International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:06, Issue:04 "April 2021"

CHILDREN AND CYBER CRIMES

Mr. Naveen Kumar

Research Scholar, Himalayan Garhwal University, Uttarakhand

. DOI: 10.46609/IJSSER.2021.v06i04.014 URL: https://doi.org/10.46609/IJSSER.2021.v06i04.014

INTRODUCTION

Cybercrime, which has also been called “computer crime”, “digital crime”, “Internet crime”, and “high-tech crime”, is commonly understood to include a broad range of criminal activities that use computers, digital devices, and the Internet. Despite almost forty years of incidents, cybercrime still does not have a universally accepted definition in literature. Most authors classify cybercrimes based on the role of technology and criminal modus operandi. We have adapted a general framework and set of definitions to set the context for the current work and will consider and explain cybercrime as:

- Computer crimes (or “true” cybercrimes), such as hacking, denial of service, and production of malware, in which computer systems and networks are the target of criminal activity; and
- Computer related crime, in which computers serve as instruments of otherwise non-digital crime, such as forgery, fraud, sexual abuse of children, or copyright infringement.

Although other broad categories of cybercrime have been proposed (e.g. computer as a place of crime) as well as different classification approaches (e.g. cybercrime classification based on the level of technological sophistication), they have not been widely adopted.

The past decade has seen the rapid development and tremendous growth in the use of electronic, computer- based communication and information sharing via the “internet”. Defined as a “decentralized, self-maintaining series of links between computer networks”, the internet operates throughout much of the world. Never designed as a mass communication medium, the internet was originally developed by the US Defense Department in the 1950s as means of connecting the Department’s internal computers. The speed at which society has adopted this technology, penetration into work, school and family life, has been described by some as a “revolution”.

Use of the internet promises many benefits for society, by circumventing the effect of geographical distance and facilitating information sharing. It has been contended, for example, that the internet can revitalise a sense of community by facilitating meaningful communication between “grass root electronic communities”. The internet has also been found to have particular benefits for children and young people, who claim that its use facilitates social contacts, improves their writing and language skills and makes them’ better students’.

The development and spread of the internet, has increased the child’saccess to offensive and/or age-inappropriate material through the internetmedia’ thus providing increased opportunities for the solicitation of children and the committing of abusive acts by offenders outside the family. The internet also facilitates the activities of offenders byproviding a simple and quick means of communication which allows a person to remain anonymous and/or create false identities.

ONLINE RISKS AND THREATS ON CHILDREN IN INDIA

Digital technologies offer significant developmental and educational benefits for children. However, the growing access and use of internet by children also increases their exposure to potential risks of online abuse and exploitation. Cyber offences against children are spreading and diversifying as new methods are used to harass, abuse and exploit children. In many instances, children are also online offenders. Digital technologies provide new avenues to reinforce and spread existing social and cultural norms, as well as to mediate virtual social contexts and relationships.

Offline forms of crime and violence against children are finding new forms of expression in the online world and their effects on children are amplified. In many cases offline and online violence are interrelated, with online abuse also including offline components. Non-contact abuse can be harmful to children and can facilitate the transition to contact abuse. Being able to stay anonymous online and impersonate others may embolden people into offensive and criminal acts and lower the deterrent potential of laws.

Current forms of child online abuse and exploitation include:

- Cyberbullying: emotional harassment, defamation and social exposure, intimidation, social exclusion,
- Online sexual abuse: distribution of sexually explicit and violent content, sexual harassment,
- Online sexual exploitation: production, distribution and use of child sexual abuse material (CSAM) (child pornography), “sextortion”, “revenge pornography,”
- Cyber extremism: ideological indoctrination and recruitment, threats of extreme violence,
- Online commercial fraud: identity theft, phishing, hacking, financial fraud,

- Habit formation and online enticement to illegal behaviors: access to alcohol, cheating, plagiarism, gambling, drug trafficking, sexting and self-exposure,
- Grooming: preparing a child, significant adults and the environment for sexual abuse and exploitation or ideological manipulation.

