"Cybersecurity and Juvenile Cyber-Delinquency: Sociological Insights into Youth Crime Prevention in Lucknow"

First Author -**Dr. Saurabh Tiwari**
Assistant Professor, Department of Liberal Education
Era University, Lucknow Uttar Pradesh, India, 226003
E-mail-saurabh28s95@gmail.com

Corresponding Author –**Ms. Hershika Verma**
Faculty of Fine Arts, Department of Liberal Education
Era University, Lucknow Uttar Pradesh, India, 226003
Email-hershika.verma@gmail.com

Abstract

The rapid expansion of digital technologies has transformed social interaction, education, and leisure among youth, while simultaneously creating new vulnerabilities to cybercrime. This study, titled "Cybersecurity and Juvenile Cyber-Delinquency: Sociological Insights into Youth Crime Prevention in Lucknow", investigates the intersection of adolescent engagement with cyberspace and emerging patterns of delinquent behaviour in an urban Indian context. Drawing upon sociological theories of deviance, peer influence, cyber-culture and digital socialization, the research explores how structural factors such as family environment, educational institutions, peer networks, and socio-economic disparities shape juvenile involvement in cyber-delinquency. The study employs a mixed-methods approach, combining survey data from secondary school students in Lucknow with qualitative interviews of educators, law enforcement officials, and parents. Findings reveal that curiosity, peer pressure, and lack of digital literacy often drive youth toward activities such as hacking, online harassment, and identity misuse. Moreover, inadequate parental supervision and limited institutional awareness exacerbate risks. The paper highlights the dual role of cyberspace as both a site of empowerment and a domain of potential deviance. Preventive strategies are analysed through the lens of community policing, school-based digital literacy programs, and culturally sensitive awareness campaigns. The research underscores the importance of integrating sociological insights into cybersecurity frameworks, advocating for holistic interventions that combine technical safeguards with social education. By situating juvenile cyber-delinquency within the broader socio-cultural fabric of Lucknow, the study contributes to global debates on netiquettes, youth crime prevention in the digital age. Ultimately, it calls for collaborative efforts among families, schools, policymakers, and technology providers to foster responsible digital citizenship and mitigate the risks of juvenile cyber-offending.

Keywords- Cyber-Culture, Cyber-Crime, Cyber-security, Juvenile Delinquency, Netiquettes

Introduction

Human societies have continually evolved across historical epochs, and the contemporary era is marked by unprecedented transformations driven by the Internet, Artificial Intelligence, and rapidly expanding social media environments. These technological domains have reconfigured social practices, communication patterns, and risk landscapes at a global scale. This qualitative research, drawing upon both primary and secondary sources, investigates the multidimensional contours of cyber society with specific reference to juvenile experiences in the Lucknow region of Uttar Pradesh. It examines critical themes such as cybercrimes, cybersecurity vulnerabilities, cyber-cultural shifts, and the rising prevalence of internet addiction among children and adolescents.Within today's highly interconnected network society, Information and Communication Technology (ICT) undergoes continuous evolution, simultaneously shaping and being shaped by cultural processes. ICT serves as a central instrument for processing and disseminating information, thereby restructuring contemporary social institutions and reinforcing the emergence of digitally mediated social networks (Castells, 1996). In

academic and policy discourse, Information Technology, frequently used interchangeably with ICT-constitutes the foundational infrastructure of modern socio-technical systems and increasingly permeates all spheres of daily life (Giddens, 2003). When ICT becomes embedded within internet-driven environments, it manifests as the domain commonly conceptualized as "cyber," encompassing the dynamic interactions between technologies, society, and emerging juvenile cyber-delinquent behaviours. The term 'Cyber' originates from 'Cybernetics,' which refers to the science of communication and control between machines and humans. Norbert Wiener first used 'Cyber' as a prefix in 'Cybernetics' in 1948. As, ICT and internet are nowadays an integral part of human society, it is creating its own sort of culture and a new cyber world which consists of its own behavioural patterns and norms leading to give rise a new phenomenon of cyber culture. Culture, society and development are deeply interconnected.

