(IJRSSH) 2025, Vol. No. 15, Issue No. I, Jan-Mar **e-ISSN: 2249-4642 p-ISSN: 2454-4671**

Addressing Youth Cyber Offenses: The Impact of Cyber-Security in Lucknow, India

***Dr. Saurabh Tiwari, **Ms. Hershika Verma**
*Assistant Professor, **Faculty of Fine Arts,
Department of Liberal Education Era University, Lucknow Uttar Pradesh, India, 226003

DOI:10.37648/ijrssh.v15i01.007

[1] *Received: 29/01/2025; Accepted: 25/03/2025; Published: 27/03/2025*

ABSTRACT

Human society has continually evolved throughout history, from ancient times to the present day. The emergence of the Internet, Artificial Intelligence, and various dynamic social media technologies has significantly transformed our globalized world. This qualitative research article, based on both primary and secondary data, explores the complex nature of cyber society, with a particular emphasis on Cyber- Crime, Cyber-security, Cyber-Culture, and internet addiction, especially among children in the Lucknow region of Uttar Pradesh.

The intersection of crime and internet technology has nurtured the rise of Cyber-Crime, particularly among children. In the digital realm, Cyber-Culture not only shapes societal interactions but also creates an environment that fosters Cyber-Crime through digital technology and the internet. When internet devices are used as tools or mediums for committing crimes, these acts are classified as Cyber-Crimes. Cyber-Crimes, ranging from hacking to online fraud, leverage the ever-evolving technological landscape. Deviations from traditional norms within Cyber-Culture often lead to both conventional and cyber-specific criminal behaviours, highlighting issues of Juvenile Delinquency and the importance of Netiquettes.

Keywords- *Cyber-Culture; Cyber-Crime; Cyber-security; Juvenile Delinquency; Netiquettes*

INTRODUCTION

The advent of the Internet, Artificial Intelligence, and various social media technologies has brought about significant transformations in our globalized world. This qualitative research article, drawing on both primary and secondary data, investigates various facets of cyber society, including cyber-crimes, cyber-security, cyber-culture, and internet addiction, with a particular focus on children in the Lucknow region of Uttar Pradesh. In our interconnected global society, Information and Communication Technology (ICT) is continuously evolving and is influenced by cultural phenomena shaped by these technologies. ICT, as a tool for processing and transmitting information, impacts modern social structures and contributes to the development of a network society (Castells, 1996). Information Technology (IT), often synonymous with ICT, permeates all aspects of contemporary life (Giddens, 2003). When ICT is combined with the internet, it is termed 'Cyber.' The term 'Cyber' is derived from 'Cybernetics,' the science of communication and control between machines and humans, first introduced by Norbert Wiener in 1948.

As ICT and the internet become integral to human society, they foster a unique culture and a new cyber world with its own behavioural patterns and norms, leading to the development of cyber culture. Culture, society, and development are deeply intertwined. Development is a complex societal process that encompasses socio-economic and cultural growth, technological progress, and social change. Culture, defined as the shared beliefs, patterns, and practices of a group or society, shapes this process by influencing societal values and norms. It can either promote or

[1] How to cite the article: Tiwari S., Verma H.; (March, 2025); Addressing Youth Cyber Offenses: The Impact of Cyber-Security in Lucknow, India; *International Journal of Research in Social Sciences and Humanities*; Vol 15, Issue 1; 48-59, DOI: http://doi.org/10.37648/ijrssh.v15i01.006

hinder development, depending on whether it encourages innovation and change or upholds irrational traditions. Society provides the context in which development occurs and culture is formed. Understanding the intricate relationship between development, culture, and society is crucial for creating policies that foster sustainable growth and social well-being in a fair and just manner. The relationship between culture, technology, and crime is intricate and reciprocal.

Culture influences the use and perception of technology, which in turn can affect crime. Technological advancements can create new opportunities for crime but also offer innovative solutions for crime prevention. Cyber culture can be understood as, "a collection of cultures and cultural products enabled by the Internet, along with the narratives about these cultures and products." (Silver, 2004) According to Merriam-Webster, "cyber culture encompasses shared attitudes, practices, and goals related to computers and the Internet. It also involves the creation of art, literature, music, and other creative works using the Internet and multimedia tools." Cyber-culture is linked to the electronic generation of new ideas, behaviours, and technological innovations. It includes the social expectations, netiquettes, practices, behaviours, and languages of people active on the World Wide Web or any digital platform powered by the Internet. Donna J. Haraway in early 1990s viewed "cyber culture as a blend of nature and culture through the concept of the cyborg, a fusion of machine and living organism. She argues that cyber culture challenges traditional views of feminism, identity, and politics by blurring the lines between human and animal, natural and artificial, and physical and non-physical." (Haraway, 2010) Howard Rheingold argued that, "cyber culture as the emerging global culture shaped by the convergence of computing, telecommunications, and media technologies."(Rheingold, 2000)

