of Advanced Computing (C-DAC) carrying out regular R&D in IT, Electronics and related areas. Indian Computer Emergency Response Team (CERT-In) is operational since 2004 and is Indian Cyber Community. It is a nodal agency which responds to computer security happenings. It also disseminates information, alerts and forecast cyber security incidents and creates awareness on security issues through its website (http://www.cert-in.org.in). The another initiative by MeitY called " Cyber Swachhta Kendra " which is Botnet Cleaning and Malware Analysis Centre and is a part of the Government of India's Digital India which create a secure cyber eco system in India.

The Government of Maharastra launched 'Cyber Safe Campaign' for women and children across the state on 3rd January, 2020. The Campaign will disseminate information and spread awareness against crimes and violence committed against children and women. It will create awareness about various cybercrimes such as child pornography, online gaming, bank frauds etc. the campaign will disseminate information about cyber laws with the help and support of state police, cyber call and public relations departments of government.

@CyberDost- Twitter handle launched in 2018 by the Union Ministry of Home Affairs to spread awareness about laws, prevention and precaution regarding cybercrimes through regular posts.

The Cyber Crime Prevention against Women and Children Scheme (CCPWC) was launched by the Union Ministry of Home Affairs on January, 2019 to safeguard women and children against the atrocities of cyber crimes.

VI. The role of ICT and Civil Society sectors

Amway India (a multi-level marketing company) started digital literacy program for government schools at Tata Workers' Union High School at Kadma, Jamshedpur on September, 2019 as the news published in The Pioneer, news portal. Amway will distribute computers over 5000 students in 14 schools under this initiative.

A not-for-profit industry body namely Data Security Council of India (DSCI) setup by NASSCOM for data protection in India. It is committed in establishing best practices to make cyberspace safe, secure and trusted. It organizes workshops, conferences, seminars and roundtable meetings on regular basis for cyber security.

Ahmedabad based a registered NGO named *Centre for Cyber Victim Counselling* "Helping Cyber Crime Victims" (https://www.cybervictims.org) committed to counsel cyber victims and prevent crime in the cyber space. They help in understand the nature of cybercrime, guide the victims to take legal action against it. They guide and support the cyber victims to overcome from trauma.

Ranchi, Jharkhand based grassroots civil society body *Cyber Peace Foundation* (https://www.cyberpeace.org) started in 2013. It is rare organization working tremendously for promoting cyber peace and trust in the internet. The various programmes initiated by the foundation are iSafe Alliance, Digital Shakti, e-Raksha, Cyber Clinic, Internet De-Addiction, Cyber Security Helpline, etc. which continuously create awareness about digital literacy and online safety to women and children. It also provides legal help counseling to the victims.

Cyber Peace Clubs and *Cyber Peace Corps* are other innovative initiatives to work for cyber peace in the world by the Foundation. Cyber Peace Clubs aims to form student and faculty forces to aware children about the digital literacy, pro and cons of internet across the country.

eProtect Foundation (https://www.eprotectfoundation.org/) which is based in Uttarakhand is working tremendously for women empowerment and Cyber Crime Prevention and driven by cyber security expert. *Cyber Society of India* (https://www.cysi.in/) was formed on the 6th of July 2004 in Chennai which provide a forum for research, debate and training to promote good Cyber netizen Society.

Legislation and policies by national and international bodies to regulate children from online abuse and exploitation

In India the following laws to address and regulate cybercrimes:

The **Information Technology Act, 2000**, was notifies on October 17, 2000 deals with aspects related to cyberspace cybercrime and electronic commerce in India and the Information Technology (Amendment) Act, 2008 regulate legislation and monitor the activities of cyberspace and any communication device which is used to disseminate, transmit or publicize any text, graphics, audio-visual or image etc. The Protection of Children from Sexual Offences Act, 2012 which is reinforced under the provisions of the Information Technology Act which deals with online offences, abuse, molestation, torture and exploitation against children and young ones including child pornography and grooming.

- **National Policy of ICT in Schools**, 2012 devise, catalyze, formulate, support, monitor, regulate and sustain Information and Communication Technology (ICT) and enabled activities to improve and enhance the school education for children in terms of access, quality and efficiency in the education. It also regulates the ICT to protect children from online risks.

- **National Cyber Security Policy, 2013** deals with the comprehensive, collective and collaborative efforts to works for cyber security in the country. Its vision is to build secure and resilient cyberspace for the people, businesses and government at large.

National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India

This portal https://cybercrime.gov.in/ under Nirbhaya Fund is an initiative of Government of India to report cybercrime online which ease victims/complainants. This portal deals and supports the complaints of cybercrimes against women and children.

VII. International instrument

United Nations Convention on the Rights of the Child (CRC)

'*Every Child has the Right to Survival, Protection and Education*'- UNCRC, an International agreement for child rights. *Save the Children*, change the future, movement work for child rights such as cultural, social, economic, civil and political. Being a legally-binding international organization works tremendously for the overall development of child irrespective of caste, creed, race etc. It works with more than 100 countries across the globe. https://www.savethechildren.org.uk/where-we-work/asia/india

UNICEF for every child works with more than 190 countries across the globe regularly and tremendously for rights and inclusive development of child.

Recommendations for the holistic development and security of children from cybercrimes

In present times, children are digital native and most vulnerable to cybercrimes. They need to be trained, monitored and guided to become good and responsible digital native. Digital literacy is the need of the hour for children for safe use of cyberspace. The following are some measures to control the cybercrime to children.

- Educate children about digital literacy at schools in order to make them informed, engaged and assure safety in digital world.
- Enhance the digital skills, competency and literacy of teachers.
- Aware and understand the threat of content which is generated, created and shared by children which can be accessed and mishandled by strangers.
- Children should be oriented through workshops/lectures at schools for various setting of social networking sites such as two-step verification, privacy, security in order to protect the personal, private and professional data online.
- Children should be oriented and motivated about the tolerance and empathy in digital world and which will be strengthen through socio-emotional learning which will develop and strengthen online resilience and reduce online abusive language and action.
- Parents, teachers and guardians can be good digital role models for children.
- Prevent or block the websites, networks, social networking sites and services from distributing and dissemination of materials or content which abusive and offensive for children such as porn sites, dangerous online games or activities.
- Parents should access parental lock of various online applications.
- Parents, teachers, guardian and mentors should safeguards and protect children's privacy, personal information and reputation.

VIII. REFERENCES

[1]. Kirwan, G., & Andrew, P. (2013). Cybercrime the Psychology of Online Offenders. United Kingdom: Cambridge University Press

[2]. Paranjape, V. (2010). Cyber Crimes & Law. Allahabad: Central Law Agency

[3]. Bhagtani, H.T. (2017). Cyber Crimes and Cyber Security. Mumbai: Himalaya Publishing House Pvt. Ltd.

Online References

[4]. https://www.dailypioneer.com/2019/state-editions/amway-launches-digital-literacy-initiative-for-govt-schools-kids.html
[5]. https://meity.gov.in/writereaddata/files/HOW_TERRITORY.pdf
[6]. https://indianexpress.com/article/education/international-literacy-day-why-india-needs-to-achieve-digital-literacy-now-more-than-ever-5972022/
[7]. https://www.pmgdisha.in
[8]. https://www.cert-in.org.in
[9]. https://www.cyberswachhtakendra.gov.in

Cite this article as :

Madhu Kumari, " Cyber Crime and Children in Digital Era ", International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 8, Issue 1, pp.151-160, January-February-2021. Available at
doi: https://doi.org/10.32628/IJSRST218124
Journal URL : http://ijsrst.com/IJSRST218124