Development constitutes a multidimensional societal process that integrates economic progress, technological innovation, socio-cultural transformation, and shifts in collective behavioural patterns. Culture-understood as the shared beliefs, values, norms, and practices of a social group-plays a pivotal role in shaping developmental trajectories. It may either catalyse progress by fostering creativity, adaptability, and openness to innovation, or impede it by reinforcing rigid, outdated, or irrational traditions. Society, as the broader structural and relational context in which individuals interact, provides the foundational environment within which both development and culture evolve. A nuanced understanding of the interdependence between development, culture, and society is therefore essential for designing equitable and sustainable policy frameworks that enhance social well-being and resilience. Within the contemporary digital era, the intersection of culture, technology, and crime exhibits a complex and mutually constitutive relationship. Cultural orientations influence how technological tools are adopted, perceived, and utilised, while technological advancements continually reshape social practices and create new domains of vulnerability. As digital technologies proliferate, they generate unprecedented opportunities not only for socio-economic advancement but also for emergent forms of deviance, including cyber-crime and juvenile cyber-delinquency. Conversely, the same technologies provide innovative mechanisms for surveillance, regulation, and crime prevention.
Cyber-culture, as articulated by Silver (2004), encompasses the diverse cultures, practices, and symbolic products facilitated by the Internet, along with the narratives that frame them. Merriam-Webster similarly describes cyber-culture as the shared attitudes, behaviours, and creative outputs associated with digital environments. It embodies emerging norms, netiquettes, linguistic innovations, and behavioural patterns shaped through continuous interaction on networked platforms. Haraway's (2010) theorisation of the cyborg conceptualises cyber-culture as a hybrid space that destabilises conventional boundaries of identity and social behaviour, while Rheingold (2000) emphasises its global, technologically mediated character. Collectively, these perspectives illuminate the evolving digital context in which youth engage, learn, and, in some cases, become susceptible to cyber-delinquent behaviours.

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.

The safeguarding of privacy and the application of data encryption have become pressing imperatives, extending beyond the physical sphere into the far more complex terrain of the digital domain. Within cyberspace, victims frequently remain unaware of ongoing intrusions, while the identification and prosecution of cyber-offenders pose persistent challenges. The

behavioural dynamics of this virtual environment diverge significantly from those observed in the physical world. In particular, children often occupy dual positions as vulnerable victims and as potential offenders. Their involvement is shaped by insufficient knowledge of cyber-security practices, limited awareness of digital risks, and heightened susceptibility to manipulative tactics such as deceptive advertisements or fabricated online identities that deliberately target young users.

When individuals below the age of 18 engage in unlawful online activities, they are legally designated as juvenile cyber-delinquents. This study undertakes a sociological inquiry into juvenile cyber-delinquency, situating it within the broader discourse on cyber-security and youth crime prevention. Drawing upon field-based observations conducted at the Boys' Observation Home in Lucknow, alongside statistical data from the National Crime Records Bureau of India (NCRB), the research provides a comprehensive account of youth cyber-offending patterns and explores preventive strategies aimed at mitigating such risks.

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 study, entitled "Cybersecurity and Juvenile Cyber-Delinquency: Sociological Insights into Youth Crime Prevention in Lucknow," adopts a comprehensive exploratory design that integrates both qualitative and quantitative dimensions of inquiry. The research is grounded in an extensive review of existing scholarship on cyber-culture, cybersecurity, juvenile delinquency, and the broader sociological implications of information and communication technologies in the contemporary internet era.

The central objective of this inquiry is to unravel the complex interrelationships between internet technologies, evolving cyber-cultural practices, and juvenile delinquency, with particular emphasis on the sociological contours of cybersecurity in India, and more specifically, within the urban context of Lucknow.Sampling constitutes a pivotal stage in social research, as it provides the empirical foundation for representing the research problem with precision. In alignment with the study's objectives, purposive sampling was employed to identify and engage respondents most relevant to the research questions. Purposive sampling also referred to as selective sampling is a non-probability technique that involves the deliberate inclusion of individuals or groups whose characteristics directly correspond to the criteria established by the research framework.