Cyber-security is the practice of protecting systems, networks, and data from digital attacks. It can also be understood as "the collection and concerting of resources including personnel and infrastructure, structures, and processes to protect networks and cyber- enabled computer systems from events that compromise the integrity and interfere with property rights, resulting in some extent of loss."(Schiliro, 2022).As our reliance on technology grows, so does the importance of safeguarding sensitive information from cyber threats. Key components of cyber-security include network security, which protects the integrity of networks and data; information security, which ensures data confidentiality and integrity; and application security, which focuses on keeping software and devices free of threats. Cyber-security strategies involve a mix of technologies, processes, and practices designed to defend against unauthorized access, data breaches, and other cyber threats. These strategies include the use of firewalls, encryption, multi-factor authentication, and regular security audits. Additionally, educating users about safe online practices is crucial in preventing cyber incidents. Ethical considerations are paramount in cyber-security. Professionals must respect intellectual property rights and avoid plagiarism by properly attributing sources and obtaining necessary permissions. This includes not copying code, research, or documentation without authorization. Organizations should implement policies and training programs to emphasize the importance of ethical behaviour and compliance with copyright laws. By doing so, they can maintain the integrity of their cyber-security practices and avoid legal issues. In current cyber-world, strong cyber- security practices are essential, particularly in addressing cyber offenses and misconduct among young people. As youth become more involved with internet technology, they are at risk of both falling victim to and committing cyber-crimes. Actions such as hacking, phishing, cyber-pornography, cyber-bullying, and identity theft, which are certain prominent types of cyber-delinquency, art serious dangers to our children and youth.

Implementing strong cyber-security practices is essential to protect sensitive information and maintain the integrity of internet systems. Educating youth and children about the ethical use of technology and the consequences of cyber offenses is a crucial step in prevention. Schools and parents must collaborate to provide comprehensive cybersecurity education, emphasizing the importance of responsible online behaviour.

Privacy and encryption of data are not only serious concern for physical world but are more serious and important for cyber-world. Here, in cyber world many times victims even don't know about being victimized and also it is also difficulty to identify and track cyber-criminals. In this realm of cyber culture, behavioural patterns get differs in comparison to physical world, as here many times children becomes victims as well as culprits too because of multiple reasons like lack of knowledge and awareness about cyber-security measures, fake ostentatious advertisements and profiles which lures the children and youth. When children (who has not attended the legal age of 18 years) commits a cyber-offence known as juvenile cyber delinquent. Further, this article will go in-depth exploration of all phenomenon related with Juvenile cyber-delinquency and cyber-security measures through field visit of Boys' Observation Home Lucknow and data sourced from National Crime Records Bureau of India (NCRB-India)

METHODOLOGY AND RESEARCH DESIGN

Methodology and Research Design are fundamental elements of any research. They provide the blueprint for the pattern and pathways of research and ensures us that the study is reliable, valid, and can be justified. Methodology means the systematic approach used by researcher to conduct research. It includes the theoretical analysis of the methods and principles associated with a branch of knowledge to explain "what" is happening. It also involves selecting the appropriate methods for data collection and analysis. This work on "Addressing Youth Cyber Offenses: The Impact of Cyber-Security in Lucknow, India" employs a comprehensive qualitative approach that is the exploratory in nature with the collection and analysis of both qualitative and quantitative data. The study proceeded on her way with a comprehensive review of existing literature on cyber-culture, cyber-security, juvenile delinquency and aspects of information and communication technology in the era of internet.

A review of the literature and theoretical framework oriented this study towards a multi-faceted approach that integrates both qualitative and quantitative analysis of the data. This exploratory work aims to figure out the intricate dynamics among internet technology, cyber-culture, and juvenile delinquency, particularly within the multidimensional context of the cyber-security in India (particularly in context of Lucknow). Sampling is a fundamental and most important step in social research in bringing the exact picture of research problem. In this core context of our study which allows us to focus on a specific section based on our research query of interest, in this context, juvenile delinquents in Lucknow constitutes as our primary respondents in our sampling paradigm for the same purposive sampling have been selected. Purposive sampling, which is also known as selective sampling, is a non-probability sampling technique used in social research. It involves the intentional selection of individuals or groups that can match our specific criteria relevant to our research question. This method relies on the need for respondent's coherence with the research question directly. As specific to our research query, by the application of purposive sampling data sourced from Boys' Observation Home, Lucknow. Further, secondary data for has been sourced from National Crime Records Bureau (NCRB) of India. The limitation of study is that the primary respondents that is the juveniles who are apprehended at observation home in Lucknow were boys only. The primary data solely based on responses from juveniles, superintendent and counsellors of observation home.

THEORETICAL ORIENTATIONS

Theoretical frameworks, is an essential part of research it provides the argument building philosophical stances or perspectives that provide a logical basis for the research process. They guide the researcher in understanding how to approach their study, what factors to consider, and how to interpret their findings in coherence with data and research question. This research not only binds on technical aspects because when it comes to data breach, piracy, morphism, cyber pornography and cyber-sextortion, we cannot neglect the other perspectives as we know, culture consist of both material and non-material aspects of society. It also demands to look from other aspects of like socio-economic, psychological and cultural perspectives. Cyber-security is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes. Implementing effective cyber-security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. Meeuwisse in "Cyber-security for Beginners" argued that "cyber-security is crucial for anyone using digital devices, the concern of cyber threats, basic security principles, and practical steps must be strictly ensure the internet service providers and law-enforcement agencies to protect personal and organizational data." (Meeuwisse, 2017).Further, Ozkaya in his, "Cyber-security: The Beginner's Guide" says that "cyber threats come in various forms, including malware, phishing, ransomware, and denial-of-service (DoS) attacks. Malware, short for malicious software, includes viruses, worms, and trojans that can damage or disable computers.

