NATIONAL ACTION RESEARCH ON CYBER-ENABLED HUMAN TRAFFICKING

PRAJWALA
AN ETERNAL FLAME
PRAJWALA

ACKNOWLEDGEMENTS

Sunitha Krishnan
Founder, General Secretary, Prajwala

Prajwala is grateful for the active collaboration and partnership of police from 15 States in the completion of this National Action Research Report

Prajwala acknowledges the support of:

Director General of Police of the following states:
Telangana, Andhra Pradesh, Kerala
Punjab, Rajasthan, Madhya Pradesh
Maharashtra, Gujarat, Goa
Bihar, West Bengal, Jharkhand, Odisha, Assam, Meghalaya

Research Team

Ms. Sunitha Krishnan
Principal Investigator and Advisor

Ms. Swasti Rana
Project Coordinator

Mr. Mallesham Yadav
Operation Head

Mr. Mohammed Riyazuddin
Cyber Investigator

Mr. Tabish Ahsan
Research Officer

Ms. Aparna Bhat
Legal Expert

Ms. Aadira Srinivasan
Assistant Legal Researcher

Lt. Col. Vijay Kishore Jha (Retd.)
Technology Expert

Ms. Aletha Tavares
Editor

NATIONAL ACTION RESEARCH ON CYBER-ENABLED HUMAN TRAFFICKING

Prajwala, 2024
Year of Publication: 2024

A publication of Prajwala, Hyderabad

Survey No. 64/2, 65/3
Basavaguda Road
Mankhal (Village & Post)
Maheshwaram (Mandal)
Ranga Reddy (Dist)
Telangana State-501359
www.prajwalaindia.com

Disclaimer

Prajwala has developed this document for the Project **"Developing A Framework To Counter Cyber-Enabled Human Trafficking (CEHT)"** of U.S. Consulate General Hyderabad.

This handbook was funded by a grant from the U.S. Consulate General Hyderabad. The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the U.S. Government.

Designed by:
Parrot Communications
www.parrotcommunications.com

Printed at:
Pragati Art Printers
www.pragati.com

TABLE OF CONTENTS

Justice Madan B. Lokur

Former Judge
Supreme Court of India

A-26, First Floor, Gulmohar Park
New Delhi - 110 049
E: madanlokur@outlook.com
M: +91 9868219007

2nd September, 2024

FOREWORD

Sunitha Krishnan is an indefatigable crusader. She has spent several decades of her life fighting against human traffickers and rehabilitating women and girls whom she has rescued from these traffickers. Her struggles on the ground, not only in Hyderabad where she is based, but in different parts of the country, have given her a deep insight into how traffickers operate, whether it is for the sex trade or for cheap labour amounting to slavery.

Rescuing victims of human trafficking is, quite naturally, a very dangerous assignment. But, without caring for the consequences, Sunitha has undertaken multiple rescues. What does one do, after a successful rescue, with women and girls who have been trafficked either in the sex trade or for slavery and who are traumatised both physically and emotionally and stigmatised by society and even shunned by their family? If the rescued women and girls are not immediately taken care of and gradually rehabilitated, they will have nowhere else to go but back to their traffickers. What then is the purpose of rescue? Sunitha established a home for these women and girls way back in 1996 through her organisation called Prajwala, meaning an eternal flame. Having met some of these unfortunate women and interacted with them, I can say with certainty that they have overcome the horrors of their past and have since been reintegrated into society.

Many, not only in Hyderabad but in different parts of the country, are aware that reliable information received by them and forwarded to Sunitha will surely be acted upon with the urgency it deserves. This information includes not only incidents of trafficking but also sharing pornographic videos, including of child sexual abuse. Armed with enough material to stir the conscience of the Supreme Court, she filed a public interest litigation for directions to the Government of India to utilise its resources to stop the unrelenting transmission of pornographic material and prosecute offenders. The material that stirred her, originated not only from India but from other parts of the world and many videos were widely circulated.

As luck would have it, her public interest litigation landed in my court and with Sunitha's assistance who appeared in person on almost every hearing, and with the assistance of an equally concerned brother judge and an amicus curiae we set about the task of trying to bring some sanity in the madness of the situation. Officers of the Government of India dealing with issues of technology, particularly cybercrime fully appreciated the potential harm that could be caused if urgent steps were not taken to prevent the situation from going out of control. In a departure from practice, Sunitha and the amicus Aparna Bhat were invited by senior officers of the Government of India to discuss measures and share their knowledge and expertise for the good of society in an effort to crush the abominable dissemination of harmful content and extremely distressing goings-on.

The crusading spirit and determination of Sunitha and Aparna eventually led to the establishment of an interactive cybercrime portal by the Government of India which gradually came to be fine-tuned with the assistance of domain experts and agencies in different countries particularly the United States, Canada and the United Kingdom, all of whom were working with the same ultimate goal. Over the years, the efforts began to show positive results and eventually led to the establishment of the Indian Cyber Crime Coordination Centre (I4C).

While remarkable advancement has been made in preventing human trafficking through the Internet, the traffickers have, unfortunately, managed to be a step ahead. These developments prompted Sunitha to put her experience and knowledge of crime prevention and carry out a research project on human trafficking, in all its forms and aspects. The result is this remarkable study aimed at persuading the decision and policy makers in the Government of India to frame a national policy to curb the menace of human trafficking through the use of technology and the Internet.

The research carried out by Sunitha Krishnan and her team at Prajwala with the able assistance of several experts, focusses on an enormous, yet rarely discussed human problem. We discuss trafficking of drugs, of wildlife, of firearms, but not of humans. This is despite the fact that human trafficking is carried out quite openly on the Internet, as the research suggests, and participation is open to everyone, often free or on a small payment. Sunitha's investigator obtained, as a decoy customer, 32 GB of child sexual abuse material for as little as INR 530.

The study reveals that obtaining sexual abuse material is only one facet of human trafficking. Procuring humans for the sex trade is a major worrying aspect of trafficking. Anonymous, faceless individuals entice gullible persons, or persons out to make a quick buck to perform minor acts that they would never do otherwise and then the journey of horror begins. The victims have no way out after entrapment.

While human trafficking for the sex trade is a major and serious concern, other forms of trafficking have also been diligently researched. Instances of modern slavery, for example, take many forms and have been discussed. It is now common knowledge that hundreds from our country have been trafficked to south east Asia to work as cyber criminals. They work under inhuman conditions and their principal assignment appears to be to entice the gullible to participate in cyber scams. While these crimes are being investigated, it will be a very long haul before conviction. There are also instances of our countrymen having been lured with lucrative overseas jobs finding themselves compelled to participate in the war between Russia and Ukraine. Illegal inter-country migration and adoption of children in India and other countries is another form of human trafficking adverted to in the research.

The purpose of the research by Sunitha Krishnan and her team at Prajwala is not to give statistical information – this is probably already available with the several anti-human trafficking units of the Government of India. The purpose is to enable the government to formulate a policy to tackle this horrendous crime from the stage of investigation to conviction of the traffickers. Keeping in mind that human trafficking is a global phenomenon, a detailed study has also been carried out of the laws in other countries and the institutions for implementing them. Also discussed are challenges and legal hurdles such as identification of anonymous, faceless and nameless traffickers;

cracking the tight nexus between traffickers in different countries; difficulties in prosecution and trial, including jurisdictional issues. There is a wealth of knowledge and learning in the research.

The benefit of this research to society is that it will bring necessary awareness of horrific crimes enabled by technology. The debate and discussion that will be generated, hopefully, should enable the formulation of a comprehensive policy to tackle the complex problem of human trafficking in all its manifestations, including contemporary forms of slavery. It will also, hopefully, strengthen our existing institutions so that investigations close quickly and conviction obtained swiftly.

It is time for us to face reality and take strong remedial steps, and Sunitha Krishnan's research of great significance helps us do that.

(Madan B. Lokur)

Rekha Sharma
Chairperson
Tel.: 011-26944808

भारत सरकार
राष्ट्रीय महिला आयोग
प्लाट नं. 21, जसोला इंस्टीट्यूशनल एरिया
नई दिल्ली-110025

GOVERNMENT OF INDIA
NATIONAL COMMISSION FOR WOMEN
PLOT NO. 21, JASOLA, INSTITUTIONAL AREA
NEW DELHI-110025
Website: www.ncw.nic.in
E-mail: chairperson-ncw@nic.in
sharmarekha@hotmail.com

FOREWORD

Human trafficking is a multi-dimensional organised crime with a global reach. With the rapid increase in internet usage and fast changing technologies, an exponential increase in varied forms and dimensions of human trafficking is being reported across countries. The internet has shifted the recruitment, advertising and selling process from the street to the digital domain. Correspondingly, this rapid growth of digital technologies has left a gap in laws, services, and awareness to ensure a corresponding safe and positive online environment. Communities, policy makers and governments face new challenges in keeping men, women and children safe online.

Digital empowerment, while positive, has raised concerns about safety, evident in the rise of cybercrimes during the pandemic, despite a decline in reported crimes. A study conducted in India by CyberPeace Foundation and Space2Grow sought to explore trends in online abuse and trafficking of women and children and examine their vulnerability to abuse in rural and semi-urban communities in India. It was reported that India has 646 million active internet users aged two years and above as of December 2021. Among them, 592 million are aged 12 years and above with an increase of 37 per cent from 2019.

As an early response to these challenges, the National Commission for Women (NCW) launched "Digital Shakti" in 2018 to support women on the digital aspects. The initiative works towards helping women report online abuse, access redressal mechanisms, understand data privacy, and use of technology for their benefit. Through the four phases of the campaign, over 4.5 lakh girls, women and netizens across the country have been sensitized with the aim to build resilience in online spaces. In 2022, the NCW established an Anti-Human Trafficking Cell to improve effectiveness in tackling cases of human trafficking, raising awareness among women and girls, capacity building and training of Anti Trafficking Units and to strengthen and sensitize law enforcement machineries.

While there is a generic understanding of what is cyber-enabled human trafficking (CEHT), in the last few years, more-so in the wake of the COVID-19 pandemic, there are varied elements and dimensions that have emerged which require closer understanding in order to develop an effective national level response in India to effectively counter this crime.

I commend the tireless efforts of Prajwala, a leading anti-human trafficking organization led and supervised by Padma Shri Sunitha Krishnan, for protecting the rights of the most vulnerable and marginalized members of society.

New Delhi
22nd July, 2024

(Rekha Sharma)

From the Researchers Desk

In the past three decades of my work as an anti-trafficking activist, the last one was the most challenging and disturbing. The nature of trafficking changed due to the introduction of cyber technology in human trafficking. I was exposed to this new modus operandi via a case of sex trafficking that we dealt with at Prajwala where the victims were rescued after a decoy operation on the popular classifieds website, Locanto. What was deeply disturbing was the fact that the victims could not identify a single trafficker. And it was not due to threat or intimidation, but only because none of them had actually seen their trafficker! When more such cases got reported, a clear pattern started emerging. The traffickers and their networks were increasingly concealing their identities using technology. Fake identities and false profiles were being used on social media to lure or groom a vulnerable person. These facts made it clear that cyber technology had reached the scene of crime as an enabler. The COVID-19 pandemic, which pushed the world to adopt cyber technology as a way of life, completed the picture with traffickers finding a new route to reach the most vulnerable persons. Time and geography were no longer a limiting factor, and these criminals could strike any place around the world, in complete anonymity.

Cyber technology is a vast and powerful tool that has transformed the way we live, work, and communicate. With over 646 million internet users in India, technology penetration has irreversibly changed our lives. But it is also a fact that the anonymity, accessibility, and the dynamic nature of the internet has facilitated the perpetration of cyber-crimes on an unprecedented scale. The organised crime of human trafficking is no exception.

Post-pandemic, the visibility of cyber-crimes has increased several folds. A significant number of cyber-enabled human trafficking (CEHT) cases for various purposes of exploitation also started coming to light. Ironically, the cases booked under human trafficking did not reflect the role of technology. This resulted in some cyber-crimes, which potentially were also cases of human trafficking, getting passed off as a less severe crime. As more and more cases of CEHT were detected, the legal lacunae in addressing such cases became evident. At the same time, it also highlighted the need for technology firms to make their platforms safer for users and when required, ensuring cooperation with the prosecution in bringing cyber criminals to justice.

Responding to this situation required a more in-depth understanding of the problem. It is this insight that prompted the need to conduct a national action research on CEHT, which provided us with empirical data on the scale and complexity of the problem. That said, understanding the problem will definitely give us a better perspective, but change can only happen if a solution-based approach is integrated into the process of gaining this understanding. Hence, the research contained in this document aims to create a draft national plan of action (NPoA), which will outline schemes, programs, and specific legal reforms that help us thwart efforts of cyber criminals.

This national study is not intended to quantify CEHT cases or map out its regional impact, rather it aims to understand the trends and patterns of CEHT, the role that technology and technology companies can play, and gaps in the legal mechanism to redress this organized crime. The learnings from the study will feed into drafting the first ever NPoA to combat CEHT. The methods adopted in the research not only elicit a better understanding of the crime and the modus operandi used, but also provide a means to authenticate and validate the findings by validation investigations.

Undertaking an exercise of this nature and on this scale would not have been possible without the active collaboration and partnership of the Telangana State Police under the leadership of then Director General of Police, Shri. Anjani Kumar, IPS. My heartfelt gratitude to Shri. Mahesh Muralidhar Bhagwat, IPS, the then ADGP, CID and the entire team from the Crime Investigation Department (CID), Telangana Police for providing unstinting support in this challenging endeavour.

I place my humble gratitude to the Directors General of Police of Andhra Pradesh, Kerala, Punjab, Rajasthan, Madhya Pradesh, Maharashtra, Gujarat, Goa, Bihar, West Bengal, Jharkhand, Odisha, Assam, and Meghalaya, who enabled us to carry out the data collection exercise in their respective states despite pressing situations created by the announcement of the general elections just before the field research exercise.

This research would not have been complete without the support of several of our valued partners based globally and nationally who facilitated the global consultations. I humbly acknowledge the support of our partners the U.S. Department of State; DKA Austria; the British Deputy High Commission, Hyderabad; the Royal Thai Consulate-General, Chennai; the Counter Extremism Project, Spain; and the International Justice Mission, Philippines.

All good ideas, every right effort requires a strong platform to get help it take off and succeed. I place my deepest gratitude to Shri Nara Chandrababu Naidu, the Honourable Chief Minister of Andhra Pradesh, for providing us that platform. He is a visionary leader who has always demonstrated extraordinary leadership in acknowledging the most complicated problems and finding solutions to them. I sincerely thank him for his collaboration and partnership in disseminating this important research at a national level and supporting the practical and applicable solutions that have emerged after our collective efforts.

The U.S. Consulate General Hyderabad has been our longstanding partner and collaborator, supporting us actively in the anti-trafficking mission and in funding this national action research. I humbly acknowledge members of the Public Diplomacy Section of the U.S. Consulate General Hyderabad who supported our efforts in drafting both the national action research report and the NPoA.

And finally, to my team of domain experts who assisted me in this humongous effort, I can only express much gratitude and appreciation. They, despite the extremely challenging and sometimes hostile work conditions, remained focused on the task undertaken and successfully completed the same as planned.

Jai Hind!