There are no reliable figures on the extent, patterns and trends of child online abuse and exploitation in India, since no comprehensive surveys have been carried out on these issues. Several researchers have conducted surveys and polls among urban youth. These surveys focus mostly on young people’s use of the Internet and do not provide more in-depth data regarding online risks. National crime statistics include a category of cybercrime, but this focuses only on commercial fraud and online radicalization, with no component of child online abuse. Although there are several sources of data on child online sexual exploitation, including Childline, law enforcement and ICT (Information and Communication Technologies) companies, these sources have not been analyzed and access is often restricted due to privacy concerns and the reluctance of ICT companies to be associated with child sexual abuse.

LEGISLATIONS AND POLICIES TO PROTECT CHILDREN ONLINE

India’s policy and legal framework for cybersecurity is evolving and, despite its limitations, provides a base for building a comprehensive strategy for child online protection. The following laws exist to address cybercrimes:

- The Information Technology Act, 2000, which addresses aspects related to cyberspace, and the Information Technology (Amendment) Act, 2008 are the main pieces of legislation concerned with online activities and cover any communication device used to transmit any text, video, audio or image. The provisions of the National Cyber Security Policy, 2013 enable the development of a dynamic legal framework.
- The National Policy for Children (NPC), 2013 does not refer directly to online risks. All policies related to education, ICT or cybersecurity are expected to incorporate the principles of the NPC and provide children with equal opportunities for learning and empowerment, while protecting them from harm.
- The National Policy of ICT in Schools, 2012 is more explicit about regulating ICT to protect children from potential risks. It recognizes online risks and has provisions for regulating and monitoring Internet access. The promotion of ICT systems in schools and adult education is included in the National Education Policy.
- The National Cyber Security Policy, 2013 addresses the prevention, investigation and prosecution of cybercrimes, including those against children. It calls for strengthening

capacities of law enforcement agencies to investigate cybercrimes and gather data to enable prosecution.

- The Indecent Representation of Women (Prohibition) Act, 1986 prohibits indecent representations of women and criminalizes the performance of obscene acts and songs but does not punish the audience or those who make the person perform such acts.
- The provisions of the Information Technology Act have been strengthened by the Protection of Children from Sexual Offences Act, 2012 which deals with online offences against children, including child pornography and grooming. As the Information Technology Act does not have specific provisions for criminal intimidation, hate speech and defamatory content, the provisions of the Indian Penal Code apply in cases of online offences.

CHILD ONLINE PROTECTION RESPONSE SYSTEM

The multidimensional and fast-changing nature of ICT and social media, combined with problems related to regulation of the Internet, due to its transnational nature and the key role it plays in the democratization of information in society, pose unprecedented challenges for the prevention of and response to child online violence. In order to establish and sustain child online protection systems and preventive strategies, adequate structures, coordination mechanisms, capacities and resources need to be operational.

Traditional legislative frameworks are obsolete against the ubiquitous crimes and offences perpetrated in the virtual world. Indian legislation on child online protection needs to quickly adapt to technology developments and work in close collaboration with international law enforcement agencies and ICT companies to be effective. Strong multisectoral and international collaborations and coordination mechanisms are necessary to ensure that transborder child online abuse cases are investigated and prosecuted in a timely and effective manner.

The Internet and social media can only be regulated and controlled to a certain extent as technological developments enable virtual offenders to swiftly find new ways toovercome control systems. It is also important to balance privacy with protection. The invasion of privacy poses a serious ethical and moral challenge to the task of preempting and proactively addressing online offences. Children’s right to privacy often comes in conflict with the imperative of protection, and a shared narrative on the boundaries has not emerged in India. Prepaid mobile phones present another barrier to monitoring or regulating Internet access for children.

They are convenient for consumers but create major challenges for law and order organizations as well as service providers attempting to track errant behaviors and help bring offenders to justice. Finally, because cases of online offences against children are rarely reported, there is no indicator of the actual incidence and prevalence of child online abuse and exploitation in India. All of the above pose incredible challenges to ensuring the online safety of Indian children and require innovative and technologically advanced approaches and solutions.

For the purpose of this assessment, three distinct areas of intervention were identified as follows:

- monitoring, reporting and removing online child offensive material;
- criminal investigation and prosecution of online sexual abuse and exploitation; and,
- sidentification and service provision for child victims of online exploitation and abuse.

The combination of these three areas of intervention constitutes the emerging child online protection system in India.