Phishing involves tricking individuals into providing sensitive information, such as passwords or credit card numbers, by pretending to be a trustworthy entity."(Ozkaya, 2019)

The importance of cyber-security cannot be neglected in today's digital age. With the increasing reliance on internet technology for personal and professional activities, the potential impact of cyberattacks is significant. Data breaches can lead to financial losses, reputational damage, and legal consequences. For businesses, a robust cyber-security strategy is essential to protect intellectual property, customer data, and operational integrity. Brotherston et al. highlights the critical role of "cyber-security in safeguarding assets and ensuring business continuity. Their work provides practical advice on building a strong cyber security posture, including risk assessment, incident response, and security awareness trainings". (Brotherston, 2024). Knerler argues that implementing cybersecurity is the best practices to mitigating risks of cyber-threat and phishing. Some fundamental practices include using strong, unique passwords, enabling multi-factor authentication, regularly

updating software, and backing up data. Additionally, educating people about cybersecurity risks and how to recognize potential threats is crucial. The book covers various strategies, such as threat intelligence, incident management, and continuous monitoring, to enhance an organization's overall security posture.(Knerler et al. 2023).The future of cyber-security is shaped by emerging technologies and evolving threats. As artificial intelligence (AI) and machine learning (ML) become more integrated into cyber-security solutions, they offer new ways to detect and respond to threats. However, these technologies also present new challenges, as cybercriminals can use AI and ML to develop more sophisticated attacks.

The future of cyber-security and the skills needed to navigate this dynamic landscape. The book emphasizes the importance of continuous learning, collaboration, and adaptability in staying ahead of cyber threats. (Fitzgerald, 2018).However, many times due to lack of awareness and knowledge about cyber-security, children and youth becomes prey to cyber-criminals or many times they move towards path of deviance. In this line, when we are discussing about cyber-security it important to discuss the socio-cultural and psychological factors which makes someone to do such illegitimate acts.

In this line, Manuel Castells, in his prominent work, "The Rise of the Network Society" explored the socio-economic and technical dynamics of the informative internet age. He called the modern society an 'informative society'. He point outs that "we are transitioning from the industrial society into the information society. This shift is driven by the advent of new information technologies, particularly those for communication and biological technologies." While the society is capitalistic, the technological means by which it operates has shifted from the notion energy and money to information and data collection. The society which is now interconnected, he refers it as network society, here in this, information is central to determining economic productivity. According to him, power and authority now rests in networks and information. Some networks, such as that of financial capital like trade and commerce organizations, are global in scale. (Castells, 1996)

The concept of "netiquettes" emerged, shaping a unique internet culture and influencing e-business and the broader economy. The geo-political implications of the internet are central to Castells' analysis.

While the internet has the power to liberate, it can also marginalize those without access or technological literacy and also harm to sections like children or those who are not enough mature to identify the wrong digital data. The digital divide, viewed from a global perspective, presents challenges to the network society. He analysed how the internet has created new opportunities for criminal activities and facilitated the proliferation of cybercrimes. He argued that the current emerging borderless world and decentralized nature of cyberspace has challenged conventional notions of jurisdiction and law enforcement, making it increasingly difficult to regulate and control criminal behaviour especially if committed via online devices/platform. Castells' analysis of cybercrime is the notion of 'anonymity and pseudonymity' afforded by the internet. He discusses how individuals can engage in illegal activities such as hacking, identity theft, and online fraud while concealing their true identities behind digital avatars/profiles or anonymous online identities. This anonymity complicates efforts to identify and prosecute cyber-criminals, as conventional methods of investigation and surveillance are not efficient in cyberspace. Furthermore, he also examined the role of social networks and online communities in facilitating these cybercrimes. Castells highlighted the need for greater transparency, strong and firm cyber-security measures and accountability in data collection practices to protect individuals' privacy and lessen the risk of cybercrimes. (Castells, 1998)

In era of globalization, we can‘t deny the interplay of culture, capitalism and, technology, in this line George Ritzer and Paul Dean in their argued the impact of globalization on culture, emphasizing the increasing interconnectivity and intermixing of thoughts and perceptions that often result in ‘hybrid’ cultures. They tried explored how the diffusion of commodities and ideas reflects a standardization of cultural expressions globally. However, it also acknowledges that while homogenizing influences exist, they are far from creating a single world culture. They also argued the negative global flows and processes, which can be interpreted as modern crimes in the context of globalization. They highlighted, how globalization driven by technological advancements and global corporations, creates new winners and losers by any of the means either ethical or non-ethical by the use of information and data. They also said that there is increase in global crimes such as trafficking, cybercrimes, financial crimes, terrorism, and green crimes (crime that damages/harms environment) which many times facilitated by internet media. They also acknowledged the role of the internet in driving the phenomenon of globalization. They said that, high-tech global flows and structures, including the rise of dark web, block-chain technology and crypto-currencies are leading illicit and un-lawful activities through internet which is creating a negative impact on physical world. The internet has facilitated the diffusion of ideas and commodities, contributing to the standardization of cultural expressions. It has also made it easier for illicit actors to operate, thereby increasing the prevalence of modern crimes. With the fusion of world boundaries and inter-connectedness of ideas, the society is networked and all are inter-related and

inter-connected through internet either directly or indirectly. (Ritzer & Dean, 2015)Merton's strain theory is a socio-criminological framework which tried to explain how societal pressures can lead individuals to engage in non-conforming behaviour. This theory illustrates disconnect that can occur between cultural goals and the means available to achieve them, often resulting in a strain that pushes people toward deviance. The theory posits that societal structures, such as the cultural emphasis on wealth and fame attainment like as in the idea of 'American Dream', can pressurize individuals into committing crimes. This is particularly true for lower-class individuals who lacks legitimate means to get ahead, leading to deviant behaviour as they pursue success through crime. Merton's Strain Theory evolved from studies of 'anomie' or normlessness; a concept first introduced by French sociologist Emile Durkheim.