Sunitha Krishnan
Padma Shree Awardee
Project Advisor & Principal Investigator
Founder, Prajwala

Abbreviations

ADGP	Additional Director General of Police
AHTU	Anti-Human Trafficking Unit
AI	Artificial Intelligence
API	Application Programming Interface
App	Application
ASI	Assistant Sub Inspector
ASW	Adult Service Website
ASEAN	Association of Southeast Asian Nations
ASEAN-ACT	ASEAN-Australia Counter Trafficking
ASF	Akancha Srivastava Foundation
AWF	Analytical Work File
BBA	Bachpan Bachao Andolan
BKS	Bal Kalyan Sangh
BNS	Bharatiya Nyaya Sanhita
BOI	Bureau of Immigration
BPR&D	Bureau of Police Research and Development
C3P	Canadian Centre for Child Protection
CARA	Centralized Adoption Resource Agency
CBI	Central Bureau of Investigation
CBO	Community Based Organizations
CCI	Child Care Institution
CCIPS	Computer Crime & Intellectual Property Section
CCPCJ	Commission on Crime Prevention and Criminal Justice
CCVC	Centre for Cyber Victim Counselling
CDA	Communications Decency Act
CEHT	Cyber Enabled Human Trafficking
CEOP	Child Exploitation and Online Protection Centre
CEPOL	European Union Agency for Law Enforcement Training
CID	Crime Investigation Department
CIF	Childline India Foundation
CINI	Child in Need Institute
CLPRA	Child Labor (Prohibition and Regulation) Act

COE	Council of Europe
CPF	Cyber Peace Foundation
CPS	Child Protection Services
Cri-MAC	Crime Multi Agency Centre
CrPC	Criminal Procedure Code
CSO	Civil Society Organization
CSA	Child Sexual Abuse
CSAM	Child Sexual Abuse Material
CSE	Commercial Sexual Exploitation
CSR	Corporate Social Responsibility
CWC	Child Welfare Committee
DCPO	District Child Protection Officer
DeitY	Department of Electronics and Information Technology
DHS	Department of Homeland Security
DLSA	District Legal Services Authorities
DM	Direct Messaging
DNA	Deoxyribonucleic Acid
DPDP	Digital Personal Data Protection Act
E4J	Education for Justice
ECA	Employment of Children Act
ECAP	Endangered Child Alert Program
ECOSOC	Economic and Social Council
ECPAT	End Child Prostitution in Asian Tourism
ESIC	Employees' State Insurance Scheme
ECS	Engineering and Computer Simulations
ESP	Electronic Service Providers
EU	European Union
FBI	Federal Bureau of Investigation
FGD	Focused Group Discussion
FIR	First Information Report
FOSTA	Fight Online Sex Trafficking Act
FRRO	Foreigners Regional Registration Office
G8	Group of Eight
GBCAT	Global Business Coalition Against Trafficking

Glo. ACT	Global Action against Trafficking in Persons and the Smuggling of Migrants
GPS	Global Positioning System
GRETA	Group of Experts on Action Against Trafficking in Human Beings
GSI	Global Slavery Index
HSI	Homeland Security Investigation
HT	Human Trafficking
I4C	Indian Cybercrime Coordination Centre
ICAC	Internet Crimes Against Children
ICAT	Inter-Agency Coordination Group Against Trafficking
ICDS	Integrated Child Development Scheme
ICMC	Impulse Case Management Centre
ICMEC	International Centre for Missing and Exploited Children
ICPF	India Child Protection Fund
ICT	Information and Communication Technology
ID	Identity
IJM	International Justice Mission
ILO	International Labor Organization
IM	Instant Messaging
INGON	Impulse NGO Network
INTERPOL	International Criminal Police Organization
IO	Investigating Officer
IOM	International Organization for Migration
IP	Internet Protocol
IPC	Indian Penal Code
IPS	Indian Police Service
IRRC	Integrated Resource-cum-Rehabilitation Centre
ISP	Internet Service Providers
IT	Information Technology
IT Act	Information Technology Act
ITPA	Immoral Traffic Prevention Act
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
JJ Act	Juvenile Justice (Care and Protection of Children) Act

JJS	Jan Jagran Sansthan
JOO	Joint Operational Office
KYC	Know Your Customer
LEA	Law Enforcement Agency
LEAP	Law Enforcement Analysis Project
LEO	Law Enforcement Officer
LJI	Love Justice International
MEA	Ministry of External Affairs
MeitY	Ministry of Electronics and Information Technology
MIB	Ministry of Information and Broadcasting
MO	Modus Operandi
MPPPG	Ministry of Personnel Pension and Public Grievances
MSB	Money Service Business
MWCD	Ministry of Women and Child Development
NALSA	National Legal Services Authority
NAP	National Action Plan
NARR	National Action Research Report
NCII	Non-Consensual Intimate Image
NCMEC	National Centre for Missing and Exploited Children
NCPCR	National Commission for Protection of Child Rights
NCRB	National Crime Records Bureau
NCW	National Commission for Women
NEFT	National Electronic Fund Transfer
NGO	Non-Governmental Organization
NHRC	National Human Rights Commission
NIA	National Investigation Agency
NLP	Natural Language Processing
NOC	No Objection Certificate
NOTTO	National Organ and Tissue Transplant Organization
NPL	Dutch Postcode Lottery
NPoA	National Plan of Action
NPU	National Police of Ukraine
NRM	National Referral Mechanism
OAS	Organization of American States

OCSE	Online Child Sexual Exploitation
OCSEA	Online Child Sexual Exploitation and Abuse
OHCHR	Office of the United Nations High Commissioner for Human Rights
OSA	Online Safety Act
OSEC	Online Sexual Exploitation of Children
OSC	One Stop Centres
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open-Source Intelligence
P2P	Peer to Peer Network
PACT	Protect All Children From Trafficking
PAGCOR	Philippine Amusement and Gaming Corporation
PAP	Prospective Adoptive Parents
PC	Personal Computer
PCMA	Prohibition of Child Marriage Act
POCA	Proceeds of Crime Act
POCSO	Protection of Children from Sexual Offences Act
POGOs	Philippine Offshore Gaming Operators
PI	Principal Investigator
PLV	Para Legal Volunteers
PMLA	Prevention of Money Laundering Act
PPHSA	Punjab Prevention of Human Smuggling Act
ROCU	Regional Organized Crime Unit
ROC	Registrar of Companies
RPH	Revenge Porn Helpline
RSO	Regional Support Office
RTGS	Real Time Gross Settlement
SAA	Specialized Adoption Agency
SAARC	South Asia Association for Regional Cooperation
SCROL	Safety for Children and their Rights Online
SESTA	Stop Enabling Sex Trafficking Act
SHO	Station House Officer
SI	Sub Inspector
SIM	Subscriber Identity Module

SLSA	State Legal Services Authority
SOM	Smuggling of Migrants
SOP	Standard Operating Procedure
SP	Superintendent of Police
STEP	Support to Training and Employment Programme for Women
STR	Suspicious Transaction Report
SWGFL	South West Grid for Learning
TAT	Tech Against Trafficking
TDH	Terre Des Hommes
Tech	Technology / Technological
THB	Trafficking in Human Beings
THOTA	Transplantation of Human Organs and Tissues Act
TIP	Trafficking In Persons
TOR	The Onion Router
TV	Television
TVPA	Trafficking Victims Protection Act
UAE	United Arab Emirates
UK	United Kingdom
UNTOC	United Nations Convention on Transnational Organized Crime
UNICEF	United Nations Children's Emergency Fund
UNODC	United Nations Office on Drugs and Crime
UNVTF	United Nations Voluntary Trust Fund
UPI	Unified Payments Interface
URL	Uniform Resource Locator
USA/US	United States of America
USD	United States Dollar
VGT	Virtual Global Taskforce
VOT	Victim of Trafficking
VPN	Virtual Private Network
WP	Writ Petition

Chapter

01

Introduction

Chapter 1

Introduction

Technological advancements have revolutionized virtually every aspect of human life. Central to this transformation has been the proliferation of digital technologies and the internet that has taken global connectivity and information exchange to an unprecedented scale.[1]

The widespread availability of high-speed internet connectivity and the proliferation of mobile apps have democratized and empowered individuals to participate in the digital economy. This has accelerated the pace of technological adoption, enabling individuals to access information and services on the go. The offshoots of these applications, for example the social media platforms, have given new meaning to forging associations, sharing and engaging with content, and fostering virtual communities and networks transcending geographic boundaries. Artificial Intelligence (AI)-powered algorithms are increasingly being used to automate tasks, optimize processes, and personalize experiences, transforming the way businesses operate and individuals interact with technology.

Against this backdrop of technological advancement, there is also a dark side. Digital platforms have also offered safe havens to criminal elements who exploit these platforms for their illicit activities.[2] Cyberspace is the new crime scene, encapsulating fraud, identity theft, doxing, morphing, phishing, and many other crimes, including CEHT. The anonymity, accessibility, and dexterous nature of the internet have facilitated the perpetration of crimes on a global scale,[3] in addition to its original form. Trafficking in persons itself is expanding into various forms, and with the entry of technology, the entire dynamics of technology-supported human traffickers are taking it to the next level.[4] Technology has become a tool for traffickers to facilitate, organize, network, and evade authorities with greater speed, less cost and more anonymity.[5]

Prajwala is an anti-trafficking organization that has been fighting sex trafficking for the last

1 World Economic Forum. (2022). Global Technology Trends to Watch. Retrieved from https://www.weforum.org/agenda/2022/01/tech-trends-in-2022/

2 Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA). Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

3 United Nations Office on Drugs and Crime (UNODC). (2023). Global Report on Trafficking in Persons. Retrieved from https://www.unodc.org/documents/data-and-analysis/glotip/2022/GLOTiP_2022_web.pdf

4 Various manifestations of human trafficking are emerging and are being documented with forced criminality being the latest as reported both in the TIP report of UNODC as well as TIP report of the US State Department.

5 The use and abuse of technology in human trafficking in Southeast Asia (July 2022); https://www.aseanact.org/story/use-and-abuse-of-technology-in-human-trafficking-southeast-asia/

three decades. It has been closely observing and tracking the usage of technology for sex trafficking during the last decade, with many victims rescued from technological platforms such as Locanto and Facebook. In 2015, Prajwala[6] sent a letter to the Hon'ble Supreme Court of India pursuant to the circulation of sexual violence imagery on social media platforms. The Court converted this letter into a petition,[7] and that became the cause for the creation of an online reporting portal and one of the first cases that looked at intermediary accountability for sexual crimes in India followed by setting up the first ever national Indian Cyber-Crime Coordination Centre (I4C) under the Ministry of Home Affairs. Research into how technology and intermediaries are dealing with sex crimes during the conduct of the cases exposed the vulnerability of the trafficked, the expanse of the technology canvas, the limitations of the service providers (intermediaries), and the preparedness of law enforcement to address it.

Against this backdrop and taking forward previous learnings, Prajwala, with the support of the U.S. Consulate General Hyderabad, and in collaboration with Telangana State Police, initiated a process towards developing an all-encompassing and comprehensive draft NPoA, which holistically embodies the aspects and elements of cyber-enabled human trafficking and provides for coordinated responses. This National Action Research Report is part of that initiative and aims at understanding the trends and patterns of CEHT, identifying the gaps in the legal framework, understanding the global patterns and best practices and evolving a solution-based framework for the country.

1.1 Trafficking In Persons

Human trafficking has evolved over the years, and throughout history, individuals were subjected to exploitation and forced labor in various forms, driven by economic, political, and social factors.[8] Trafficking flourished in the context of colonization, war, and economic upheaval, where vulnerable populations were exploited for labor or sexual servitude. The transatlantic slave trade, for example, saw millions of Africans forcibly transported to the Americas and Europe to work on plantations, mines, and other labor-intensive industries.[9] The 19th and early 20th centuries witnessed the emergence of organized crime networks engaged in trafficking women and children for sexual exploitation, and forced labor. Women and girls were trafficked across borders and sold into brothels or domestic servitude, while children were often exploited in factories, mines, and agricultural estates. The crime has only expanded, with diverse forms surfacing as each day progresses.[10]

The 20th century saw significant strides in the international recognition of human trafficking as a crime against humanity. The adoption of international treaties and conventions, such as the

6 Prajwala is an anti-trafficking civil society organization located in Hyderabad, Telangana. The present endeavor is Prajwala's self-driven efforts.

7 SMW (crl) No.3/2015, In re Prajwala

8 International Labour Organization (ILO). What are forced labour, modern slavery and human trafficking? Retrieved from https://www.ilo.org/global/topics/forced-labour/definition/lang--en/index.htm

9 Shelley, L. (2010). "Human trafficking: A global perspective". Cambridge University Press. https://dl.icdst.org/pdfs/files4/bd2523edf8d7f5e86255690f65a06589.pdf

10 *Id.*

Universal Declaration of Human Rights (1948)[11] and the United Nations Protocol to Prevent, Suppress, and Punish Trafficking in Persons (2000),[12] marked important milestones in the global anti-trafficking movement.

Human trafficking, despite interventions, remains a pervasive and complex problem, fuelled by poverty, inequality, conflict, and corruption. In recent decades, the proliferation of digital technologies has facilitated the evolution of trafficking into a new insidious form of exploitation, which is cyber-enabled, posing new challenges for law enforcement and anti-trafficking advocates.[13]

1.2 Cyber-Enabled Human Trafficking (CEHT)

This phenomenon represents a paradigm shift in the way human trafficking was perpetrated and managed, leveraging the vast capabilities of the internet and digital platforms to facilitate the exploitation of vulnerable individuals for profit. As we delve deeper into understanding CEHT, it is imperative to examine its historical context, the role of technology in its proliferation, its global and local definitions, the factors driving this shift, and its present and future implications.