Within this study, the primary respondents comprised juveniles housed at the Boys' Observation Home in Lucknow. This institution provided a critical site for data collection, as it enabled access to individuals apprehended for cyber-related delinquent activities. Supplementary insights were obtained from institutional stakeholders, including the superintendent and counsellors of the observation home, thereby enriching the primary dataset with professional and administrative perspectives.In addition to primary data, secondary data were systematically incorporated from the National Crime Records Bureau (NCRB) of India. This dual reliance on institutional records and field-based qualitative engagement facilitated a more nuanced understanding of juvenile cyber-delinquency within the broader national and regional criminological landscape.

A notable limitation of the study arises from the demographic composition of the primary respondents. The sample was restricted to male juveniles apprehended at the Boys' Observation Home in Lucknow, thereby excluding female perspectives and experiences. Consequently, the findings must be interpreted within the gendered boundaries of the sample, acknowledging the absence of female juvenile voices in the data set.

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. The theoretical orientation derived from this literature review informed a multi-layered methodological approach, enabling the integration of diverse data sources and analytical perspectives. 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. Berlin 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”. (Berlin, 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 illegitimateacts.

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. 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.

Cyber-Crime and Juvenile Delinquency

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, "Cybercrime 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 behavior 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.

In our visits to Juvenile Boys Observation home in May 2024, 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.

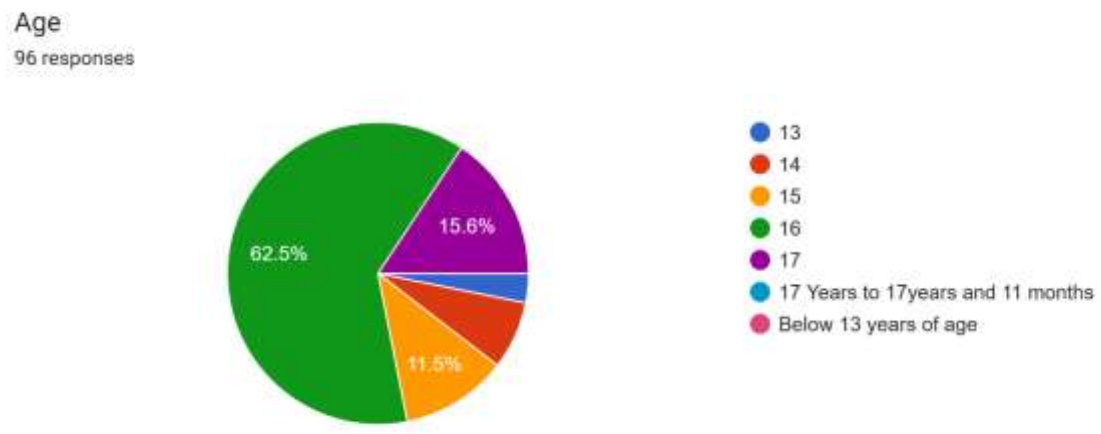

Fig. 1 The above pie-chart shows juvenile of different age groups apprehended at Boy’s Observation Home

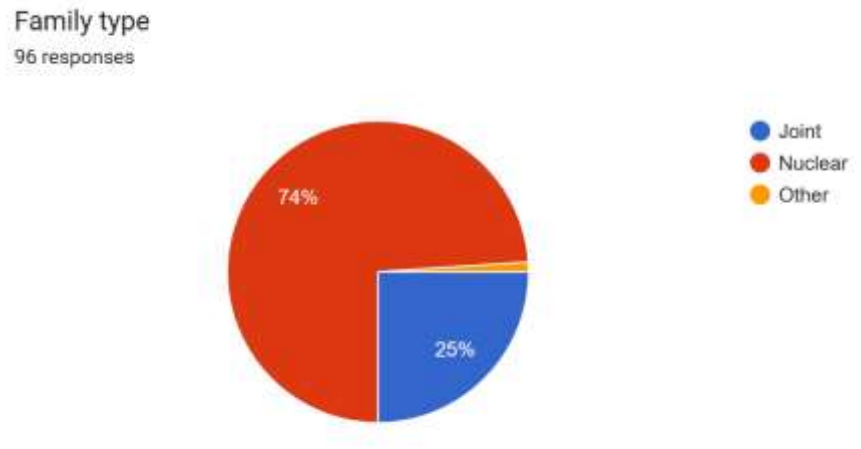

Fig. 2 The above pie chart shows family type of juveniles apprehended at Boy's Observation Home