INTERCONNECTION OF CYBER DELINQUENCY AND CYBER-SECURITY

When the crime interacts with internet technology, it nurtures and paves the path for cyber-crimes. In the digital expanse, Cyber Culture not only shapes societal interactions but also provides a breeding ground for cyber-crimes via. Digital technology and internet. When internet/internet devices are used as a tool/medium for committing crime, then may be called as cyber-crime. Cyber-crimes, ranging from hacking to online fraud, leverage the evolving technological landscape. Deviations from conventional norms within Cyber-Culture often leads to both traditional and cyber-specific criminal behaviours. The rapid proliferation of information and communication technology introduces new challenges, requiring a recalibration of legal frameworks and sociological perspectives. The term 'Cyber-crime', in general, was first proposed by 'Barry Collin' researcher at the 'Institute for Security and Intelligence in California', in the mid-1970s. He used this to describe criminal activities conducted through computer networks. Later, computer scientists, 'Gary Sussman and Michael Heuston', popularized the term in their research talks on computer-related crimes. Cyber-crime cannot be defined from a linear definition/assertion, it is best defined as collection of acts or conducts which are regarded as illegal, unethical and are conducted through Internet or any of the digital device or digital tool/technology.

Cyber-crime, as per Merriam Webster, refers to, "illegal activities like fraud, theft, or the distribution of pornography, carried out using a computer to unlawfully access, transmit, or manipulate data. While the term technically refers to the disruption and violation of internet network systems, it encompasses a wide range of criminal activities." A broad definition of cybercrime could be "unlawful acts where the computer is either a tool, target, or both" (Chawki et al.2015). The terms "cyber-crimes" and "computer crimes" are often used interchangeably, but "computer crimes" specifically refers to offenses committed not only on the computer systems but also in relation to or with the help of internet systems. Further, Moitra says that, "Cyber-crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc."(Moitra, 2005)

The term "juvenile" originates from the Latin word "juvenis," meaning young, while "delinquency" comes from "delinquentia," referring to fault or crime. "A juvenile is a child who has not reached an age where they can be held accountable for criminal acts as an adult. Although "juvenile" and "minor" are often used interchangeably in everyday language, they have distinct legal meanings." "Juvenile" pertains to a young offender, whereas the "minor" relates to a person's legal capacity. Therefore, a juvenile is a child (under 18 years old, as per the JJ Act 2015, Govt. of India) accused of committing acts that violate the law. The term "juvenile" refers to a 'young individual who has committed acts or omissions that violate the law,' while "minor" pertains to legal capacity or majority status. In India, "a juvenile is defined as anyone under the 18 years of age, according to the Indian Juvenile Justice (JJ) Act of 2015." However, for heinous offenses, which are crimes punishable by a minimum of seven years of imprisonment, individuals who are 16 years or older may not be considered juveniles, depending on an assessment of their mental, social, and physical capacity, here the legal system plays a significant role by defining the nature and meaning of offences. (Kohli & Mittal, 2015) D. R. Cressey defined "juvenile delinquency as minors engaging in illegal activities before reaching the statutory age limit." (Cressey, 1979). T. Hirschi described it as "the violation of legal codes by minors." (Hirschi, 1969). J. J. Macionis and K. Plummer noted that "juvenile delinquency encompasses antisocial acts by children and youth that are subject to legal action." (Macionis &Plummer, 2005). In this line, A. Giddens and P. W. Sutton viewed it as "socially unacceptable behaviour by young people that may involve breaking the law." (Giddens & Sutton, 2021). Delinquency is a global serious social issue present in all societies. When minors uses the internet or internet-enabled devices to commit unlawful acts, it is termed as cyber- delinquency. Employing advanced cyber-security tools such as firewalls, encryption, and intrusion detection systems is vital for defending against unauthorized access and cyber threats. Law enforcement agencies play a key role in overseeing and addressing cyber-delinquency, ensuring that offenders are held accountable. By fostering a culture of cyber-security awareness and implementing stringent protective measures, we can significantly reduce cyber offenses among youth and children. This strategy not only protects individuals but also contributes to a safer and more secure digital

environment for everyone.

In our visits to Juvenile Boys Observation home which is also known as "Rajkiya Bal Samprekshan Grah". During our visits at Boy‘s Observation home, there were 96 juveniles were present. Among 96 juveniles majority of juveniles that is 62.5% (60) of juvenile boys were of 16 years of age. Among them, most of them that is 74%(71) of boys belongs to nuclear family that is living with their parents and siblings only. Out of 96 juveniles who were apprehended there 59.3% (57) juveniles were belonging to schedule castes, while 13(13.5%) were from other backward castes, 11.5% (11) belonging to general category and 15.6% (15) from minority (Muslim). There were, 16.7% (16) juveniles were apprehended for petty offences, while 38.5% (37) juveniles were apprehended for serious offences and 44.8% (43) for heinous offences. Among 96 juveniles, 94(97.9%) were aware about smartphone and internet. All juveniles were aware and able to use smartphones, also using social media platforms mainly, Instagram, YouTube, Facebook, snapchat, WhatsApp and other video and reel making applications, here 25(26%) boy juveniles are highly active on Instagram, 24(while 25%) juveniles mainly prefers YouTube and 17(17.7%) are active and using all above mentioned applications. Among 96 juveniles, 59.4% (57) boys were having their own smartphones prior to apprehension while, 40.6% (39) juveniles were using their parent‘s/siblings' smartphones. Out of 96 juveniles, 82.3% (79) juveniles had seen porn movies/videos while only 17.7% (17) boys haven‘t seen the porn movies. Despite that it is age of learning-education and positive socialization, in teenage they came in the grip of pornography and adult content. With only exception to 2 boys, rests, 97.9% (94) of juveniles were active on social media applications.