The adverse impact of the internet was noticed in the early nineties, and there were several studies conducted in the United States of America and Europe. One of the collaborative studies initiated by the Council of Europe was based on a study by a team that further based its report on two reports by a U.S. based researcher, Ms. Donna Hughes.[14] This study, even though limited to Commercial Sexual Exploitation, documented certain key observations that remain prophetic even at the time of writing this report. The impact of internet can be best explained by the experience shared by a law enforcement officer at that time (2000/2001) who stated in an interview that he had noticed a decrease in the pattern of child pornography in the late eighties, which showed dramatic increase post the advent of the internet, and by 2000, nearly 77 percent of the available content was online.[15]

The penetration of cyber technologies into the realm of human trafficking, given the way it contributed to increasing online CSAM, was a natural progression over time. However, despite that, it remains a significant evolution, given the way exploitation of humans is orchestrated and enabled, its expanse and its speed. Online platforms, including messaging applications, and chatrooms offered on social media, have become pivotal tools for traffickers to identify, recruit, and exploit victims, leveraging the unbridled reach and relative anonymity afforded by the digital landscape. These spaces serve as virtual hunting grounds where traffickers prey on vulnerable individuals, often masquerading as friends or benefactors to gain their trust. The use of deceptive tactics, such

11 United Nations General Assembly. (1948). Universal Declaration of Human Rights. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights

12 United Nations Office on Drugs and Crime. (2000). United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children. Retrieved from https://www.unodc.org/documents/human-trafficking/UNTOC/Publications/UNTOC_Trafficking_in_Persons_protocol_ebook.pdf

13 United Nations Office on Drugs and Crime (UNODC). (n.d.). Technology Facilitating Trafficking in Persons. Retrieved from https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.html

14 Directorate General of Human Rights, Council of Europe; The Impact of the use of new information technology on trafficking in human beings for the purpose of sexual exploitation; 2003

15 Interview with Raymond Smith, Fraud, Child exploitation and asset forfeiture group, Office of Criminal Investigations, US Postal Inspection Service, 7 May 2001 as referred in study at supra.

as false promises of employment or romantic relationships, enables traffickers to lure victims into exploitative situations, exploiting their vulnerabilities for profit.[16] As observed in the news release of the UNODC, victims are being targeted and recruited via social media and online dating platforms where personal information and details of people's locations are readily available.[17] The pattern, however, is not limited to this alone. Digital utilities have crept into the modus operandi of the trafficker seamlessly and they are known to use it for recruitment, management, control, money transfer, addressing demand, and coercing victims into submission. The penetration of cyber technologies also extends to the control and surveillance of victims, with traffickers exploiting digital devices and online platforms to exert dominance and monitor their movements. Mobile phones equipped with GPS tracking capabilities are used to monitor victims' whereabouts and ensure compliance, while surveillance cameras and hidden recording devices are employed to maintain control and deter escape attempts. In some cases, traffickers leverage digital platforms to live stream abuse and exploitation, additionally catering to the demands of online consumers seeking illicit content.[18]

They exploit the anonymity, accessibility, and global reach of digital platforms to target vulnerable individuals, deceive them into exploitative situations, and evade detection from law enforcement as well as overcome geographical barriers.[19] The use of crypto currency and other anonymous online payment methods further complicates efforts to track and disrupt trafficking transactions, enabling traffickers to operate with impunity in the shadows of the digital realm.[20]

In addition to the above, innovations in technology are offering novel opportunities to the traffickers as well. For instance, the emergence of technologies such as AI, virtual reality, and deep fakes presents new opportunities and challenges in the realm of human trafficking. These technologies can be harnessed by traffickers to create lifelike simulations of exploitation, manipulate images and videos to deceive victims and law enforcement, and automate certain aspects of the trafficking process.[21] AI-powered chatbots and virtual avatars may be deployed to engage with potential victims, gather personal information, and tailor grooming tactics to exploit individual vulnerabilities.[22] Deep fakes are the latest challenge faced by victims and law enforcement at the time of writing this report.[23]

---

16 UNODC. "The Role of Technology in Human Trafficking." UNODC, www.unodc.org/unodc/en/human-trafficking/Webstories2021/the-role-of-technology-in-human-trafficking.html.; United States Government Accountability Office. (2022, February). Use of Online Marketplaces and Virtual Currencies in Drug and Human Trafficking: Report to Congressional Committees. TRAFFICKING. Retrieved from https://www.gao.gov/assets/720/719089.pdf

17 UNODC; Good Use and Abuse: The Role of Technology in Human Trafficking, 2021, accessed on March 8, 2024

18 United Nations Office on Drugs and Crime. (2021). Global Report on Trafficking in Persons 2020: Chapter 5. Retrieved from https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf

19 Council of Europe, Supra note 16

20 *Id.*

21 The Conversation. (2024, February 8). Cybercriminals are creating their own AI chatbots to support hacking and scam users. Retrieved from https://theconversation.com/cybercriminals-are-creating-their-own-ai-chatbots-to-support-hacking-and-scam-users-222643

22 New York Post. (2023, August 9). Outlaw AI chatbots make cybercrime easier and more frequent. Retrieved from https://nypost.com/2023/08/09/outlaw-ai-chatbots-make-cybercrime-easier-and-more-frequent/ Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf

23 NewsIndiaRashmika Mandanna deepfake case: Delhi Police tracks down 4 who uploaded video

1.3 Defining Cyber-Enabled Human Trafficking (CEHT)

CEHT is a multifaceted phenomenon in human trafficking that leverages technology to facilitate the exploitation of vulnerable individuals. It encompasses a range of online activities used by traffickers to exploit victims, including online recruitment through social media platforms, advertisement of victims on online marketplaces, negotiation of transactions through encrypted messaging apps, and coordination of exploitation activities using digital communication tools. Referred to by different terms and phrases, it encompasses diverse manifestations and dynamics. This report uses the term CEHT. The term is synonymous with "technology-facilitated/enabled/assisted human trafficking," cyber-trafficking, digital trafficking, Information and Communication Technologies (ICTs), facilitated sexual exploitation, and misuse of technology for human trafficking. Various terms used for CEHT are:

Online Trafficking:[24] This term emphasizes the use of online platforms and digital technologies in the trafficking process, including recruitment, advertising, and exploitation of victims.

Digital Exploitation:[25] Digital exploitation highlights the role of technology in perpetrating exploitation, encompassing a wide range of activities such as online grooming, sextortion, and cybersex trafficking.

Internet-Facilitated Trafficking:[26] This term underscores the role of the Internet as a facilitator of trafficking activities, including the use of social media, messaging apps, and online marketplaces to recruit and exploit victims.

Cybersex Trafficking: [27] Cybersex trafficking specifically refers to the exploitation of victims for sexual purposes through online platforms, including live streaming of sexual abuse and the production and distribution of child sexual abuse material (CSAM).[28]

Digital Slave Trade: [29] This term draws parallels to historical forms of slavery while highlighting the modern-day manifestations of exploitation facilitated by digital technologies and online networks.

Virtual Trafficking:[30] Virtual trafficking emphasizes the digital nature of exploitation, including

---

24 Council of Europe. Online trafficking in human beings Retrieved from https://www.coe.int/en/web/cyberviolence/trafficking-facilitated-by-ict

25 Sterner, G. Pursuing Offenders of Digital Exploitation on the Dark Web. Criminal Justice Research Center, Penn State Abington. Retrieved from https://www.porh.psu.edu/wp-content/uploads/General-Session-II-Glenn-Sterner-Penn-State-Abington.pdf

26 United Nations Office on Drugs and Crime (UNODC). (2022, May). Exploitation and abuse: the scale and scope of human trafficking in South Eastern Europe. Retrieved from https://www.unodc.org/documents/human-trafficking/Exploitation_and_Abuse.pdf

27 International Justice Mission. Cybersex trafficking FAQs. Retrieved from https://ijmstoragelive.blob.core.windows.net/ijmna/documents/IJM-Cybersex-Trafficking-FAQs.pdf

28 The Exodus Road. (2019, March 15). Cybersex trafficking: Grooming, exploitation, online. Retrieved from https://theexodusroad.com/cybersex-trafficking-grooming-exploitation-online/

29 Stoll, K. (2023, June 19). Human rights and the digital domain primer - Part 2. Retrieved from https://circleid.com/posts/20230619-human-rights-and-the-digital-domain-primer-part-2

30 Council of Europe Directorate General of Human Rights. (2003). The impact of the use of new information technologies on trafficking in human beings for the purpose of sexual exploitation: Final report of the Group of Specialists. Retrieved from https://rm.coe.int/0900001680928cab

the use of virtual reality, artificial intelligence, and deep fakes to manipulate and exploit victims online.[31]

Tech-Facilitated Exploitation: [32] Tech-facilitated exploitation encompasses a broad range of trafficking activities enabled by technology, including recruitment, coercion, and exploitation through digital means.

While the global definition of CEHT is still evolving, for the purpose of this report it is defined as follows:

> ***"CEHT encompasses the use of digital technologies and online platforms for the recruitment, transportation, transfer, harboring, or receipt of persons, by means of threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability, or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for exploitation, including sexual exploitation, forced labor, organ trafficking and other forms of servitude.***[33],[34]

Human trafficking in India is defined within the framework of international treaties and conventions aimed at combating trafficking in persons, such as the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children.[35] CEHT can be defined within the broader legal framework governing human trafficking and cyber-crimes. Section 143 of the Bharatiya Nayaya Sanhita (BNS) specifically addresses the trafficking of persons, prohibiting actions such as buying, selling, disposing, accepting, receiving, detaining, persuading, or inducing individuals for forced labor or sexual exploitation while the Information Technology Act, 2000,[36] addresses cyber-crimes, including those related to trafficking and exploitation online. At the time of writing this report, there is no definition of CEHT within the Indian law.

1.4 Reasons for the Shift including Contribution of Covid-19

The emergence and proliferation of CEHT represents a significant paradigm shift in the landscape of human exploitation, driven by a complex interplay of socioeconomic, technological, and global factors. Technological advancements, particularly the widespread adoption of digital platforms and the internet, which have fundamentally altered the dynamics of life have organically transcended into human trafficking. This has, in turn, provided traffickers with unprecedented

---

31 Sykiotou, A. P. (2017). Cyber trafficking: Recruiting victims of human trafficking through the net. Retrieved from http://crime-in-crisis.com/en/?p=363

32 Amerhauser, K. (2021). Commercial Sexual Exploitation of Children in the Western Balkans – Regional Vulnerabilities and Legal Responses. Retrieved from https://jied.lse.ac.uk/articles/10.31389/jied.102

33 Council of Europe, Supra note 16

34 Council of Europe. (2022, March). Online and technology-facilitated trafficking in human beings: Summary. G.R.E.T.A. (Group of Experts on Action against Trafficking in Human Beings). Retrieved from https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c

35 UN General Assembly, Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime, 15 November 2000, Retrieved from https://www.refworld.org/legal/agreements/unga/2000/en/23886

36 Government of India. (2000). Information Technology Act, 2000. Retrieved from https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

opportunities to exploit vulnerable individuals. Traffickers have understood the advantages of digital media and have seamlessly incorporated it into their realm. For instance, online classifieds, social media platforms, and messaging apps have become fertile grounds for traffickers to recruit and exploit victims. Cases abound where traffickers lure unsuspecting individuals into exploitative situations through false promises of employment or romantic relationships, only to subject them to forced labor or sexual exploitation.[37] Economic incentives play a pivotal role in driving the proliferation of CEHT, as traffickers capitalize on the demand for cheap labor and sexual services facilitated by digital platforms. Social vulnerabilities, including poverty, homelessness, and discrimination used to be the primary factors for trafficking.

Traffickers often target marginalized communities, such as migrant workers, refugees, and stateless persons, due to their heightened vulnerability and lack of access to support services. The process of recruitment remains the same with technology providing an extremely powerful tool to the trafficker. The anonymity provided by the internet and digital transactions has made it convenient for traffickers to conduct their illicit activities and has made it increasingly challenging for law enforcement agencies (LEAs) to track and disrupt these trafficking networks. Notable examples include cases where traffickers use encrypted messaging apps and Virtual Private Networks (VPNs) to evade detection while coordinating the trafficking of victims across multiple countries.[38]

The canvas of the vulnerable has expanded with the emergence of CEHT, as traffickers prey on individuals facing desperate circumstances who are not necessarily poor, uneducated, or socially backward. Educated people who are emotionally vulnerable when accessing the internet for their routine communication, socializing, etc. are also entrapped.

During the Covid-19 pandemic, economic instability and job losses have exacerbated vulnerabilities, making individuals more susceptible to exploitation. Lockdown measures and economic disruptions have left individuals more susceptible to exploitation and more exposed to cyberspace.[39] Traffickers have taken advantage of the economic downturn to recruit and exploit individuals facing financial hardships, offering false promises of employment or financial assistance through online platforms. Some reports have recorded that there was a 22 percent increase in online recruitment into trafficking schemes and reported the internet as the top recruitment location for all forms of trafficking. This trend is evident in the rise of online job scams, where individuals are lured into fraudulent job offers and subsequently trafficked for forced labor or sexual exploitation.[40] Studies reveal that social media usage of some platforms increased as much by 38 percent,[41] and with social media being one of the major recruiting processes for trafficking, CEHT increased significantly in this period.

---

37 UNODC. "The Role of Technology in Human Trafficking." UNODC, www.unodc.org/unodc/en/human-trafficking/Webstories2021/the-role-of-technology-in-human-trafficking.html.

38 Council of Europe, Supra note 16

39 ReportOUT. (2023) Not an Ideal Victim? Trafficking, Homelessness, and Risks Faced by LGBTQI+ Young People. A Global Scoping Report for the UN Special Rapporteur on Contemporary Forms of Slavery. Retrieved from: https://www.ohchr.org/sites/default/files/documents/issues/slavery/sr/reporthrc54/submission-slavery-hrc54-cso-reportout_0.pdf

40 Dela Luna, J. (2018). The Role of Economic Incentives in Child Exploitation and Human Trafficking in Thailand. University of Chicago Law School Chicago. Retrieved from https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1082&context=international_immersion_program_papers

41 Increased time spent on social by U.S. users during COVID-19 pandemic 2020 https://www.statista.com/statistics/1116148/more-time-spent-social-media-platforms-users-usa-coronavirus/

Lockdowns imposed during the pandemic made it difficult for traffickers to recruit using traditional processes that made them take to the internet.[42] Moreover, this was the time when a large section of the population had been socially isolated, physical interaction being negligible or non-existent, and digital access being the only window for human interaction. Exploring the internet at this time did play a significant role in making people vulnerable to trafficking even when these sections were not vulnerable to being trafficked otherwise.

1.5 Implications of CEHT

The implications of CEHT are profound and multifaceted, extending across various dimensions of human rights, socioeconomic development, and global security. Digital technologies facilitate immeasurable harm and significant humanitarian toll, inflicting exploitation, coercion, and abuse on victims. Victims of trafficking have always endured physical and psychological trauma and prolonged periods of exploitation in situations where their autonomy is stripped away. CEHT has multiplied manifold while simplifying traffickers' roles. Traffickers are exploiting both the physical and digital advantages they are gaining from the same act. For example, individuals who are coerced into performing sexual acts now additionally cater to online audiences. These individuals are compelled to engage in forced labor through remote work arrangements facilitated by online platforms. These forms of exploitation not only inflict immediate harm but also have long-term consequences for victims' physical and mental well-being.

In terms of global security, CEHT poses significant challenges due to its transnational nature and the complexity of trafficking networks operating across borders and jurisdictions. Traffickers exploit legal loopholes and jurisdictional challenges to evade detection and prosecution, complicating law enforcement efforts to combat trafficking networks effectively. For example, traffickers may exploit differences in legal frameworks and enforcement capacities between countries to traffic victims across borders, exploiting the lack of coordination and cooperation between LEAs. The exploitation of individuals for illicit purposes, such as forced labor, cyber-sex trafficking, and organ trafficking, threatens global stability and security by perpetuating cycles of violence and exploitation.

The long-term implications of CEHT extend beyond immediate humanitarian, socioeconomic, and global security concerns, impacting future generations and perpetuating intergenerational cycles of exploitation. In many cases of CEHT, especially in cases of sex trafficking, the creation of digital content of the abuse has also increased. This poses other challenges since the digital footprint is permanent and the victim can be haunted throughout their life. The normalization of online exploitation and the commodification of human beings pose ethical challenges for society, undermining fundamental principles of human dignity and equality. In addition to the immediate humanitarian, socioeconomic, and global security implications, CEHT also has broader societal and ethical ramifications that warrant consideration. As society becomes increasingly desensitized to online content and interactions, there is a risk of diminishing empathy and moral outrage towards victims of trafficking, perpetuating a cycle of indifference and inaction.

42 January Contreras, ACF Assistant Secretary and Katherine Chon, Director; Office on Trafficking in Persons, Technology's complicated relationship with Human Trafficking; Administration for Children and Families, July 2022, accessed on March 8, 2024

Traditional processes of trafficking involved physical interactions with the trafficker, where the trafficked had a face to associate with the crime. Penetration of CEHT has brought in nameless, faceless persons driving the trafficked, offering digital guidance, and earning through digital currency. Even though the exploitation has remained the same, technology is helping the trafficker remain anonymous.