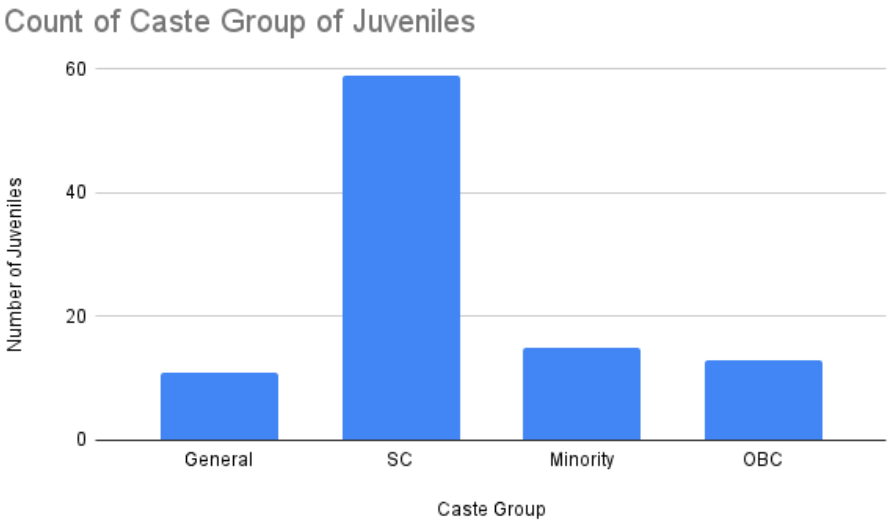

Fig.3 The above graph shows caste dynamics of juveniles apprehended at Boy's Observation Home

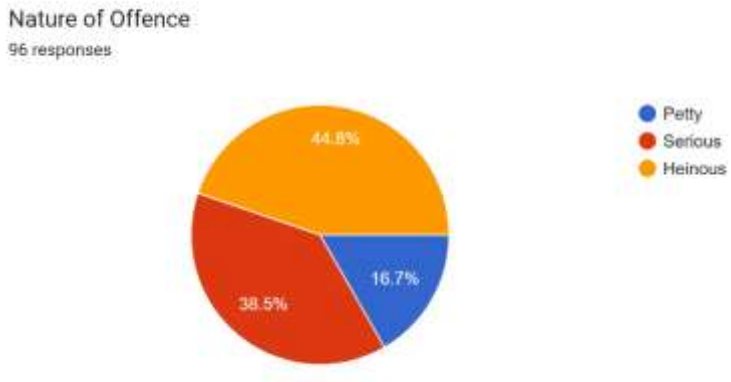

Fig.4 The above pie chartshowed the nature of offence committed by juveniles apprehended at Boy's Observation Home

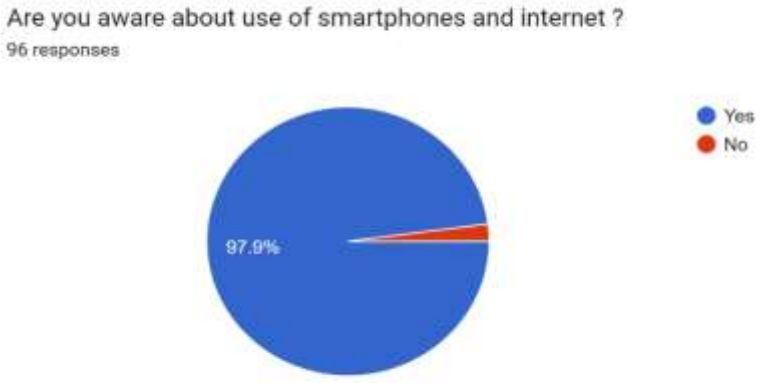

Fig. 5 The above pie chart shows the awareness about use of smartphones and internet among juveniles apprehended at Boy's Observation Home