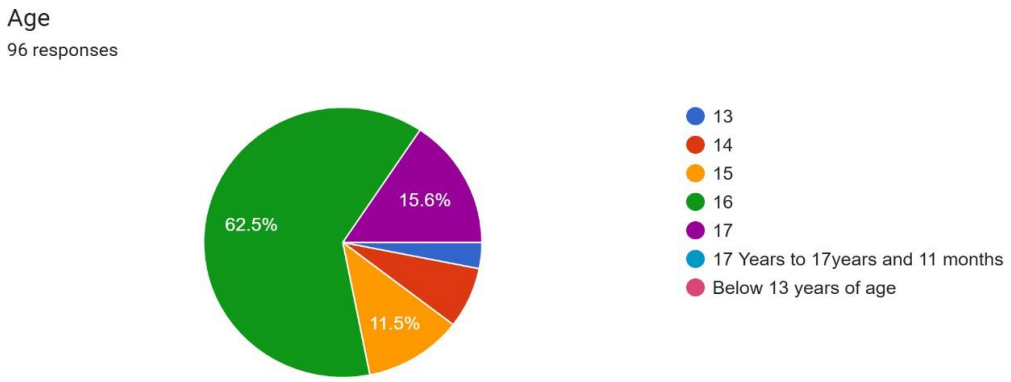

Fig. 1 The above pie-chart shows juvenile of different age groups apprehended at Boy’s Observation Home

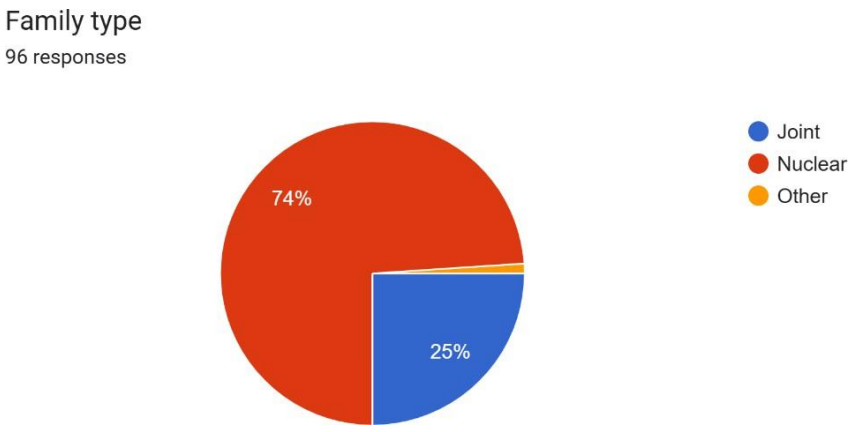

Fig. 2 The above pie chart shows family type of juveniles apprehended at Boy’s Observation Home

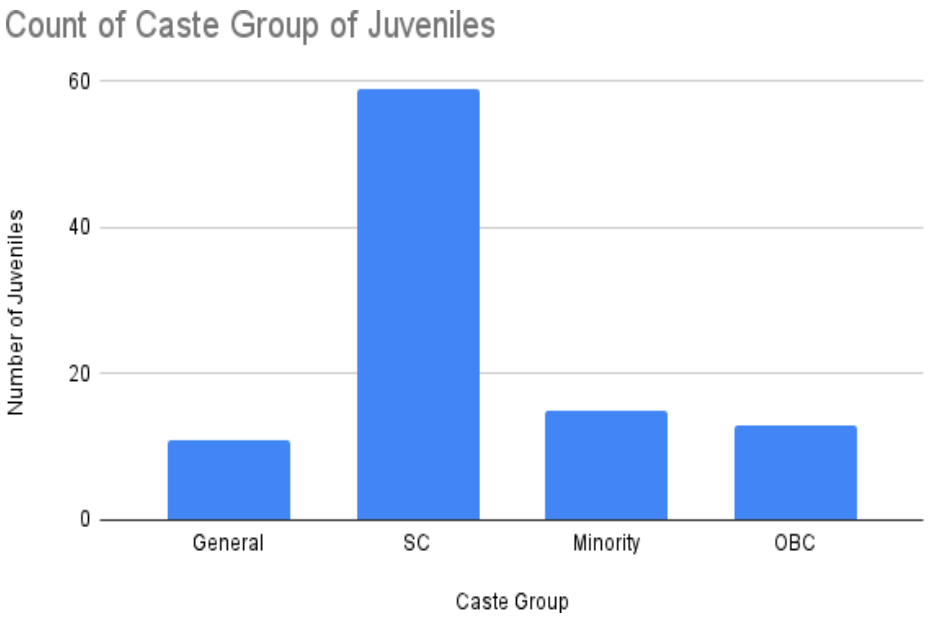

Fig.3 The above graph shows caste dynamics of juveniles apprehended at Boy's Observation Home