Looking towards the future, the evolving nature of CEHT presents challenges and opportunities for prevention and intervention efforts. Trafficking operations that span across multiple countries and jurisdictions present obstacles for LEAs seeking to investigate and prosecute perpetrators. Addressing the long-term implications of CEHT requires holistic approaches that address the root causes of exploitation, including poverty, inequality, and social injustice, while also leveraging technological innovations to prevent and combat trafficking in the digital age. As traffickers adapt their tactics to exploit emerging technologies and online platforms, there is a need for innovative approaches to combat CEHT effectively using the same tool. To be able to achieve that, there is a dire need to understand the penetration of CEHT into the system. This includes leveraging technological advancements such as AI, Machine Learning (ML), and Data Analytics (DA) to identify patterns of trafficking activity, predict risk factors, and target interventions more effectively. This requires coordinated efforts across multiple sectors, including education, economic development, and social welfare. Investing in community-based prevention programs, empowering vulnerable populations with education and economic opportunities, and strengthening social support networks are essential strategies for reducing the prevalence of trafficking and protecting individuals from exploitation.

In summary, addressing the complex challenges posed by CEHT requires a national policy that highlights comprehensive and coordinated efforts at the local, national, and international levels, involving governments, LEAs, civil society organizations, and the private sector. By addressing the root causes of vulnerability, leveraging technological innovations, and prioritizing victim-centered approaches, we can work towards preventing and combating CEHT and protecting the rights and dignity of all individuals. To implement this in a sustained manner, a framework to address CEHT is imperative. The present National Action Research Study is attempting to do the same.

1.6 Organization of the Research Work

To be able to arrive at an understanding of a framework to address CEHT and develop a draft NPoA, the research undertook a multi-pronged exercise detailed in the methodology chapter. The study was conducted through an elaborate process of a review of literature, structured interviews in 15 workshops with over 365 law enforcement officers dealing with cases of human trafficking and cyber-crimes in 15 states across the country, validation investigations of selected forms of human trafficking, interactions with victims and a few selected civil society organizations. Data collection was done through focused group discussions (FGDs) with law enforcement officers in addition to actual data shared by the officers. Global experts and practitioners consulted reviewed the existing legislation and institutional frameworks, further bolstering the research. Global experts from six countries were consulted, and the detailed methodology of the research can be found in Chapter 3.

A significant process adapted from the research was conducted by a team of six domain experts, monitored and advised by a Principal Investigator. The team was responsible for preparing the

research tools and administering them. The domain experts jointly analyzed the data and wrote specific chapters of the report. The team greatly benefited from the constant input given by project stakeholders, in particular Shri Mahesh Muralidhar Bhagwat, IPS of Telangana State Police.

1.6.1 Research Partners

At the onset of the research, the organization forged a partnership with the Telangana State Police. The Crime Investigation Department (CID) with an attached cyber-crime police station was designated as the focal point for the research, making it critical for this partnership. The validation investigations and interactions with the victims that led to filing a criminal complaint were facilitated through this cyber-crime police station. Senior officers from CID also took part in the global consultations. After the team identified 15 states that would provide a fairly good representation of the country, partnerships were forged with the respective state police to facilitate smooth data collection. In many states, the State Police hosted data collection workshops within the Police Headquarters, providing valuable support for authentic data to be shared.

1.6.2 Monitoring Mechanism

All the tools used in the research were field-tested in the partner state of Telangana with extensive discussions with senior police officers and domain experts. Weekly reviews were conducted to assess progress and consolidate the learnings. All stakeholders connected were regularly updated on the progress of the research and their responses were sought for crucial decisions taken in connection with the project.

1.7 Structure of the Report

The report is presented in two sections. The first section includes:

- The analysis and interpretation of the primary data, and where the quantitative data has been suitably merged with the qualitative data received during the FGDs.
- Presentation of secondary data through a comprehensive review of international and national studies, along with reports available via open source.
- A Chapter that exclusively deals with the methodology including the tools, techniques and instruments of the research.
- A Chapter on the findings, conclusions, and recommendations that emerge from the study.

The second section of this report consists of:

- In-depth case studies conducted by the study team that emerged from the validation investigations and interactions with victims.
- A detailed description of specific forms of CEHT that have emerged during the study.
- The existing institutional framework provided by non-state partners.
- The gaps within the legal and institutional framework of the state, and its preparedness to respond to CEHT.
- Technology firms and their responses.
- International responses to combat CEHT.

1.8 Challenges Faced

Any research that is attempting to review a relatively unexplored terrain is bound to face challenges and the present study is no different. To begin with, CEHT is an evolving problem, with new trends rapidly surfacing across the globe. Interventions to address CEHT are still grappling with its spread and the pace with which the problem is growing. It was seen during the course of the research that frameworks to address CEHT were still being developed and many interventions were overlapping with interventions to address CSAM. CSAM can be one tiny variant of CEHT, and interventions that are attempting to address CSAM cannot assume that the same processes would be effective in addressing CEHT. Through the course of the research, this was one problem that continued to surface.

Besides the issue of grappling with a lack of common understanding of the subject, there were various administrative challenges that the team encountered. The research was dependent on cooperation from law enforcement across the country, as the police were the primary source for data collection. Law enforcement, besides being inundated with enormous responsibility in their discharge of duties, is also dealing with a varied range of cases with additional responsibility for law and order and special situations like the elections in some states. Human trafficking and cyber-crime are two separate units of law enforcement, and this research warranted a merger of the two. Since they are not merged administratively, there were challenges in capturing complete data. The research team encountered some excellent officers dealing with cyber-crime who had no knowledge of human trafficking and vice versa.

This was a challenge, in addition to the following:

a. Language Barriers: Language differences among participants posed challenges during data collection, potentially leading in some instances to misunderstandings or incomplete responses.

b. Varying Participant Numbers from Across States: Disparities in the number of participants across different states deterred the research team from understanding the real magnitude of the problem. While anecdotal references were indicating a large number of cases, there was no commensurate documentation available to support the same.

c. Challenges in Securing Dates for Data Collection: Difficulties in scheduling dates for data collection sessions may have impacted the timeliness and efficiency of the research.

The other challenges faced that are typical to India were:

a. Sampling Challenges: The regional division of states for sampling purposes may not fully capture the nuanced variations within each state.

b. Participant Bias: The study heavily relies on the insights and experiences of law enforcement professionals, potentially overlooking the perspectives of other key stakeholders such as technology experts who have unique insights into CEHT.

c. Data Validity and Reliability: The accuracy of self-reported data from questionnaires and FGDs is contingent on the participants' willingness to disclose information. In some states,

the presence of senior officers during the FGDs may have inhibited the junior officers from sharing information freely.

d. Limited Generalization: The findings may be context-specific to the selected states and may not be generalized across the country. The regional and cultural variations within India could pose challenges in extrapolating the results to a broader population.

e. Ethical Considerations in Validation Investigation: While the validation exercises and interactions with victims aimed to mirror real-world scenarios, ethical considerations, such as potential harm to unsuspecting individuals, was carefully addressed. However, we would like to flag the unpredictable nature of online interactions, which can pose challenges to fully controlling and mitigating ethical risks.

Despite the challenges, the team successfully completed data collection in 15 states within the limited time available. The report is an outcome of the data collection, interaction with global experts, interaction with national experts, desk review of global initiatives, interactions with victims and the cases that came to be filed as part of the research. The findings of the research have culminated into the drafting of the NPoA to address CEHT for India.

Chapter

02

Review of Literature

Chapter 2

Review of Literature

2.1 Introduction

Our rationale to carry out an in-depth and comprehensive review of the literature was based entirely on the nature and scope of the Action Research as outlined in the Introduction. The primary focus was to understand the knowledge and information that currently exists and thus augment the Action Research. To enable this, we garnered secondary data sources and reports, globally and nationally, and confirmed that there was no duplication of efforts and resources, and thereby enriched the global and national understanding of CEHT. The second objective of this review was also to identify the gaps in knowledge and practice that would need to be taken further and addressed by the Action Research.

The literature review process was conducted under the expertise of the Principal Investigator and entailed a comprehensive examination of a substantial pool of over 50 documents encompassing reports, research papers, policy documents, and action plans relevant to CEHT. The final selection of the six reports for this literature review was based on the assessment of the quality, content, and relevance of the sources. Certain factors were kept in mind, such as the credibility of sources, methodology used to carry out the study, the context in which they were written, the time period and geographical coverage, and its relevance in the current context, within the purview of the objectives of the Action Research.

During this process one of the significant gaps that emerged, which this Action Research will seek to address, was that the focus of the reports was primarily centered on issues related to cyber safety and cyber-crimes primarily against women and children, and very few of the reports dealt directly with CEHT. Furthermore, none of the reviewed reports clearly defined or explicitly used the term CEHT. Nonetheless, the six selected literature provide distinctive and nuanced exploration of the complex dynamics inherent in the intersection of cyber technologies and human trafficking.

Against this backdrop, the following documents reviewed contributed to this Action Research:

I. Online and Technology-Facilitated Trafficking in Human Beings, *Group of Experts on Action against Trafficking in Human Beings (GRETA), 2022*

II. How Technology Fuels Trafficking and Exploitation in the Asia and the Pacific, *Mekong Club, 2018*

III. Changing Trends in Online Abuse and Trafficking of Women and Children, *Space2Grow and Cyber Peace Foundation, 2022*

IV. Using Technology in Human Trafficking: International Law Perspective and Reflections within Middle Eastern Countries, *Yaser Khalaileh and Nazzal Kisswani, 2015*

V. The Cyberworld and Human Trafficking: A Double-Edged Sword, *Bridget Dukes, Cybersecurity Undergraduates Research Project, Old Dominion University, USA,2020*

VI. Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children's Cases, U*niversity of Nottingham Rights Lab and Global Fund to End Modern Slavery, 2023*

The broad parameters adopted to review the selected literature, in line with the objectives of the Action Research, are:

1. Conceptualizing CEHT
2. Usage of Cyber Technology in the process of Human Trafficking
3. Technological Firms as Enablers
4. Legal Framework to tackle CEHT
5. Solutions and Responses to Combat CEHT

2.2 Review of Literature

2.2.1 Conceptualizing CEHT

This segment reviewed the literature to understand how it has conceptualized CEHT from the perspective of:

(1) Defining the term
(2) The specific trends and patterns mentioned, indicating the magnitude of the crime
(3) The various vulnerability factors that perpetuate this crime

2.2.2 Definition of CEHT

Of the six studies reviewed, it is important to state at the outset that "CEHT" was not expressly defined or explained in any of the studies. The report titled ***"How Technology Fuels Trafficking and Exploitation in the Asia and the Pacific, Mekong Club, 2018,"*** [43] limited itself to defining technology as, *"Information and communication technologies, particularly those constituting digital and networked environments. Technologies that allow users to exchange digital information over networks include the Internet, online social networks, and mobile phones."*

43 The Mekong Club is an anti-slavery non-profit with a focus on business engagement. Since its inception in 2012, the vision of the Mekong Club is to harness the power of the private sector to change business practices in a way that will significantly reduce modern slavery. Its founders and current board members are representatives of the private sector who understand the key role companies can play in this fight.

The report titled ***"Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children Cases, 2023,"*** [44] mainly focused in the Philippines, referred to the Online Sexual Exploitation of Children (OSEC) as, *"a complex hidden crime that is particularly challenging for the global community to measure and address."*

2.3 Trends and Patterns

In the absence of a definition of CEHT, the review focused on the scope and magnitude of the crime of CEHT across different countries and regions. The reports reviewed broadly looked at Asia, Pacific, Europe and the United States of America.

While seeking to understand the penetration of CEHT in **India**, a study was undertaken by Space2Grow[45] and CyberPeace Foundation,[46] titled ***"Changing Trends in Online Abuse and Trafficking of Women and Children, 2022."*** It is important to note that although the report's title mentions the trafficking of women and children, the content primarily focuses on cyber-crimes and internet usage among men and women, with a particular emphasis on different age groups. A descriptive and exploratory approach was employed in the research design, with personal interviews conducted in selected districts of four states i.e. Jharkhand, Madhya Pradesh, Rajasthan, and West Bengal. Chosen states served as source and/or transit hubs for human trafficking, witnessing increased mobile and internet technology adoption, and had available data on cyber-crimes.

The report highlighted a 61 per cent increase in the number of female active internet users, 24 per cent increase in the number of male active internet users, 45 per cent growth in the internet users from rural areas, and 28 per cent increase among the urban users since 2019. It also reported that India has 646 million active internet users aged two years and above as of December 2021. Among them, 592 million are aged 12 years and above with an increase of 37 per cent from 2019. These statistics reflected the magnitude of internet penetration in the everyday lives of people belonging to different age groups and gender across diverse geographical locations.

The study reported that India has the second largest user base of Facebook next to the United States. There is a stark gender divide in the social media space, as only 33 per cent women access social media against 67 per cent of men in 2019. Digital empowerment, while positive, raised concerns about safety, evident in the rise of cyber-crimes during the Covid-2019 pandemic, despite a decline in reported crimes. The report delved into social media usage, exposing widespread engagement, especially among the 13-18 age group, and highlighted the prevalence of cyber fraud and abuse, including phishing, cyber-bullying, identity theft, and exposure to inappropriate content. Cyber-bullying affected a significant portion of participants, and identity theft was notably prevalent among the 13-18 age groups.

---

44 University of Nottingham Rights Lab and Global Fund to End Modern Slavery

45 Space2Grow, is a social impact consulting firm founded with a belief that the role of nonprofits, social startups and community-based organization in addressing socio-economic issues is a key to create last mile impact.

46 CyberPeace Foundation is an Indian nonpartisan, Nonprofit organization of Cyber Security that works to build Resilience against Cyberattack and Cybercrimes. CyberPeace closely works with several state and national governments, Educational Institutions worldwide and United Nations.

The report also noted that children have increasingly adopted the internet in recent times. According to UNICEF estimates from 2016, one-third of internet users worldwide are children. Additionally, statistics from the International Telecommunication Union (ITU) in 2017 indicate that the 15-24 age groups are leading in internet adoption.

The report titled ***"How Technology Fuels Trafficking and Exploitation in the Asia and the Pacific, Mekong Club, 2018,"*** focused on bringing out the scope and magnitude of human trafficking in Asia and the Pacific region. It highlighted that the total number of modern slavery victims in the world is estimated to be 40.3 million, of which more than half of the victims - at least 24.9 million - are in **Asia** and the **Pacific**. This region also accounted for the highest number of victims across all forms of modern slavery, 73 percent of victims were forced into sexual exploitation, 68 percent were under state imposed forced labor, 64 percent were exploited related to the private economy, and 42 percent were in forced marriages (Global Slavery Index [GSI], 2018).[47] Asia and the Pacific is also an origin of trafficking outside of the region and as per the United Nations Office on Drugs and Crime's 2018 data, 36 percent of trafficking victims detected outside their region of origin come from Asia and the Pacific (United Nations Office on Drugs and Crime [UNODC], 2018). [48]

These two reports indicated that despite a huge accessibility divide between rural and urban areas, Asia now accounts for half of the total internet usage globally. In India, Indonesia and Philippines there are 560 million, 143 million and 67 million internet users respectively (Internet World Stats, 2019).[49] Social media penetration is also very high whereby 92 percent of Filipinos and 88 percent of South Koreans who have access to the internet also have a Facebook account. In China, WeChat (the "local version" of Facebook) has 612 million daily users and an 85.5 percent penetration rate.