JUDICIAL PROCESS

There are no special or fast-track courts for cyber offences and the justice system is already overloaded with the backlog of cases. The Protection of Children from Sexual Offences Act covers some aspects of cyber offences against children and 605 special courts have been set up under the Act across the country; however, there is inadequate confidence in the capacity of these courts to handle sexual assault/child sexual abuse cases. According to the feedback reported from several states and a recent study of the special fast-track courts for sexual assault and child sexual abuse cases in Karnataka, there is a critical need for training on dealing with sexual assault cases for prosecutors, judges and other participants in the criminal justice system, with specialized and ongoing training on violence against women as a minimum provided to judicial officers, prosecutors, lawyers and registrars.

In this scenario, the potential contribution of these courts to handle child online abuse cases cannot be relied upon. The National Judicial Academy, Bhopal, and 21 state judicial academies conduct occasional orientations on cyber laws for the judiciary. The NLSIU in Bangalore and the NALSAR University of Law in Hyderabad also conduct awareness and training programmes on cyber laws and cybercrimes for judicial officers. Not only are these trainings inadequate to meet the existing and growing requirements, the training of prosecutors is an exceptionally weak link in the justice system. They are currently not included in police training or judicial trainings.

They need to be trained and updated on cybercrime, especially cyber offences against children, in a systematic manner.The Cyber Appellate Tribunal, earlier known as Cyber Regulations Appellate Tribunal, was established in October 2006 in accordance with provisions under Section 48 (1) of the Information Technology Act, 2000. As per the Information Technology Act, any person aggrieved by an order made by the Controller of Certifying Authorities or by an adjudicating officer under the Act can prefer an appeal before the Cyber Appellate Tribunal.

There is a Cyber Appellate Tribunal constituted under the Information Technology Act situated at New Delhi, but a judge to preside and decide on the cases has not been appointed since 2011.

RECOMMENDATION

INDUSTRY RECOMMENDATIONS

It is recommended that Industry:

1. Facilitate the development of positive, legal pathways that inspire young people, cultivate and harness their technology skills, possibly through the provision of educational workshops/seminars, internships, youth industry placements and mentoring programmes;

2. Support the development of general educational awareness programmes for young people that could be designed on the basis of the detailed data gathered in this study;

3. Collaborate with law enforcement and policy makers to ensure that where feasible, the online environment where young people are most likely to encounter other hackers or become involved in criminal activity contains warnings about the illegality of this behavior and the serious consequences of being caught.

4. As previously stated, hackathons and other forms of competition where youngsters receive recognition for their talent should be considered, along with gamification as an important delivery mechanism. Investment is required to develop technology solutions to technology facilitated problem behavior (for example; automatically delivered network warnings at the onset of a cyber-intrusive event) and develop software that can specifically profile juvenile/experimental hacking behavior and issue appropriate warnings;

5. Champion - large organizations producing online games, such as Microsoft, should through their social corporate responsibility budgets develop cyber champion programmes to harness the talents of very gifted computer literate youth to highlight and reward positive pathways. These programmes could be based upon competitions at school level and could carry a prestigious award on successful completion.

INTERVENTIONS WITH YOUNG PEOPLE AND AWARENESS RAISING

1. Awareness raising to inform all young people and parents about hacking and cybercrime through general awareness raising programmes in schools;

2. Educate young people about cyber security, cybercrime and the law - this could include e-learning, micro-learning, gamification and relevant topics in school curricula.

3. Identify young people most at risk and work with them to raise awareness about the possible consequences of illegal online behavior;

4. Development of a cyber-peer mentoring programme developed and delivered by young people who have been hackers to the most at-risk groups, identified through awareness raising work in collaboration with law enforcement and industry partners;

5. Ensure that awareness raising and educational initiatives extend to parents through programmes and campaigns;

6. Disseminate - National advertising campaigns (traditional and digital media) should highlight the serious consequences of hacking amongst young people. Online resources should be made available to parents, schoolteachers and youth to educate and inform.

7. Support- Practitioners working with vulnerable youth should be trained to enable an understanding of hacking behavior and should be equipped to respond to their specific support needs.