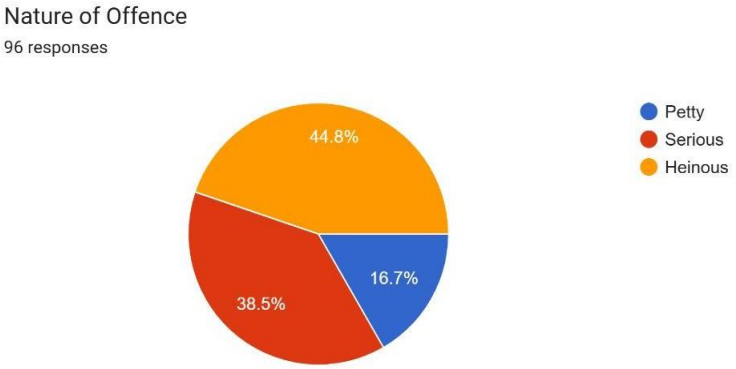

Fig.4 The above pie chart showed the nature of offence committed by juveniles apprehended at Boy's Observation Home

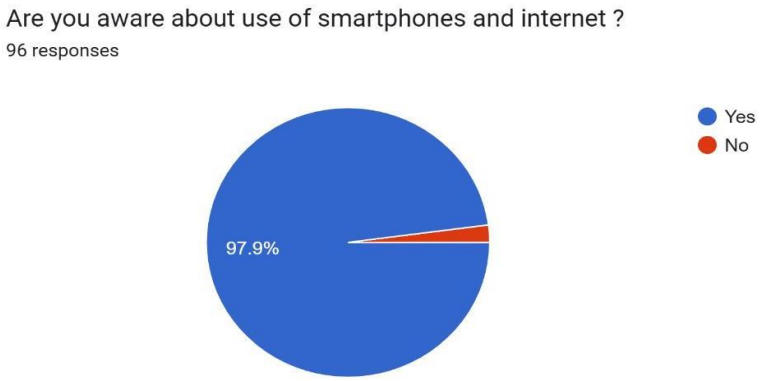

Fig. 5 The above pie chart shows the awareness about use of smartphones and internet among juveniles apprehended at Boy's Observation Home

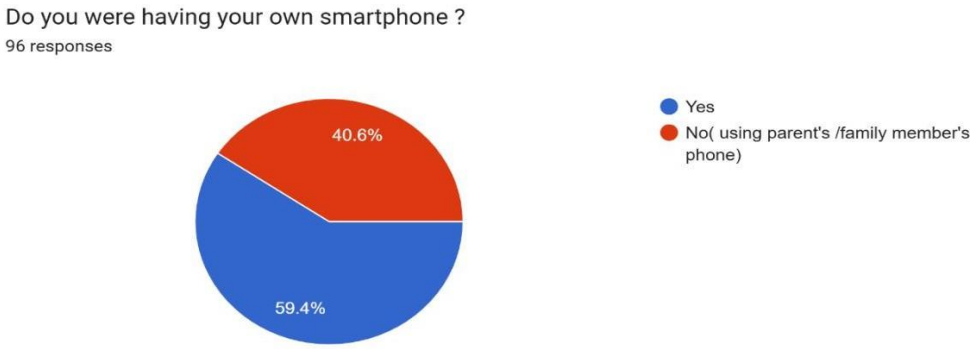

Fig. 6 The above pie chart shows count of juveniles having their own smartphones

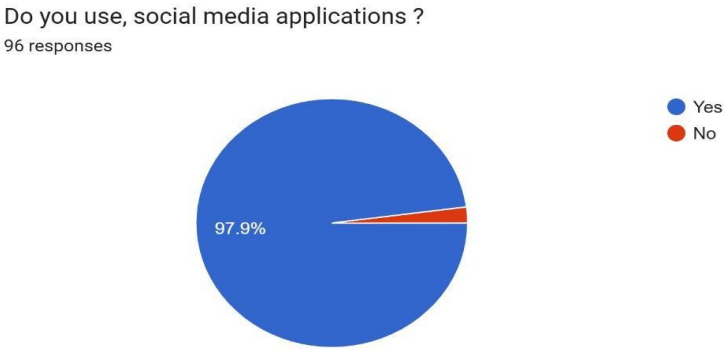

Fig.7 The above pie-chart shows the count of juveniles who were active on social media applications

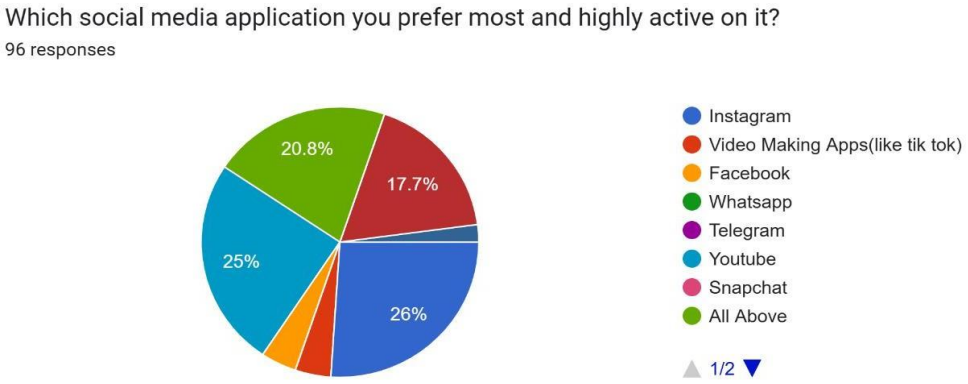

Fig.8 The above pie chart depicts various social media platforms being used by among juveniles apprehended at Boy's Observation Home