The report titled ***"Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children Cases, 2023,"***[50] primarily focused on OSEC in the Philippines. Recent reports found OSEC continues to grow, with a dramatic increase noted during the Covid-19 pandemic. The research revealed that the content providers of OSEC material are often relatives of the victim or known to the family and the content receivers are from North America, EU Countries, and Australia. In 2019, IWF[51] identified 288 dark websites selling materials related to OSEC, 197 of which only accept payment in virtual currencies. The same year, Chainalysis[52] tracked almost $930,000 worth of payments made via Bitcoin and Ethereum to addresses associated with OSEC providers, representing a 32 percent increase over 2018 and 212 percent increase over 2017.

47 The Global Slavery Index is a global study of modern slavery published by the Minderoo Foundation's Walk Free initiative.

48 UNODC is a global leader in the fight against illicit drugs and international crime and produces global reports on trafficking in persons, provides technical assistance and guidance to countries, and supports partnerships and initiatives to combat this crime.

49 Internet World Stats is a useful source for country and regional stats (statistics), international online market research, the latest Internet information, world Internet penetration data, world population statistics, telecommunications information reports, and Facebook Stats by country.

50 University of Nottingham Rights Lab and Global Fund to End Modern Slavery

51 The Internet Watch Foundation (IWF) is a global registered charity based in Cambridge, England. It states that its remit is "to minimise the availability of online sexual abuse content, specifically child sexual abuse images and videos hosted anywhere in the world and non-photographic child sexual abuse images hosted in the UK.»

52 Chainalysis is an American blockchain analysis firm headquartered in New York City and is the first start-up company dedicated to the business of Bitcoin tracing. It offers compliance and investigation software to analyse the blockchain public ledger, which is primarily used to track virtual currencies.

Although the report does not directly address CEHT, it is understood that one of the most rampant forms of exploitation facilitated by technology is OSEC, which can be interpreted as child trafficking.

The report titled ***"Using Technology in Human Trafficking: International Law Perspective and Reflections within Middle Eastern Countries, 2015,"*** [54] referenced data from the ILO in 2008. The report stated that approximately 12.3 million people were working as forced laborers who were trafficked both domestically and internationally. It also emphasized that most of these crimes were facilitated using the internet. Furthermore, the ILO estimated that 2–14 percent of the national income for some countries like Indonesia, the Philippines, Malaysia, and Thailand was yielded from sex tourism.

The report, ***"Online and Technology-Facilitated Trafficking in Human Beings, 2022",*** authored by GRETA,[53] delved into the harsh realities of online trafficking, portraying a disturbing picture of the online underworld where seemingly innocuous platforms transform into instruments of manipulation and control. The report highlighted that online platforms and technologies are increasingly used to facilitate all forms of human trafficking, including forced labor, sexual exploitation, and organ trafficking.

The contributors to this Report included 40 States Parties to the Council of Europe Convention on Action against Trafficking in Human Beings, 12 Non-Governmental Organizations (NGOs) and 2 Information Technology (IT) companies (limited input was provided from technology companies regarding their efforts and challenges in combating online trafficking).

While the report's primary focus was on the experiences and trends observed in the member states of the Council of Europe, which currently includes 47 countries, nonetheless, the information and recommendations presented in the report are relevant and applicable to a wider global context due to the increasingly interconnected nature of online platforms and technologies used for trafficking.

The report titled ***"The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,"*** focused on the United States, referred to the Polaris Project,[54] which in its report published in 2019, identified 22,326 victims and survivors of human trafficking in the United States. Of these, 14,597 (almost two thirds) were of sex trafficking. Though the demographic profile of the victims is largely unknown, the trends from those that are known indicate that a high number of cases include minors, females, and foreign nationals. It further identified 11,500 trafficking situations and 4,384 traffickers. Comparatively, the earlier Polaris report (2014) had identified 5042 human trafficking cases, including 3,598 cases of sex trafficking. The numbers indicate a steep multi-fold rise in human trafficking as well as sex trafficking cases from 2014 to 2019. Furthermore, the presented data reflected only the reported/ detected cases, whereas a large number of cases are either never reported or discovered.

---

53 The Group of Experts on Action against Trafficking in Human Beings, more commonly known as GRETA, is the monitoring mechanism on human trafficking established by the Council of Europe Convention on Action against Trafficking in Human Beings.

54 Polaris is a non-profit non-governmental organization that works to combat and prevent sex and labour trafficking in North America.

2.4 Vulnerability Factors

A related component of the review was the vulnerability factors that contribute to CEHT as revealed in the reports.

The report, "***Changing Trends in Online Abuse and Trafficking of Women and Children, 2022***", with its focus on India, showed that poor education and digital literacy, especially in rural areas, led to under-reporting and self-censorship in internet usage. The qualitative insights revealed the disproportionate vulnerability faced by women, particularly concerning online shaming and humiliation. The findings underscored the importance of fostering open communication between parents, caregivers, and children to navigate the complexities of internet usage. This study also shed light on the challenges faced by teachers, who often lack awareness and involvement in students' online activities. The study accentuated the vulnerability of women and the reluctance to report due to procedural hassles, emphasizing the need for cultural shifts and efficient redressal mechanisms.

The report titled "***Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children Cases*, 2023,"** stated that financially motivated OSEC cases mostly occurred in communities that are suffering from extreme poverty or destitution. Recent studies found that children are sexually abused by their parents and close relatives motivated for economic gain. Although the monetary rewards from OSEC cases are relatively small, yet they are much larger than a day or weeks' worth of the Philippine minimum wage, which makes it an attractive proposition for facilitators and traffickers. According to the World Bank Group, 16.7 percent of the population of the Philippines was living below the national poverty line in 2018.

Similarly, the report titled "***How Technology Fuels Trafficking and Exploitation in the Asia and the Pacific, Mekong Club, 2018,"*** highlighted that the business was usually handled by the victims' neighbours, relatives and sometimes even their impoverished parents. They usually get between 10 and 100 dollars per "show", a big amount in a country where about 60 percent of the population earns only two dollars a day.

The report also highlighted another dimension, the supply chain of human beings. In 2017, there were 62 million international migrants in Asia and the Pacific and more than 100 million migrants around the globe were from countries within the region. The majority of them moved in search of better economic opportunities. Most cases of debt bondage and trafficking happen at some point during this process, sometimes trapping the victims in a situation of slavery even before they leave their homes. While traditional recruitment channels are still widely used, with the internet now being vastly accessible, more and more migrant workers are going online to seek information on job opportunities abroad. For example, the report referred to a popular Filipino website called workabroad.ph containing 25,000 overseas job posts that attracted more than 700,000 Facebook likes as of May 2019.

The report, "***Online and Technology-Facilitated Trafficking in Human Beings, 2022***", authored by GRETA, highlighted key vulnerabilities that make individuals susceptible to online trafficking. These vulnerabilities are not mutually exclusive and can often overlap with traffickers exploiting a combination of factors to target and manipulate individuals.

Personal vulnerabilities:

- Financial hardship: The individuals experiencing poverty or debt are more likely to be lured by promises of quick money or employment opportunities, even if they seem unrealistic.
- Social isolation or lack of support: The individuals who feel lonely, disconnected, or lack strong social networks, are more susceptible to manipulation and exploitation by traffickers online.
- Mental health challenges or trauma: The individuals experiencing depression, anxiety, or past trauma may be more vulnerable to manipulation and control tactics used by traffickers.
- Limited digital literacy or awareness: The individuals with limited understanding of online platforms and technologies may not be aware of the risks and dangers associated with interacting with strangers online.

Specific demographic vulnerabilities:

- Children and adolescents: Children and adolescents are particularly vulnerable due to their poor understanding of online risks, increased reliance on technology, and potential lack of parental supervision.
- Migrants and refugees: Individuals who are displaced or living in unfamiliar environments may be more susceptible to exploitation due to their lack of support networks and legal documentation.
- Individuals from marginalized communities: Individuals facing discrimination or social exclusion may be more likely to fall prey to traffickers who offer false promises of acceptance or belonging.

Technology-related vulnerabilities:

- Sharing personal information online: Oversharing personal details on social media platforms or online profiles can make individuals easier to target and exploit.
- Falling for scams or deceptive practices: The individuals who are easily lured by online offers or promises of quick success may be more susceptible to manipulation and recruitment tactics.
- Lack of cyber security awareness: Weak passwords, unsecured devices, and lack of understanding of online privacy settings can make individuals vulnerable to data breaches and online stalking.

The report titled "***The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,***" focused on the United States, found that the targets are often minors, females, and foreign nationals. Traffickers tend to seek those who show signs of substance abuse issues, destabilization within the home and peer group (i.e. emotional and physical isolation from friends and family), domestic violence, nomadic tendencies, runaway behaviour, and social discrimination and separation. That said, the tactics used to entice and recruit victims are similar for each of these populations. Sex traffickers mainly utilize two different types of deception and coercion to draw in victims after tirelessly working to form online bonds, friendships, and relationships with them. They go through a deliberate process to identify the suitable target and tactic to gain their trust and confidence. The

first grooming technique commonly involved traffickers using a word of honour and the assurance of love, romance, affection, and a lifetime of appealing guarantees, gifts, and protection. The second grooming technique involved traffickers making promises for successful jobs and work promises. Both techniques require manipulation, control, lying, and subterfuge on the trafficker's part, and innocence and naïveté on the victim's part.

The reviewed literature illustrates that in the digital realm, human trafficking has adapted to exploitation via online spaces, social media, and communication apps under the new terminology of CEHT, which involves using technology and online platforms for various aspects of human trafficking, including recruitment, communication, and financial transactions.

2.5 Usage of Cyber Technology in the Process of Human Trafficking

The literature was reviewed to understand how cyber technology was used in the process of human trafficking.

1. The current use of technology to facilitate human trafficking
2. Challenges in using technology as a tool to combat crime

2.5.1 Usage Of Cyber Technologies in Carrying out the Crime of Human Trafficking

In the pursuit of understanding the tools utilized for exploitation and the impact of technology on human trafficking, a study conducted in India, titled "**Changing Trends in Online Abuse and Trafficking of Women and Children, 2022**," brings to light the online experiences of girls and women. The data based on the total number of 749 participants, provides valuable insights into this critical issue. The findings indicated widespread engagement on social media platforms like Facebook (87 percent), Instagram (59.60 percent), and Twitter (17.07 percent). Participants reported facing significant challenges, including phishing incidents (73 percent), discomfort in online interactions (57.14 percent), and cyber-bullying (33.48 percent). Disturbingly, 44.59 percent experienced online stalking, but only 12.08 percent reported it, drawing attention to the common experience of under-reporting of such crimes.

The research authored by the Mekong Club titled "***How Technology Fuels Trafficking and Exploitation in the Asia and the Pacific, 2018,"*** focused extensively on how cyber technologies are being used to facilitate human trafficking, in Asia and the Pacific region.

The identification of different forms of exploitation aided by technology, are as follows:

a) **Commercial sexual exploitation,** in particular cyber-sex, is aided by technology. Traffickers recruit victims using websites and apps designed for dating, escort services, job advertising, gaming and social media. For example, in Vietnam, traffickers posed as police officers on social media or established online dating relationships to lure sex trafficking victims and gain their trust. In another case, perpetrators have recruited girls through job service centers and then sold them to sex trafficking gangs based in China and Malaysia.

b) **Misuse of Technology to exploit children for sex**, according to an NGO's research, 95 percent of commercial sexual exploitation of children in South Korea is arranged over the

internet. Globally, the majority of CSAM is exchanged via non-commercial channels such as public peer-to-peer platforms like Gnutella, eDonkey and eMule. Mid-level offenders often use private peer-to-peer networks to establish closed groups and exchange encrypted files.

c) The internet is also used to traffic and trade children in the **adoption black market**. In February 2014, Chinese authorities rescued over 300 babies and arrested more than 1,000 people suspected of buying and selling young children online. This followed a six-month operation in which authorities were made aware of a website promoting private adoptions.

d) Another emerging trend was that of Technology enabling **voluntourism**. This is a fast-growing part of the adventure travel market, often advertised and booked online, for people who want to do good in the world and volunteer their time to charitable causes - often in orphanages. The term "orphanages" is misleading. Research shows that 80 percent of all children in institutional care have one or both parents alive.

e) Another less spoken form of CEHT is **labor exploitation**. In 2017, there were 62 million international migrants in Asia and the Pacific and more than 100 million migrants around the globe were from countries within the region. Most cases of debt bondage and trafficking happen at some point during this process, sometimes trapping the victims in a situation of slavery even before they leave their homes. While traditional recruitment channels are still widely used, with the internet now being vastly accessible, more and more migrant workers are going online to seek information on job opportunities abroad. Vietnamese organised crime networks recruit Vietnamese adults and children under the pretence of lucrative job opportunities and transport them to Europe - particularly the United Kingdom - and subject them to forced labor on cannabis farms. Smartphone apps are increasingly being used to lure and recruit people from Indonesia, Philippines, Thailand, Vietnam, China and Cambodia into exploitative labor situations in Taiwan, which hosts more than 675,000 foreign workers who perform low-skilled work such as home caregivers and domestic workers, or in farming, manufacturing, construction, and fishing.

The report titled "***Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children Cases*, 2023,"** highlighted how offenders benefit from technology to disguise OSEC, using internet-enabled mobile devices, anonymization and encryption tools, new payment methods, and the Darknet to continue their activities online without disruption by law enforcement. Online payment services, money transfer services, and local payment centers are the most common payment methods in relation to live streaming of child sexual abuse.

The GRETA report titled "***Online and Technology-Facilitated Trafficking in Human Beings, 2022,***" noted that the "impact of technology on trafficking of human beings is of particular concern during two stages of the trafficking process: recruitment and exploitation".

Social Media and Dating Apps:

Recruitment: Platforms like Facebook, Instagram, and Tinder are used to find and target potential victims, often exploiting their vulnerabilities like financial hardship or loneliness.

Communication and Control: Traffickers can use chat features and direct messaging to maintain contact with victims, monitor their activities, and exert control.

Job Boards and Classifieds:

Recruitment: Platforms like Indeed, Craigslist, and LinkedIn can be used to lure victims with false promises of employment opportunities.

Filtering and Targeting:

Advanced search features and algorithms can be used to target specific demographics and vulnerabilities, making it easier for traffickers to connect with potential victims.

Live Streaming Platforms:

*Exploitation***:** Traffickers can exploit platforms like Twitch and OnlyFans for forced labor, particularly in the context of sexual exploitation.

Control and Monitoring: Live streaming features can be used to monitor victims and enforce compliance, often with threats and blackmail tactics.

Dark Web and Encrypted Messaging:

Communication and Coordination: Traffickers can use platforms like Tor and Telegram to communicate securely and anonymously, making them difficult to track.

Organizing and Planning: The dark web can be used for illegal marketplaces and forums where traffickers can share information, recruit accomplices, and plan activities.

Mobile Technologies and Spyware:

GPS Tracking: Traffickers can use apps and spyware tools to track victims' movements, monitor their activities, and restrict their freedom.

Financial Control: Mobile banking apps and online payment platforms can be used to exploit victims financially and control their access to resources.

Crypto currencies:

Financial Transactions: Traffickers can leverage crypto currencies like Bitcoin and Monero for anonymous and untraceable transactions, making it difficult to track their financial activities and hold them accountable.

Evasion and Laundering: Crypto currencies can be used to launder proceeds from trafficking activities, further hindering law enforcement efforts.