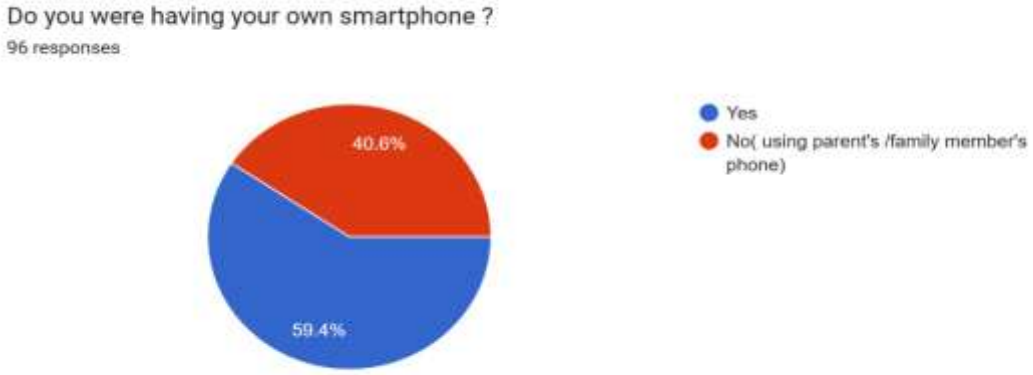

Fig. 6 The above pie chart shows count of juveniles having their own smartphones

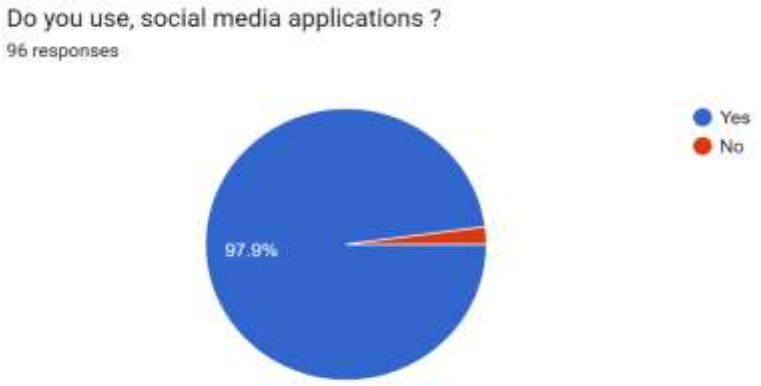

Fig.7 The above pie-chart shows the count of juveniles who were active on social media applications

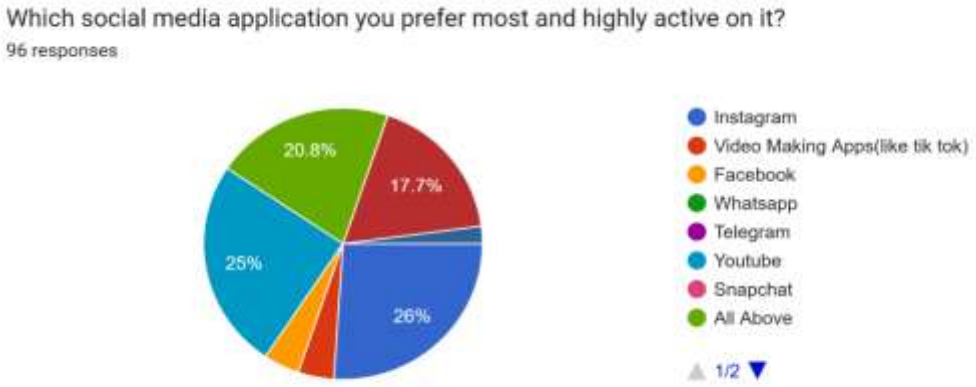

Fig.8 The above pie chart depicts various social media platforms being used by among juveniles apprehended at Boy's Observation Home