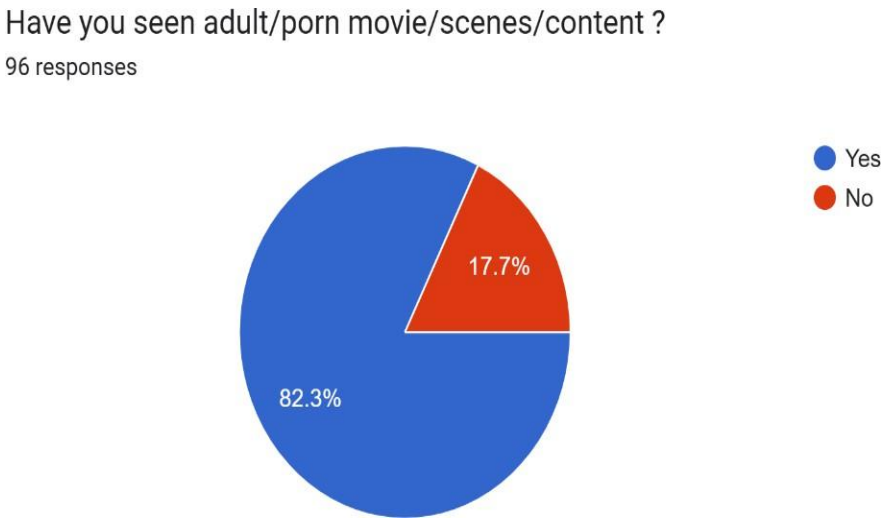

Fig. 9 The above pie chart shows number count of juveniles who had seen porn/adult content on internet

Apart, this the juveniles who were apprehended under serious and heinous offences, were charged for IPC 376 and NDPS act used smartphones in committing the offences. In this line the online gaming is also responsible for making children both victim as well as culprit of cyber-offences. Earlier due to increase adverse effect of internet gaming government of India has to ban “Blue Whale Game Suicide Challenge" and "PUBG" games which made many children victims as well as culprit of cyber- gam extortion are also the reflections that how due to lack of cyber-security and inefficient monitoring of internet world is destroying the tender lives of our children. As, data from NCRB shared in Rajya Sabha on dated 24-11-2024 shows a significant high rise in cyber-crimes in India.

ANNEXURE-I

RS USQ. NO. 234 FOR 27.11.2024

STATE/UT-WISE CASES REGISTERED UNDER CYBER CRIMES DURING 2018-2022

SL	State/UT	2018	2019	2020	2021	2022
1	Andhra Pradesh	1207	1886	1899	1875	2341
2	Arunachal Pradesh	7	8	30	47	14
3	Assam	2022	2231	3530	4846	1733
4	Bihar	374	1050	1512	1413	1621
5	Chhattisgarh	139	175	297	352	439
6	Goa	29	15	40	36	90
7	Gujarat	702	784	1283	1536	1417
8	Haryana	418	564	656	622	681
9	Himachal Pradesh	69	76	98	70	77
10	Jharkhand	930	1095	1204	953	967
11	Karnataka	5839	12020	10741	8136	12556
12	Kerala	340	307	426	626	773
13	Madhya Pradesh	740	602	699	589	826
14	Maharashtra	3511	4967	5496	5562	8249
15	Manipur	29	4	79	67	18
16	Meghalaya	74	89	142	107	75
17	Mizoram	6	8	13	30	1
18	Nagaland	2	2	8	8	4
19	Odisha	843	1485	1931	2037	1983
20	Punjab	239	243	378	551	697
21	Rajasthan	1104	1762	1354	1504	1833
22	Sikkim	1	2	0	0	26
23	Tamil Nadu	295	385	782	1076	2082
24	Telangana	1205	2691	5024	10303	15297
25	Tripura	20	20	34	24	30
26	Uttar Pradesh	6280	11416	11097	8829	10117
27	Uttarakhand	171	100	243	718	559
28	West Bengal	335	524	712	513	401
	TOTAL STATE(S)	**26931**	**44511**	**49708**	**52430**	**64907**
29	A&N Islands	7	2	5	8	28
30	Chandigarh	30	23	17	15	27
31	D&N Haveli and Daman & Diu+		3	3	5	5
32	Delhi	189	115	168	356	685
33	Jammu & Kashmir *	73	73	120	154	173
34	Ladakh	-	-	1	5	3
35	Lakshadweep	4	4	3	1	1
36	Puducherry	14	4	10	0	64
	TOTAL UT(S)	**317**	**224**	**327**	**544**	**986**
	TOTAL (ALL INDIA)	**27248**	**44735**	**50035**	**52974**	**65893**

Source: Crime in India

Note : '+' Combined data of erstwhile D&N Haveli UT and Daman & Diu UT for 2018, 2019

*'Data of erstwhile Jammu & Kashmir State including Ladakh for 2018, 2019

******

Strong surveillance and strict internet security protocols must be there in order to curtail the cyber offences. Cyber-security is an urgent need of hour, as in nation like India, where internet is not only a source of communication, but also used for knowledge sharing, data transmission, data storage, entertainment and also a platform for generating income via multiple businesses. Since, Covid-19 human activities are changed significantly especially in education and corporate sectors. Nowadays smartphones and internet are becoming an integral part of school and university education, where many children are highly prone to be a victim as well as culprit of cyber offences.