In the context of the United States, the report titled "**The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,**" focused on the use of cyber technology by traffickers to identify, groom, and exploit victims. It also examined how traffickers use technology to contact buyers illegally. The report also highlighted the role of LEAs in using technology to detect these crimes, stop them, rescue victims, and bring traffickers to justice. This study broadly classified human trafficking into two forms i.e. sex trafficking and labor trafficking, but restricted itself to focus on mainly sex trafficking.

The report further discussed certain measures for the LEAs and investigators to identify advertisements related to sex trafficking. Typical keywords and emojis used in advertisements are

tell-tale signs to the investigators if the advertisement is to target the victims or contact the buyers. Also, if the image is blurred, it may indicate that it is likely that a child is being advertised. The appearance of identical advertisements with the same images but different names or descriptions across various platforms, listing different cities, states, or even countries where the services are offered, likely indicates the movement of victims. Often, the contact information in these various advertisements remains the same.

2.5.2 Challenges in Targeting Technology as a Criminal Response

A key challenge faced by LEAs is in the identification and tracking of criminals in the cyber space domain. Drawing attention to such challenges, the report titled "***The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,***" stated that there are digital footprints which may be investigated later; however, a cybercriminal can easily erase or manipulate these footprints, making it difficult for the law enforcement to investigate and identify the traffickers or the victim.

Against this backdrop, some of the key challenges highlighted in this review are:

The report titled "***Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children (OSEC) Cases*, 2023,"** highlighted that as advances in technology create serious challenges for investigation and prosecution efforts, it has become easier for offenders to engage in OSEC. Offenders benefit from technology to disguise OSEC, use internet-enabled mobile devices, anonymization and encryption tools, and new payment methods, to continue their activities online without disruption from law enforcement. Perpetrators of OSEC use different payment methods to facilitate their crimes without detection by law enforcement. Online payment services, money transfer services, and local payment centers are the most common payment methods in relation to live streaming of child sexual abuse. Traffickers leverage crypto currencies like Bitcoin and Monero for anonymous and untraceable transactions, making it difficult to track their financial activities and hold them accountable.

The report titled "***The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,"*** stated that technology today facilitates online interaction with the commercial sex actors through webcam, live streaming, and online chat rooms. Webcam sex can facilitate transnational exploitation. The live streaming of sexual acts can potentially escape blockers and censors and is often subjected to limited surveillance. While law enforcement may crackdown on a particular platform that facilitates human trafficking, the blockade to the traffickers and the buyers is temporary as they soon move onto other platforms. For example, after shutting down of Backpage that was used for posting classified advertisements for the buyers, the traffickers and buyers have moved on and use platforms such as escortindex.com, escortfish.ch and skipthegames.eu.

The study titled **"*How Technology Fuels Trafficking and Exploitation in the Asia and the Pacific, Mekong Club, 2018,***" highlighted that in the Philippines, tens of thousands of children are victims of webcam sex tourism. They are forced to perform sexual acts for foreign customers who watch from the comfort of their homes in their own countries. The videos are broadcast live. There is no need for high-speed internet - a simple phone or an internet cafe is enough. Since credit card payments are known by most offenders to risk identification, new and therefore, more valuable is the abuse material that has itself become a sort of currency often being used as "payment" for access to other material.

As is evident from the studies reviewed, the internet is providing global reach and is largely an unregulated space, thereby being susceptible for abuse by human traffickers for usage to target and victimize vulnerable people for various forms of exploitation.

2.6 Technological Firms as Enablers

In an endeavour to understand whether technology by design plays an enabling role, the selected literature was reviewed to understand how different countries have responded to this aspect and how accountability on tech firms has been enforced.

The report titled "***The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,***" discussed the role of one such tech company and action taken by the law enforcement to hold it accountable, resulting in its eventual shut down. In April of 2018, the United States Department of Justice seized and shut down Backpage.com**,** an advertisement website which covertly doubled as a buy and sell marketplace for sexual exploitation and trafficking. By censoring keywords and programming an electronic filter to delete lexicon relating to trafficking schemes, Backpage initiated participation and contribution. Backpage filtered words and phrases that could potentially indicate the trafficking of children for illegal sex purposes, including "Lolita," "teenage," "amber alert," and "schoolgirl." Previously, Section 230 of the Communications Decency Act permitted this activity, awarding immunity to Internet Service Providers like Backpage. Eventually, its complicity became obvious and grounds for prosecution.

The report "***Using Technology in Human Trafficking: International Law Perspective and Reflections within Middle Eastern Countries, 2015***" emphasized that on March 5, 2009, Thomas Dart, President of the Illinois State Police, took federal action against the owners of "Craigslist," a major online company facilitating the sex trade, particularly the trafficking of women and children through its porn websites. This company's activities led to the police spending US$ 100,000 to combat street prostitution, pimping, and human trafficking, resulting in a case seeking compensation for those costs. Despite the successful conclusion of this case, against one of the major companies in the business of prostitution and human trafficking, 'Craigslist' is only the tip of the iceberg of similar companies that do most of their business through the internet via chatroom pornography with girls paid for sex over the internet. The importance of the outcome of this case lies in the fact that, it was contrary to the provisions of the judicial precedents in the United States. The U.S. policy of freedom to use the internet has had the support of the U.S. Congress in its necessity to maintain an open market competition policy and commerce via the internet, but simultaneously encourage the fight against human trafficking.

Understanding the role of technological firms in aiding and abetting the crime of CEHT is critical to developing safeguards and solutions in the cyber arena and building accountability of the technology firms. The review of the studies highlighted cases from the United States where it is noteworthy that successful action was taken against Tech Platforms, leading the way for other countries to adopt similar measures.

2.7 Legal Framework to Tackle CEHT

A critical component of the review is to explore the existing legal landscape and legal developments, if any, to counter the new and evolving crime of CEHT. This is being done against the backdrop of the understanding that we appear to be in a nascent stage of understanding and developing adequate responses at the global and national levels, and legal frameworks are in the process of evolving to adequately respond to these emerging challenges posed by cyber technologies in facilitating and commissioning the crimes of CEHT.

Against this backdrop, this section focused on:

1. International Instruments and Existing Legal Framework
2. Provisions for holding technology enablers accountable and addressing challenges in application

2.7.1 International Instruments and Existing Legal Framework

The study titled ***"Using Technology in Human Trafficking: International Law Perspective and Reflections within Middle Eastern Countries, 2015,"***[55] started with the premise that human trafficking represents a serious violation of human rights, dignity and freedom. The United Nations, as well as the European Union and the European Council, have all strived to develop a series of documents that may now be considered as an undeniable reference in the criminalisation of human trafficking. The Convention of the Council of Europe in the fight against trafficking in human beings of 2005 developed the most important principles in criminalising human trafficking. The adoption of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially in Women and Children of 2000, additional to the United Nations Convention against Transnational Organized Crime of 2000, was the first long-awaited outcome of the international community endeavor in this respect. It further aimed at analyzing the possible effectiveness of these contributions in light of the challenges that may face the work of such organizations, to include mainly the fact that human trafficking is now widely operated through the use of internet and other means of technology. Highlighting the existing gaps, it stated that the extent of trusting statistical information provided by states about human trafficking via the internet places a serious problem. Also, the limited scope of the rules of international law governing the issue of human trafficking via electronic means is just another problem. Therefore, the sufficiency of this legal system to create the desired change in the national legal policies of states is doubtful, and the Middle East countries are no exception.

2.7.2 International Efforts in Fighting Human Trafficking via the Internet

The following listed efforts are international initiatives being made to fight trafficking via the Internet:

---

55 Yaser Khalaileh is an Associate Professor and attained his PhD in Public International Law from the University of West of England, and LLM from Bristol University. He is now an Associate Professor of International Law at the College of Law, Qatar University.

Nazzal Kisswani is an Assistant Professor of Law and attained his PhD in Business Law from Macquarie University, and a master's in international Trade and Commerce law. He is an Assistant Professor of Business Law at the College of Law, Qatar University.

1. *The Group of Eight (G8)*

   Ministers from the eight major industrialized nations, the G8, were in agreement on a plan to fight international computer crime. Interior and Justice Ministers of Britain, Canada, France, Germany, Italy, Japan, Russia and the United States expressed their views in strong terms. The main idea professed was that criminals were no longer restricted by national boundaries and all countries had to act together if they wanted to combat cyber-crime. The main recommendations of the G8 on computer-related crimes may be summarized to include the criminalization of internet based human trafficking; addressing problems of judicial investigations through effective training; promoting international cooperation in taking deterrent steps to prevent high-tech crime; the involvement of industrial sector in the fight against trafficking; enacting and implementing laws to ensure the appropriate protection of intellectual property rights against counterfeiting and piracy; public awareness of high-tech crime; and appropriate capacity building for investigating and prosecuting criminals.

2. *United Nations General Assembly*

   The United Nations issued several decisions concerning the safety in using technology and the internet and declared standards for the desired protection.

   - Resolution 45/121 of 1990 on crime prevention, as well as publishing a guide to prevent and combat crimes related to computers in 1994.
   - Resolution 55/63 of 4th December 2000 and 56/121 of 19th December 2001 on combating the criminal misuse of information technologies.
   - Resolution 57/239 on 20th December 2002 on creating a global culture of cyber security.
   - Resolution CCPCJ 16/2/07 of April 2007 on the effective prevention of crime and criminal justice to fight the sexual exploitation of children.

3. *The International Telecommunication Union (ITU)*

   The ITU comprises 192 countries and 700 companies from the private sector in addition to academic institutions. This Union is an important center for cooperation amongst the members for being one of the UN specialized agencies, devoted to helping state governments and industries once they agree on specific common principles or an entire agreement.

4. *Human trafficking via the internet in international conventions*

   These conventions are the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially in Women and Children of 2000; the CyberCrime Convention of 2001; the ILO Convention on the Worst Forms of Child Labor of 1999; and the Inter-American Cooperation Portal on CyberCrime of 1999.

5. *The Protocol to Prevent, Suppress and Punish Human Trafficking of 2000*

   It may be noted that this Protocol failed to address fighting human trafficking in children and women particularly through the use of technology, as one of the fastest growing types of crimes prevalent online. This is despite the EU's belief that the definition of trafficking contained in the Protocol covers all types of trafficking, even those made over the internet.

6. *The Council of Europe Convention on Cyber-Crime*

   This Convention is an international treaty that aimed at achieving harmonization of member states national laws on cyber-crime and seeks to improve the national capabilities

in investigating related crimes and attempts to provide for the cooperation necessary on investigations. As such, this Convention obliges member states to incorporate related laws in a way to allow effective enforcement; to search and seize computers and to access computer data; to engage in interception; and to obtain real-time and stored communications data, whether or not the crime under investigation is a cyber-crime.

7. *The Inter-American Cooperation Portal on Cyber-Crime of 1999*
   This initiative arose in recognition of the spread and potential magnitude of cyber-crime for Organization of American States (OAS) member states, with responsibility for: completing a diagnosis of criminal activity which targets computers and information, or which uses computers as the means of committing an offense; completing a diagnosis of national legislation, policies and practices regarding such activity; identifying national and international entities with relevant expertise; and identifying mechanisms of cooperation within the Inter-American system to combat cyber-crime.

8. *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981*
   Convention 108 of 1981 divided into seven chapters includes general provisions and the basic principles for data protection and the transmission of information outside the members state's borders, as well as the mutual cooperation required between them.

9. *The Arab Convention on Combating Information Technology Offences of 2012*
   The League of Arab States Convention on combating information technology crimes was one important regional effort in recent years to drum up the necessary security measures to fight crimes in all its forms and manifestations, including information technology crimes, by creating foundations and legal environment.

2.7.3 Arab Legislations Relating to Human Trafficking Via the Internet

Saudi Arabia

In comparison to the number of internet users, Saudi Arabia was one of the first ten states that suffered from electronic spams being initiated on its territory. Accordingly, the Kingdom issued a new regulation to fight cyber-crimes and issued a Royal Decree No. m/17 on 8/3/1428 AH, which contained definitions of several cyber terms including the term 'cyber-crime' and defined it as, "*any act committed with the use of a computer or cyber network in violation of the provisions of this law.*" However, this Act was criticised for not introducing deterrent punishment for this crime and did not single out specific counter punishment for those who participate in such crimes.

UAE

The UAE Federal Decree-Law No. (5), 2012, dated 13 August, 2012, on Combating cyber-crimes, whereby the UAE Federal Law No. 2/2006 was repealed, and was one of the pioneering laws in the Arab region in this regard. The previous law, unlike the Saudi Act on cyber-crimes, has provided for more detailed provisions on human trafficking crimes. Article 17 of the previous law provided that, "*everyone who established websites, or*

posts information on the internet, or any means of information technology, with a view to human trafficking or facilitating the deal, shall be punished with temporary imprisonment," the amendment in article 23 of the Law states that: "*Shall be punished by temporary imprisonment and a fine not less than five hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever establishes, administer or runs a website or publishes information on a computer network or any information technology means for the purpose of trafficking in humans or human organs or dealing in them illegally.*"

Jordan

Despite the fact that the Jordanian legislator had issued Law No. 9 of 2009 which prevented human trafficking, it made no reference to the crimes of human trafficking via the internet. Accordingly, the Cyber-Crime Law of 2010 was enacted to provide in article 9 (a) that, "*anyone who intentionally sends or publishes using information system, or the internet, any audio, printed or visual materials that are contrary to morals or that prejudice someone under 18 years of age, shall be punished with imprisonment for not less than three months and with the payment of fine of no less than three hundred JD and no more than five thousand JD*." Article 9 (b) states that: "*anyone who intentionally uses information system, or the internet to save, process, display, print, publish or promote pornographic activities or acts relating to incitement of those who are under 14 years old, or exploiting them in prostitution and pornography, libel, or sell them, or inciting them to act the same, or used them to commit a crime, shall be punished with imprisonment for no less than six months and a fine of not less than 500 JD and no more than five thousand JD.*"

Qatar

The Qatari legislator made attempts to combat online crime of all forms and the Qatari Cabinet had newly approved a law in combating the electronic crimes and has referred it to the Shura Council. It can be said that this law aims to punish whomsoever, "*has access by the internet or any of the means of information technology, to any website or information system belonging to the state or its institutions, bodies, entities or affiliates, and all whosoever has established or managed a website via the internet or any of the means of information technology, to publish false news with intent to endanger the safety of the state, its public order or its internal or external security, as well as punishing whosoever infringes any of the social principles or values, or published news, images, or audio or video materials violating the privacy of the people private and family life, even if they were true, or has insulted others by insult or slander, via the internet or any other means of information technology.*"

The GRETA report titled "***Online and Technology-Facilitated Trafficking in Human Beings, 2022,***" highlighted the Budapest (Cybercrime) Convention in the fight towards CEHT. There is a large consensus among State Parties on the value of the Cybercrime Convention – with many countries indicating it as a "very valuable tool".

Overall, State Parties expressed a positive and supporting view of the available legal instruments enabling cooperation among countries in combating human trafficking. The Council of Europe Conventions on (a) Mutual Legal Assistance and (b) Cyber-crime is considered among the "most commonly" used instrument, and judged as "adequate".

2.7.4 Provisions for Accountability of The Technology Enablers and Challenges in Legal Application

The study titled **"*Using Technology in Human Trafficking: International Law Perspective and Reflections within Middle Eastern Countries, 2015,"*** focused on two countries that professed a pioneering model in combating human trafficking via the internet, namely: the United States and Australia, unlike the UK and France whose legislations did not contain any provisions in this regard.