POLICY RECOMMENDATIONS

1. **Impact**: It is essential that governments and government agencies begin to acknowledge and recognize the extent to which vulnerable young people are becoming involved in illegal internet related activity, and the potential impact when discovered that this may have upon the lives of young people and their families;

2. **Policy**: It is imperative that comprehensive policies focused upon deterrence, prevention and rehabilitation are developed that consider potential loss to industry, but that also consider the needs of often vulnerable young perpetrators, and victim protection;

3. **Practice**: This should no longer be viewed as an industry problem but rather as a shared problem with responsibility for prevention and awareness raising resting with many key stakeholders including government agencies, NGOs and charities responsible for the welfare of children and young people, education, law enforcement, social services, industry as well as academia. The responsibility however falls upon governments to ensure that a central platform is provided to facilitate discussion, policy and practice development through organizations such as the UK Council for Child internet Safety, for example, in the UK context. Most countries will have similar organizations;

4. **Justice and the law**: Appropriate training and education for law enforcement and the judiciary is required. It is essential that criminal justice response including law enforcement investigation and sentencing practice is based upon new and emerging empirical research such as that provided here, in the development of policy guiding

practice. Practical guidelines are required regarding appropriate interviewing and detention protocols given the potential vulnerability of these young offenders.

RESEARCH RECOMMENDATIONS AND NEXT STEPS

1. **Metrics**: It is imperative that technology talented youth are identified at the first possible opportunity in the educational system. Metrics for I.Q, E.Q and C.Q exist, yet there is no early developmental metric to assess technology skills – this research team recommends the urgent development of a Technology Quotient (T.Q) with a view to early stage identification of these valuable skillsets, and subsequently nurturing and rewarding them through the educational system;

2. **Theory**: Many psychology and criminology theories have been conceptualized, tested and validated in real world environments – there is therefore an urgent need to empirically re-evaluate these theories in cyber contexts. They may need to be modified, or new theories may need to be conceptualized and tested (for example Routine Activity Theory in cyberspace, and Online Syndication);

3. **Research**: further research is urgently required to explore youth cognitive processes and motivation to engage in hacking. While a considerable amount has been written regarding the motives of hackers, much of this has been theoretical in nature, with relatively little empirical work. Research should be trans-disciplinary incorporating developmental, physiological, affective and sociological aspects of the behavior with a view to understanding and staging evidence-based interventions. (For example, research exploring hacking and internet addictive behaviors, and hacking tested according to Theory of Planned Behavior which may have predictive value);

4. **Innovation**: There is a need to develop forums to collaborate with industry in terms of developing software and hardware to incorporate appropriate concepts and safeguards 'by design';

5. **Evaluation**: There seems to be an increasing amount of 'good' practice delivered by law enforcement and the education sector in providing youth with cyber-resilience and awareness. However, many of these initiatives occur in relative isolation to each other and have focused upon online safety in the context of abuse and risk, rather than online financial crime and hacking. More communication and knowledge sharing needs to occur to share practice, and evaluations need to be rolled out to measure outcomes and impact at EU-level and internationally;

6. **Training**: Principles of 'Achieving Best Evidence' within criminal justice proceedings must be integrated into work undertaken with regard to adolescent hackers. This will

assure appropriate information is gathered in understanding elements of risk and engagement with online anti-social behavior. In turn, the information will inform future prevention and intervention practice, and will provide a range of stakeholders with descriptive, rich and rigorous data and understanding for their own practice as the threat and extent of youth cybercrime evolves. Rank and file police officers will need additional 'baseline' training across dealing with cyber juvenile delinquents in terms of detection and arrest, along with understanding key principles of cybercrime victimization and offending, including a more detailed perspective and introduction to the role of computers and technology in facilitating hacking and other forms of cybercrime. We must avoid a potential generation of law enforcement officers becoming 'un'-synced with the communities they are meant to protect, engage and support, in real world and in cyber contexts;

7. **Prototype**: There is a clear need to urgently act upon the key findings from this preliminary, ground breaking research. This work was based upon interviews with stakeholders who work closely with young hackers but does not include any interviews with this group; unfortunately it proved very difficult to gain access given the short research time frame. Funding for the second stage of this work will be sought to work proactively with industry and educators and reformed young hackers to develop a prototype educational awareness programme for young people that will be piloted and evaluated in a small number of schools.