CONCLUSION

The rapid development of cyber technology in India has resulted in significant progress, but it has also contributed to a rise in cyber-delinquency, presenting a distinct challenge to society. The easy access to the internet and digital devices has exposed children and youth to various cyber threats, often without a full understanding of the legal and ethical consequences of their actions. We can't deny that, now internet is shaping the lives of our children and youth and also sometimes impacting them in a negative manner by making them to commit offenses. Strong cyber-security measure is one of the prominent aspect but it also includes the surveillance of adult/illicit contents which are being produced and circulated on Internet. The anonymity and remoteness provided by the internet can embolden minors to engage in activities they would otherwise avoid in the physical world. Socio-economic factors also play a significant role, as children from disadvantaged backgrounds may turn to cyber-crimes for financial gain or due to peer pressure. Additionally, the lack of proper parental supervision and guidance can lead to increased vulnerability to online influences. The education system in India still facing challenges in adequately addressing cyber literacy and cyber-security awareness, leaving children ill-equipped to navigate the cyber world safely. The legal framework in India, while robust, faces challenges in effectively addressing juvenile cyber-delinquency. The Juvenile Justice (Care and Protection of Children) Act, 2015, provides a legal structure for dealing with juvenile offenders, but its implementation is often hindered by inadequate resources and lack of trained personnel. Moreover, the rapid evolution of technology outpaces the legal system's ability to keep up with new forms of cyber- crimes. To address these issues, several suggestive measures can be implemented. Firstly, integrating comprehensive digital literacy and cyber-security education into the school curriculum is essential.

These programs should focus on teaching children about the ethical use of technology, the risks associated with cyber activities, and the legal consequences of cyber-crimes. Educating parents and teachers about cyber-security can also help in creating a safer online environment for children.

Secondly, encouraging parents to actively monitor their children's online activities can significantly reduce the risk of cyber-delinquency. Tools and software that allow parents to set restrictions on internet usage and monitor online behaviour can be effective in preventing minors from engaging in cyber-crimes. Thirdly, conducting community-based awareness campaigns can help in spreading knowledge about the dangers of cyber-delinquency and the importance of cyber-security. These campaigns can involve workshops, seminars, and interactive sessions with cyber-security experts to educate both children and adults. Fourthly, updating and strengthening the legal frameworks to keep pace with technological advancements is crucial. This includes training law enforcement agencies and judicial personnel in handling cyber-crimes involving juveniles. Establishing specialized cyber-crime units within the police force can also enhance the effectiveness of law enforcement. Lastly, providing psychological support and rehabilitation programs for juvenile offenders can help in their reintegration into society. These programs should focus on addressing the underlying issues that lead to cyber- delinquency, such as peer pressure, family problems, and socioeconomic challenges. However, we can't neglect the role of internet service providers and telecom- companies, as from their end there should be strict restriction and control over dark webs, piracy, cyber pornography, cyber bullying and other cyber- illicit activities. In conclusion, preventing juvenile cyber-delinquency in India requires a multifaceted approach that combines education, parental involvement, community awareness, legal reforms, and psychological support. By addressing the sociological factors contributing to cyber-delinquency and implementing effective cyber-security measures, India can create a safer digital environment for its children and youth.

REFERENCES

Brotherston, L., Berlin, A., & Reyor III, W. F. (2024). *Defensive security handbook*. O'Reilly Media, Inc.

Castells, M. (1996). The Rise of the Network Society. John Wiley & Sons.

Castells, M. (1998). End of Millennium (Vol. 10). New York, NY: John Wiley & Sons. New York. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). Cybercrime, digital forensics and jurisdiction (Vol. 593). Springer

Cressey, D. R. (1979). Fifty Years of Criminology: From Sociological Theory to Political Control. Pacific Sociological Review, 22(4), 457-480

Fitzgerald, T. (2018). *CISO COMPASS: navigating cybersecurity leadership challenges with insights from pioneers*. Auerbach Publications

Giddens, A. (2003). Runaway world: How globalization is reshaping our lives. Taylor & Francis Giddens, A., & Sutton, P. W. (2021). Essential Concepts in Sociology. (p.687) John Wiley & Sons. Haraway, D. (2010). A Cyborg Manifesto [1985]. Cultural theory: An Anthology, 454

Hirschi, T. (1969). Causes of Delinquency. Routledge

Knerler, K., Parker, I., & Zimmerman, C. (2023). *11 Strategies of a World-Class Cybersecurity Operations Center*. MITRE

Kohli, R. & Mittal, K. (2015). Juvenile Delinquency in India

Macionis, J. J., & Plummer, K. (2005). Sociology: A global introduction. Pearson Education Meeuwisse, R. (2017). *Cybersecurity for beginners*. Cyber Simplicity Ltd

Merton, R. K. (1968). Social Theory and Social Structure. Simon and Schuster

Moitra, S. D. (2005). Developing Policies for Cybercrime: Some empirical issues. Eur. J. Crime Crim.

L. & Crim. Just., 13, 435

Ozkaya, E. (2019). *Cybersecurity: the beginner's guide: a comprehensive guide to getting started in cybersecurity*. Packt Publishing Ltd

Rheingold, H. (2000). The virtual community, revised edition: Homesteading on the Electronic Frontier. MIT press

Ritzer, G., & Dean, P. (2015). Globalization: A Basic Text. New York, NY: John Wiley & Sons Schiliro, F. (2022). Towards a Contemporary Definition of Cybersecurity. *arXiv preprint arXiv:2302.02274*

Silver, D. (2004). Internet/cyberculture/digital culture/new media/fill-in-the-blank studies. New media & society, 6(1), 55-64