The United States

The United States enacted several bills and acts to combat human trafficking and its detrimental effects. However, two of these were specifically successful towards achieving the objective, the Trafficking Victims Protection Act (TVPA) and Fight Online Sex Trafficking Act (FOSTA) and Stop Enabling Sex Traffickers Act (SESTA).

TVPA was passed in the year 2000 by the United States Congress. The Act detailed a framework for how to address and attack human trafficking. TVPA stressed on the importance of being proactive in human trafficking situations, both nationally and internationally, to decrease potential ramifications.

FOSTA - SESTA collectively aimed to end illegal sex trafficking on the Internet. The bill package was passed in April 2018. The FOSTA-SESTA bill remained in controversy, as it suggests that web servers, providers, and publishers can be held accountable and can potentially receive criminal sanctions if they are found to have engaged in the facilitation of illegal sex trafficking on their platform. This is in conflict with Section 230 of the Communications Decency Act. Section 230 of this Act stated: *"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 USC 230).*

Australia

As in the United States, the Australian Criminal Act of 1999 (and as amended in 2005) indicated elements of the crime of sexual slavery and scam employment (leading to human trafficking). These amendments aimed to renew the legal provisions on slavery subject to the developments of international human trafficking, particularly sexual exploitation. The Act combined provisions criminalising those who deliberately or in default try to enslave others for sexual exploitation, by imprisonment sentence up to 25 years, and by imprisonment up to 12 years for those who participate or assist in any act of human trafficking. The Act gave the victims the right to an appropriate visa to enter Australia without requiring their financial capacities to sue against their offenders. Unlike the policy followed in the United States that prohibits restrictions on the use of electronic means of communication, the Australian Government aimed to control the publication of internet content that is in violation of decency within its territory. For this reason, Australia has enacted its Broadcasting Services Act of 1992 that determined the three varieties of online content that service providers must refrain from publishing. Of these, the most important represents those containing harmful material for the youth under the age of 18, and ensures that sexual pictures or sexual violence are prohibited from being broadcast, giving the Australian Communications and Media Authority the right to investigate any violation and to encrypt any suspicious published data.

In order to fill the gap in the field towards fighting human trafficking via the internet, some recommendations proposed in the report titled, "*Using Technology in Human Trafficking: International Law Perspective and Reflections within Middle Eastern Countries, 2015,*" were:

- To codify new rules for fighting human trafficking crimes on the internet, taking into account the special nature of this type of crime, in particular in relation to the evidence in cases arising from such crimes. One must work to find a logical balance between the individuals' right to access information through technological means and the state's right to maintain public morality in society as a public right.
- To incorporate the necessary amendments to the rules of criminal procedures in accordance with this type of crime, and to the extent that sets out the provisions to be followed when monitoring computers and when seizing the information contained therein and seizing e-mails in order to have a reasoned proof.
- To ensure international cooperation, in fighting human trafficking over the internet on the level of jurisdiction and procedures.
- To explicitly criminalize unauthorized access to e-mail to send pornographic pictures.
- To add a special course titled 'internet ethics' into the curricula of basic education and add a university course for law colleges to study legal protection on the internet and its criminal use.
- To adhere to the Arab Convention on fighting cyber-crimes considering it as a supporting input for the enactment of laws to fight internet crimes.

The review provides insights into the existing legal frameworks, at the global, regional and national levels. It is interesting to note that some of the studies have provided detailed recommendations on how the legal landscape needs to be fortified against the existing and emerging challenges in the fight against CEHT.

2.8 Solutions and Responses to Combat CEHT

This section reviewed the literature to understand the solutions and responses adopted to prevent and combat CEHT:

1. Role of Law Enforcement in Combating CEHT
2. Role of Technology in Combating CEHT
3. Role of Financial Sector in Combating CEHT

2.8.1 Role of Law Enforcement in Combating CEHT

The report titled "***The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,***" authored by Bridget Dukes, focused on the **United States of America**, is largely based on the investigator's interaction with Agent David Desy at Norfolk FBI Office in year 2020. **Agent Desy shared certain investigation tactics beyond the technological realm.** It is common for the law

enforcement to carry out **decoy operations** by posing as buyers to meet the traffickers and victims. **Honey trapping** is another method wherein a minor when advertised, and a likely buyer expresses interest/ clicking on it, provides adequate grounds to apprehend those buyers. **Sting operations** is another commonly used method, wherein, law enforcement pose as potential victims and allow themselves to be groomed by the traffickers, and finally fix physical meetings to apprehend traffickers.

Agent Desy revealed that Government agencies, like the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), work together with federal, state, and local law enforcement departments in an effort to proactively identify and end sex trafficking across the nation. Several of these agencies have gone as far as developing child exploitation and human trafficking task forces to control this deadly problem. **Some successful initiatives by FBI to combat human trafficking, especially child trafficking, were Operation Innocent Images, Endangered Child Alert Program and Operation Peer Pressure.**

Operation Innocent Images: The United States Congress allocates money to the FBI annually to fund Operation Innocent Images. This is an undercover operation that dismantles online communities and organizations that seek out children for sexual exploitation and child pornography. Operation Innocent Images works directly with the National Centre for Missing and Exploited Children (NCMEC), whose main goal is to end the abduction, abuse, and exploitation of children everywhere.

Endangered Child Alert Program: The FBI initiated the Endangered Child Alert Program (ECAP) in 2005 to disrupt the production of child pornography on the Internet. This program releases photos of unknown individuals, known as John/Jane Does, who are shown in child pornographic videos and images. Their faces are plastered on the FBI website in the hope that someone will recognize and report them to the authorities. ECAP works directly with the NCMEC, as well.

Operation Peer Pressure: The FBI initiated Operation Peer Pressure in 2003 to attack individuals using peer-to-peer (P2P) networks to share files of child pornography. P2P networks facilitate the collection and distribution of child pornography online. Undercover agents download images of child exploitation from offenders' computers to stop the victimization of innocent children.

2.8.2 Role of Technology in Combating CEHT

The report titled "***The Cyberworld and Human Trafficking: A Double-Edged Sword, 2020,***" examined the role technology plays in combating CEHT. The law enforcement is largely relying on **Open-Source Intelligence (OSINT)** to scan the surface web and identify the human trafficking instances. OSINT method also has a framework for reverse imaging, which can help connect advertisements on different platforms using the same pictures.

Hashing is a technology that facilitates quicker comparison/ identification of files. Agencies, like the Internet Watch Foundation, create hashes of child exploitation images and make an all-encompassing list of the hashes to share with other agencies.

Web crawlers are commonly available tools that are used by the law enforcement to monitor the contents on websites to red flag suspicious advertisements that may further be investigated manually, thereby saving significant portion of manual effort. However, these online advertisements websites are known to be designed in such a way to detect and thwart web crawlers.

2.8.3 Role of Financial Sector in Combating CEHT

The report titled, **"*Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children Cases*, 2023,**" mainly focused on the Philippines, explored the payment methods in two categories: payment through Crypto currency, and Money Services Businesses (MSB) such as the Western Union and PayPal. Tracking the flow of money used to buy OSEC is crucial in preventing online child abuse and investigating and prosecuting offenders.

*Role of the Financial Sector***:**

The researchers opined that LEAs and the government should collaborate to obstruct payments for OSEC by analyzing Suspicious Activity Reports (SAR) and Suspicious Transaction Reports (STRs). Financial Intelligence Units can concentrate on the networks and activities and identify the perpetrators.

Data sharing and disclosure to law enforcement:

Data sharing plays a crucial role in the identification, investigation, and prevention of OSEC. In the report titled, **"*Payment Methods and Investigation of Financial Transactions in Online Sexual Exploitation of Children Cases*, 2023,**" Amy Crocker, Head of Child and Technology at ECPAT International, emphasized that financial institutions need to understand what to look for, the types of crime, the modus operandi, offender profile information, and how to profile their customer. Because of privacy and data-sharing laws, the above information is not shared with LEAs. The Sections 314A and 314B of the Patriot Act of the United States enabled LEAs to identify, disrupt, and prevent terrorist acts and money laundering activities through cooperation among LEAs, regulators, and financial institutions to share the information, whereas countries like Canada and Sweden do not have such enabling legislations.

This report further provided the following recommendations for strengthening responses to combat CEHT:

A. Strengthening international cooperation: LEA and governments need to work together to share information and develop coordinated responses to online trafficking. This would be particularly effective between countries at the two ends of the economic migration "corridors", which usually have formal agreements in place but lack adequate monitoring and implementation systems, as well as for countries in other regions where a high number of victims are identified.

B. Examination of national laws and policies is necessary to enable financial institutions to report suspicious transactions directly to dedicated law enforcement units.

C. The government should increase resource allocations for Financial Intelligence Units such as increasing manpower, providing logistics, increasing funding and provide sufficient training to perform their role in combating OSEC.

D. Financial institutions and tech companies should collaborate to respond to OSEC.

E. Need for governments to earmark resources to unmask and blacklist fraudulent websites and spread awareness among jobseekers on necessary due diligence.

F. Need for stricter regulation on payments gateways, crypto currency payments, and accountability for technology enablers.

G. Technology companies should be held accountable if they are not taking proactive measures to prevent their platforms from being used for trafficking.

H. Need for concerted effort towards awareness and capacity building, with a specific emphasis on educating women and children about safety and reporting mechanisms.

2.9 Gaps in the Literature

Gaps Identified in the Literature Review are:

1. Conceptualizing CEHT: After in-depth review of all reports, it is observed that there is no clear definition emerging for CEHT, in the absence of which stakeholders in the criminal justice system will fail to recognize this emerging practice as they have to address the various components of the crime under various sections of the law.

2. Vulnerability Factors: A borderless cyber space presents a new vulnerability that is not always clearly addressed in traditional forms of human trafficking literature. A nuanced understanding of this will help in designing more holistic prevention interventions.

3. Understanding of all forms of exploitation: Most of the current literature remains focused on the traditional forms of trafficking, such as for commercial sexual exploitation and labor trafficking. This restricts it from exploring the nuances of other forms of trafficking that is facilitated by the use of technology, which needs exploration.

4. Understanding of Usage of Cyber Technologies: The review drew attention to some of the commonly used platforms such as Facebook, Instagram, Tinder, Indeed, Craigslist, LinkedIn, etc., being used by traffickers to recruit and exploit victims. Globally, the majority of CSAM is exchanged via non-commercial channels such as public peer-to-peer platforms like Gnutella, eDonkey and eMule. Online payment services, money transfer services, and local payment centers are the most common payment methods in relation to live streaming of child sexual abuse.

   Given these expanding forms and manifestations of this crime, there is a need for an in-depth study on *what* and *how* technologies are being adopted and adapted to perpetuate such crimes with alarming impunity.

5. Role of Online Platforms and Technology Firms as Enablers of CEHT: The review of literature highlighted cases from the Unites States where it is noteworthy that successful action has been taken against Tech Platforms, i.e. Backpage and Craigslist. However, as is evident from the review that this aspect was not adequately addressed in the context of combating CEHT. A notable limitation is the exclusion of a focused investigation into the role of specific online platforms and tech firms in aiding and abetting CEHT. Whether such facilitation is provided *knowingly* or *unknowingly* also requires further exploration.

6. Insufficient Focus on Legal Framework: The understanding of the legal landscape is critical for evaluating the effectiveness of existing laws and identifying potential gaps or

weaknesses that further provide obstacles in the identification and prosecution of offenders and protection of victims. This becomes even more relevant in the context of the absence of an agreed definition of CEHT.

The review provided insights on the existing legal frameworks, at the global, regional, and national levels. It is interesting to note that some of the studies have provided recommendations on how the legal landscape needs to be fortified against the existing and emerging challenges in the fight against CEHT. While this is a good starting point, it is evident that the review does not provide such information for all countries uniformly. For the purposes of the Action Research, an in-depth study of the Indian Legal Framework in the context of CEHT needs to be conducted and is a stumbling block in taking this ahead.

7. Neglect of Technology-Based Solutions: A notable gap is the lack of importance accorded to technology-based solutions in detecting and preventing CEHT. This is a significant gap as technology has emerged as both a facilitator and combatant in digital-age crimes. The gap is crucial because technological advancements offer opportunities to enhance detection and preventive measures against CEHT.
8. Preparedness of law enforcement and criminal justice practitioners in dealing with CEHT: Except for examples from the United States that provide some insights into actions by LEAs in the context of combating sex trafficking and child sexual exploitation, the role of law enforcement, prosecutors, and the judiciary was either largely ignored or referred to superficially. Within the confines of the current legal and policy framework, it is imperative to comprehend the role that the criminal justice machinery plays in the identification, investigation, and prosecution of such crimes.

2.10 What This Action Research Will Address

The review of literature has brought out some striking gaps in the understanding of CEHT globally and in India. While this Action Research may not resolve all the gaps, however, within the framework of its objectives, it strives to bring greater understanding on the following in the Indian context:

1. Conceptualizing CEHT within the Indian framework and proposing a comprehensive definition.
2. Bring out an in-depth understanding of the various forms of CEHT in India.
3. Highlight the frontline role of technology firms as enablers of CEHT.
4. Gain a better understanding of the existing gaps within the legal framework in India to adequately address the issue of CEHT.
5. Gain a deeper understanding of not just the emerging global trends in CEHT, but also focus on the global solutions that have worked in other countries and can be replicated in India.
6. Design and draft the NPoA for India, which will be solution-driven and will clearly lay out the role of all the relevant stakeholders in responding to CEHT comprehensively.

Chapter

03

Methodology

Chapter 3

Methodology

3.1 Introduction

This study is part of the early pan India studies exploring how cyber technologies are being used in human trafficking. Even though there has been a significant rise in the cases of CEHT, there remains a lack of acknowledgement of its expanse in an integrated manner. Cyber-crimes and human trafficking are often seen as independent crimes by various stakeholders. This has led to a lack of empirical data on how the digital medium has penetrated into human trafficking warranting an empirical enquiry on the same.

Even though a few cases have been registered since the study was initiated, it does not reflect the gravity of the issue and the systematic recognition and response it needs. As per the National Crime Records Bureau (NCRB) data from the past years, the incidence of cyber-crimes against women and children is on a persistent rise in India.

According to NCRB data for 2021, there were 10,530 reported cyber-crimes against women, accounting for 20.2 percent of the total cyber-crimes (52,974). This marked a significant 28 percent increase compared to the figures recorded in 2019. Furthermore, in 2022, there was a notable uptick of 12.8 percent in cyber-crimes targeting women. In parallel, cases involving children as victims of cyber-crimes reached 1,823, exhibiting a substantial 32 percent surge compared to the previous year's data of 1,376 (NCRB). It is important to note that these figures may not offer a comprehensive overview, as numerous victims, particularly from vulnerable groups, refrain from reporting due to concerns related to social stigma, fear of reprisals, or a lack of awareness about reporting mechanisms.

Reported cyber-crimes against women and children include crimes such as cyber blackmailing/ threatening, cyber pornography, hosting/ publishing of obscene materials, cyber stalking/ bullying, etc. However, there is no cognizance and hence no data on CEHT that impacts not just women and children, but men too. The situation called for an initiative to study various aspects of CEHT to establish the problem, identify gaps, and recommend solutions.

Since no prior data was available on CEHT, the methodology employed in this study is largely exploratory and depends on anecdotal instances shared by law enforcement officers and domain experts from various parts of the world. The objectives for this study were:

- To understand the trends and patterns of CEHT in different regions of India and the world.