CONCLUSION

The protection of children from violence, abuse and exploitation is a major concern in India, but there is an inadequate knowledge base on violence against children in general and online risks and threats to children in particular. Although not much is known about the actual prevalence of cyberbullying, online sexual abuse and exploitation, cyber extremism, cyber addiction and other risks and threats for children, it is evident that Indian children are being affected in many ways. As ICT and the Internet are bound to expand in the course of India's socioeconomic development, these threats will increase because of the rapid technological evolution and the inherent vulnerability of children. There is sufficient indication of the worrying overall trends and patterns to urge for immediate action.

The online abuse and violence against children in India has to be perceived and understood within the context of violence and abuse against children in the country. ICT exacerbates the existing power relationships and pervasive violence against women and children and provides fertile ground for their misuse for harassment, abuse and exploitation. Social attitudes and norms influencing overall violence against women and children and mental health dimensions need to be understood to find ways of approaching them. There is a need to expand the data and knowledge base on online abuse and exploitation of children engaging a broader set of concerned experts in designing the enquiry as most of the studies on technology use and online violence are industry-supported and based on small samples.

There is a simultaneous need to address issues of comprehensive sexuality education with maturity and openness in order to address effectively the issues of adolescent relationships in today’s times, otherwise issues such as gender violence and responsible sexual behavior are difficult to address.

Immediate action may not be able to address every aspect of online protection of children but prioritization of action and rapid follow-through could strengthen the protective environment for children. The broad parameters of the overall strategic approach need to be agreed upon so that various stakeholders can contribute their resources and energies for a coordinated response to strengthen different aspects of the protective environment.

The challenge of creating a safe online environment for children lies in developing a range of responses that strike an appropriate balance between maximizing the potential of ICT to promote and protect children’s rights and opportunities while minimizing risks and ensuring children’s safety and protection. The benefits of technology and its potential to empower children, together with recognition of the resourcefulness and evolving capacity of children to take an active and responsible role in their own protection and that of others, must lie at the heart of all initiatives.

Both boys and girls have a role to play and their inherent energies and potential need to be harnessed. Developing the online competencies of children must also include building their capacities and resilience as digital citizens based on values and life skills, not just be limited to avoiding the risk of specific online threats. Furthermore, schools, teachers, parents/ guardians, policymakers, industry players and other key stakeholders should adopt a proactive approach towards fostering such a favorable environment.

As a matter of urgency, a comprehensive package of specialized services should be developed for the support and recovery of child victims of online exploitation and abuse. These services should include adequate skills, capacities and resources, especially for mental health support, to meet the specific needs of child victims of online abuse. These specialized services should of course be integrated and mainstreamed in India’s overall child protection systems and services.

References

1. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (London, UK: Elsevier Inc., Third edition, 2011).

2. Barr, T. (2001), "E-Futures: Towards a better understanding of internet users", Deakin Lectures, www.abc.net.au/rn/deakin/default.html, accessed on September 19, 2019

3. Slattery, L. (2001), "Snake oil for the ills of modern life". The Australian, 27 June, p.13

4. Starch, R. (1999). "The American Online/ Roper Starch Youth Cyberstudy 1999", Http:// www.corp.aol.com/ press/ study/youthstudy.pdf, accessed on September 19, 2019.

5. Halder D., & K Jaishankar, 'Patterns of Sexual Victimization of Children and Women in the Multipurpose Social Networking Sites'; In C. Marcum and G. Higgins (Eds.), Social Networking as a Criminal Enterprise, Boca Raton, FL, USA: CRC Press, Taylor and Francis Group. ISBN, 2014.

6. Interview with Karnika Seth, Cyber Law expert and visiting faculty to National Police Academy and National Judicial Academy, CBI Academy and National Investigation Agency, NOIDA.

7. Press Information Bureau, Government of India, Ministry of Women and Child Development, 3 March 2016. This information was given by the Minister for Women and Child Development, MrsManeka Sanjay Gandhi, in reply to a question in the Rajya Sabha.

8. Kothari, Jayna and Aparna Ravi, The Myth of Speedy and Substantive Justice: A Study of the Special Fast Track Courts for Sexual Assault and Child Sexual Abuse in Karnataka, Centre for Law and Policy Research, Bangalore.