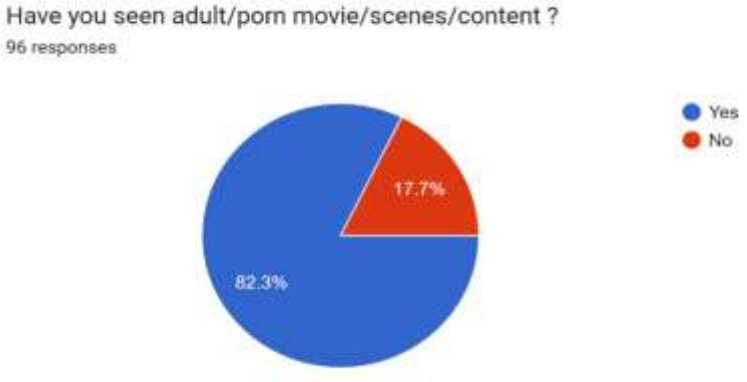

Fig. 9 The above pie chart shows number count of juveniles who had seen porn/adult content on internet

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-gamextortion 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

******

Proper 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 accelerated advancement of cyber technologies in India has yielded substantial developmental benefits; however, it has simultaneously precipitated a notable rise in juvenile cyber-delinquency, thereby posing a complex challenge to contemporary society. The widespread accessibility of digital devices and internet connectivity has rendered children and adolescents increasingly vulnerable to diverse cyber threats, often without adequate comprehension of the ethical and legal ramifications of their actions. Beyond the technical dimensions of data encryption, cyberspace also facilitates the circulation and surveillance of illicit digital content, including adult material, piracy, and cyber-pornography, which further complicates the landscape of juvenile exposure. The anonymity and spatial detachment afforded by online platforms embolden minors to engage in behaviours they might otherwise eschew in the physical world.Socio-economic determinants exert a significant influence on this phenomenon. Children from marginalized or economically disadvantaged backgrounds may be drawn into cyber-offending either as a means of financial gain or under the pressures of peer influence. The absence of consistent parental supervision and guidance exacerbates this vulnerability, leaving minors susceptible to manipulative online practices. Furthermore, systemic limitations within India's educational framework hinder the effective dissemination of cyber literacy and cyber-security awareness, thereby leaving young users ill-equipped to navigate the digital environment responsibly. Although India's legal architecture most notably the Juvenile Justice (Care and Protection of Children) Act, 2015 provides a structured mechanism for addressing juvenile offenses, its implementation remains constrained by inadequate resources, insufficiently trained personnel, and the rapid evolution of technological modalities that consistently outpace legislative adaptation. These challenges underscore the urgent need for multidimensional interventions.

Several measures are imperative to mitigate juvenile cyber-delinquency. First, the integration of comprehensive digital literacy and cyber-security modules into school curricula is essential. Such programs must emphasize ethical technology use, awareness of cyber risks, and the legal consequences of cyber-offending. Parallel efforts to educate parents and teachers on cyber-security practices can foster safer online environments for children. Second, parental monitoring of minors' digital activities, facilitated through technological tools and software restrictions, can significantly reduce delinquent behaviour. Third, community-based awareness initiatives—including workshops, seminars, and interactive engagements with cyber-security experts can disseminate knowledge across broader social strata. Fourth, legal frameworks must be continuously updated to align with technological advancements. This requires specialized training for law enforcement and judicial personnel, alongside the establishment of dedicated cyber-crime units to address juvenile cases effectively. Fifth, psychological support and rehabilitative programs are vital for reintegrating juvenile offenders into society, with interventions tailored to address underlying causes such as peer pressure, familial instability, and socio-economic hardship.

Equally critical is the role of internet service providers and telecommunications companies, which must enforce stringent controls against dark web activities, piracy, cyber-bullying, and other illicit digital practices.In conclusion, the prevention of juvenile cyber-delinquency in India necessitates a holistic and interdisciplinary approach that synthesizes education, parental involvement, community engagement, legal reform, and psychological rehabilitation. By addressing the sociological determinants of cyber-offending and implementing robust cyber-security measures, India can cultivate a safer and more resilient 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.
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., & 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. (2022). *Cybersecurity Leadership Demystified: A comprehensive guide to becoming a world-class modern cybersecurity leader and global CISO*. Packt Publishing Ltd. "Defensive Security

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. (2023). 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-