- To ascertain the role/usage of cyber technology in the act, means, and purpose of human trafficking.
- To investigate the role of technological companies/firms in enabling human trafficking.
- To identify the gaps in the Indian legal framework to tackle CEHT and assess the preparedness of the law enforcement mechanism to respond to CEHT within the existing legal framework.
- To understand the global responses to CEHT including legal reforms, technological solutions, mechanism for victim protection and international cooperation for mutual assistance.
- To evolve a comprehensive draft NPoA to combat CEHT.

3.2 Framework for The Study

A. Hypothesis: This study originated from the hypothesis derived from anecdotal experiences that traffickers leverage cyber technologies to facilitate human trafficking. Due to a lack of comprehensive understanding, these cases were often reported as either cyber-crimes or traditional human trafficking cases, neglecting the crucial role of technology in investigations and prosecutions. From experience it is also fair to assume that certain technologies by design provide an enabling environment for such crimes to be committed. The lack of recognition and understanding is likely to expand this crime to disproportionate levels and newer forms will also flourish.

B. Areas of Investigation: CEHT is a relatively new concept. It is a complex issue with different facets across different geographic spaces. Based on the objectives, this study focused on, a) trends and patterns of CEHT across various parts of India and the world; b) role and usage of cyber technologies in CEHT; c) role of technological companies in aiding CEHT; d) existing legal frameworks and the preparedness of LEAs to deal with CEHT and e) role of technology as a solution in countering CEHT.

C. Consultative Meetings:

a) Formation of a Specialized Research Team

A critical and foremost undertaking for this study was the assembly of a multidisciplinary team comprising experts from various domains poised to address the multifaceted objectives of the research. The study team comprised the following members:

i) Dr. Sunitha Krishnan: Sunitha Krishnan, founder of Prajwala has dedicated her life to ending sex trafficking and sex crime. She has been awarded the Padma Shri, the fourth highest civilian honour in India for her efforts. The project to study the role of cyber technologies in aiding and conducting human trafficking was conceived by Dr. Sunitha Krishnan. She further assembled a group of domain experts and spearheaded this team as the Principal Investigator and Advisor.

ii) Ms. Swasti Rana: Ms. Swasti Rana has over 22 years of progressive work experience in the development sector, including 11 years with the UN in India in sectors ranging from Transnational Organized Crime (including Anti-Human Trafficking

and Smuggling of Migrants), Governance, Child Protection, and Refugees. Ms. Swasti Rana plays a pivotal role in this project as the Project Coordinator.

iii) Mr. Tabish Ahsan: Mr. Tabish holds a master's degree in social work and has experience exceeding ten years in field engagement and research endeavours, with a specialized focus on criminology and justice. As a Research Officer in the team, he has contributed to bringing proficiency in research methodologies to the study.

iv) Advocate Aparna Bhat: Ms. Aparna Bhat is a designated Senior Advocate, designated by the Supreme Court of India. She has more than 30 years of experience in addressing legal issues relating to trafficking. She has worked on CSAM and online abuse of children extensively in the last 10 years. She argued the case of Prajwala which led to the creation of the first online rerporting portal in India, setting up a VPN for CSAM and created intermediary accountability.

v) Ms. Aadira Srinivasan: Ms. Aadira is an emerging cyber lawyer who comes with a multidisciplinary background in political science, mass communication, and law with an understanding of the intersection of law and technology and has supported the legal expert in this study as the Assistant Legal Researcher on the team.

vi) Lt Col Vijay Kishore Jha (Retd.): Lt Col Vijay is a military veteran with rich experience in telecommunication engineering, Information Technology, and cyber security. As a Technology Expert in the team, he assisted in the analysis of technology components of the study.

vii) Mr. Mohammed Riyazuddin: Mr. Riyazuddin has served for 33 years with the Police Department, including 8 years in the Cyber-Crimes Wing of Hyderabad. As a Cyber Investigator on the team, he leveraged his skills in carrying out validation investigations.

Each team member was meticulously selected through a process that ensured alignment with the study's scope and objectives. This cohesive and skilled team of experts formed the backbone of the research, skilled to navigate the intricate intersections of technology and human trafficking.

b) Partnership with Telangana Police

A formal partnership was forged with the Telangana Police, specifically the CID for this project, acknowledging their pivotal role as stakeholders in combating CEHT. Mr. Mahesh Bhagwat, IPS, a Trafficking in Persons Hero (U.S. State Department) who led the CID wing when the project started, added value to the project. This collaboration underscores the significance of involving LEAs as active contributors to the study's objectives. The Cyber-Crime Police Station attached to the CID facilitated the filing of cases for further investigations concerning the validation investigations carried out by the team. CID Telangana has also filed one of the first CEHT cases related to forced online criminality.

c) Development of Methodology

Domain experts, both individually and collaboratively, engaged in a focused exercise to evolve frameworks and data collection tools aligned with the study objectives and with due

consideration to the limitations. The finalization of tools ensued after thorough discussions, debates, and meticulous deliberations.

d) Preparation of the simulation sessions

Recognizing the novelty of CEHT as a subject and its terminology, it was deemed essential to conduct a pre-data collection simulation session. This session was aimed at orienting participants, fostering a better understanding of the subject, and enabling them to relate their field experience to the CEHT framework and share their insights effectively.

D. Limitations of the study

As there is no recorded data, this study is not intended to quantify CEHT or offer detailed insights into its scale across different regions. The project also firmly believes that even a single reported/detected case is one too many. The methodology employed is not geared towards drawing comparative analysis between states or countries. As an exploratory study, the focus is on elucidating trends and patterns of CEHT, including the role of technology companies, and gaps in the legal mechanism in countering CEHT, to arrive at the NPoA to address CEHT.

3.3 The Research Process

3.3.1 Sources of Data: This study utilized both primary and secondary data. Primary data was collected through questionnaires, FGDs, global consultations with international experts, and validation investigations. Secondary data was sourced through a meticulous review of relevant literature, filtering materials aligned with research objectives. Additionally, it encompassed literature, data, and reports shared by international experts.

i. Primary Data

a) Sampling: For this study, 28 states of India were the universe. Using purposive sampling, a stratified sample of 15 states was finalized. These 15 states were divided into 4 regions where states of Punjab, Rajasthan, and Madhya Pradesh were clubbed as northern region; Telangana, Kerala, and Andhra Pradesh were clubbed as southern region; Bihar, West Bengal, Jharkhand, Odisha, Assam, and Meghalaya constituted the eastern region and Maharashtra, Gujarat, and Goa represented the western region. Six states were included in the Eastern region as against three in other regions as our experience and anecdotal understanding indicated that Northeastern states have a unique pattern that needs to be recorded.

b) The Tools: The tools for the primary data collection underwent rigorous pre-testing in Telangana. From the feedback received, research team discussions, and pilot outcomes, the questionnaire and framework for FGDs were refined and finalized for the main study.

c) Units of Inquiry: Separate frameworks were tailored for each data collection method. A comprehensive questionnaire was developed specifically for police officers from Cyber Police Stations, Anti-Human Trafficking Units (AHTUs), and other police officers. Similarly, dedicated frameworks were formulated for conducting FGDs with police officers and for consultations with international experts and for the interactions with selected civil society organizations.

d) *Stratification Principle for units of enquiry*: Diverse principles of stratification were employed for this study. The selection of Cyber Inspectors and Officers from AHTUs was conducted in consultation with respective CID or Women's Safety Wing of the State Police. Purposive sampling guided the selection of participants for questionnaire administration. Additionally, participants were segregated into two groups for FGDs based on their affiliation with Cyber Investigation or AHTUs. In international consultations participants were chosen based on their expertise on CEHT as investigators, researchers, or civil society members. 365 officers in total participated in the data collection.

e) *Validation Investigations*: As an integral and distinctive component of this study, two kinds of validation investigations were conducted to affirm and substantiate the identified trends and patterns of online recruitment and entrapment in the context of CEHT, and also to understand the role of technology, role of tech enablers, and modus operandi of the predators. This unique initiative involved the active participation of a Cyber Investigation Expert who executed 6 comprehensive validations over a span of four months. The first involved decoy operations as potential victims or customers, allowing researchers to observe traffickers' tactics firsthand. The second method used for the validation investigations was to interact with victims of CEHT and through their lived experience map the crime.

The investigation uncovered the following purposes and patterns of human trafficking:

- **Job lure**: False job offers, particularly those targeting individuals seeking better opportunities abroad, were used to entrap victims who were then forced into cyber scamming and war recruitment.
- **Organ trafficking**: Organized groups exploited vulnerable individuals through promises of financial gain for organ donation.
- **CSAM distribution**: Low-tech methods were used to distribute CSAM through common technologies.
- **Online sex trafficking and exploitation**: Minors were coerced into offering online sexual services through online escort platforms and dating apps.
- **Illegal adoption**: Illegal child adoption practices were identified.

Following the identification of credible leads and based on validated information, complaints were filed at CID Telangana for further investigation.

Stratified Sampling for Data Collection

Sl.No.	State	Anti-Human Trafficking Officers	Cyber Investigation Officers	Other Police Officers	Total
Northern States					
1.	Punjab	0	30	0	30
2.	Rajasthan	0	3	11	14
3.	Madhya Pradesh	0	7	17	24
	Total	***0***	***40***	***28***	***68***
Eastern and Northeastern States					
4.	Bihar	2	10	7	19
5.	Jharkhand	1	3	16	20
6.	Odisha	0	3	16	19
7.	West Bengal	4	5	2	11
8.	Assam	0	1	25	26
9.	Meghalaya	0	0	23	23
	Total	***7***	***22***	***89***	***118***
Western States					
10.	Goa	7	5	24	36
11.	Gujarat	12	5	3	20
12.	Maharashtra	4	7	5	16
	Total	***23***	***17***	***32***	***72***
Southern States					
13.	Andhra Pradesh	2	6	53	61
14.	Telangana	2	10	12	24
15.	Kerala	0	19	3	22
	Total	***4***	***32***	***71***	***107***
	Total	**34**	**114**	**217**	**365**

International Consultations

Sl.No.	Country	Investigators/ Officers from Law Enforcement Agency	Members from Non-Government Organizations/ Institutes	Academic Researchers	Total
1.	United States of America	6	1	-	7
2,	United Kingdom	1	-	-	1
3.	Austria	2	1	1	3
4.	Spain		-	1	1
5.	Thailand	1	-	-	1
6.	Philippines	-	3	-	3
	Total	**10**	**5**	**2**	**16**

ii. Secondary Data:

Based on the objectives of the study, secondary data was gathered through a curated literature review process and case studies.

a) Literature Review: The endeavour commenced with a comprehensive examination of a substantial pool of over 50 documents encompassing reports, research papers, policy documents, and action plans pertinent to the realm of CEHT. Taking advantage of the profound expertise in the field of the Principal Investigator, this extensive corpus of literature was meticulously sifted through. The selection of documents was guided by a rigorous set of criteria, including the relevance of content to the research focus, the current up-to-date publications, the geographic locations covered, and the credibility of the publication sources.

Out of this extensive pool of literature, six documents emerged as the culmination of a discerning and strategic selection process. Each chosen document represented a pinnacle of relevance and significance within the CEHT discourse, ensuring that the literature review was anchored with the most current, geographically diverse, and credible insights available. The deliberate shortlisting facilitated a nuanced exploration of the complex dynamics inherent in the intersection of cyber technologies and human trafficking.

b) Case Studies: During data collection, numerous cases involving human trafficking, encompassing both cyber technology usage and conventional methods, as well as instances of cyber-crimes and scams were shared by the participants. Interactions with police officers from sampled states and consultations with foreign experts contributed to this repository. However, aligning with the study's scope and objectives, only cases involving the utilization

of cyber technologies in some capacity to facilitate human trafficking were chosen for detailed analysis and inclusion in the report.

The selected cases offer an insight into how diverse technological platforms were employed for CEHT. A framework for writing case studies was developed that included details about the victims and the accused, their socioeconomic profiles, the location where the crime occurred, and the reporting/detection process. Specific attention was given to how cyber technology was exploited by perpetrators. Legal challenges encountered in these cases were also a focal point of the analysis. This comprehensive framework aims to provide insights into the intricate dynamics of CEHT and the varied ways technology is harnessed to perpetrate these crimes.

3.4 Analysis of The Data

The study embraced a comprehensive and adaptable data analysis process. The questionnaire, featuring both quantitative and qualitative inquiries, underwent a hybrid analysis. Quantitative responses underwent statistical scrutiny using descriptive statistics, while qualitative aspects were subjected to thematic coding, unveiling recurring patterns, and nuanced insights.

For qualitative data from FGDs, a rigorous thematic analysis unfolded. Transcripts were meticulously reviewed and coded to extract meaningful themes, revealing participants' experiences and challenges related to CEHT.

International consultation insights underwent comparative analysis, employing a cross-case approach to identify commonalities, variations, and emerging trends in CEHT globally. This enriched the overall understanding of the subject through diverse perspectives. Secondary data, including literature reviews and documents, underwent a comprehensive review to contextualize and validate primary data.

3.5 Action Programme – NPoA to Combat CEHT

The findings of the study will feed into drafting the first-ever NPoA to combat CEHT which will provide the specific action that needs to be taken by various stakeholders to combat this emerging crisis.

The draft will go through rigorous validation through national consultation encompassing all regions of India with relevant stakeholders (police officers, judicial officers, prosecutors, officers from women and child welfare department, cyber experts, civil society organizations) and then be finalized, and consequently be submitted to the Ministry of Home Affairs, Government of India, for adoption and implementation.

Chapter

04

Global Context

Chapter 4

Global Context

4.1 Introduction

Cyber-crime is one of the fastest-growing forms of transnational crime. With the expansion of cyber-crimes globally, today cyberspace has increasingly become the scene of crime for the worst forms of human right violations including human trafficking. Given this spurt in internet usage and fast changing technologies, an exponential increase in varied forms and dimensions of CEHT is being reported globally. In keeping with the nature and scope of the study, the Action Research aimed to supplement the findings of the literature review and delve deeper into the worldwide trends, patterns, and manifestations of CEHT as well as the best practices and technological solutions that other nations have adopted. By drawing on these relevant components, the Action Research hoped to further enhance the NoPA for India.

In this context, Prajwala *virtually* connected with experts from six countries who had worked on CEHT. Their knowledge offered context for the trends and patterns of CEHT in their nation. It further provided better insights of victim profiles, the legal framework, and provisions that arose in response to these new circumstances, the difficulties encountered in the investigation and prosecution of cases. Additionally, the global expertise helped the team to understand the difficulties encountered with technology companies and intermediaries, technological solutions that were implemented, which could serve as models for other countries to follow, and suggestions for encouraging international collaboration in the fight against CEHT.

Global Consultations were conducted with expert/s from the following six countries:

1. United States of America
2. Austria
3. United Kingdom
4. Thailand
5. Spain
6. Philippines

In line with the objectives of the Action Research, discussions with the expert/s centered on the following themes:

Section 1: Trends and Patterns of CEHT: Role and Usage of Cyber Technologies

- Purpose of Exploitation, Modus Operandi and Cyber Technologies being used
- Victim Profiling

- Nature of Exploitation
- Revenue Models

Section 2: Legal Framework to Combat CEHT

- Legal Framework and Challenges in Application
- Support System for Victims

Section 3: Challenges in the Investigation and Prosecution of cases of CEHT

- Preparedness of criminal justice system to deal with CEHT
- Collection and storage of digital evidence and status of digital forensics
- Victim dependence on prosecution

Section 4: Cyber Technology as Enablers: Challenges and Responses

- Various technologies present in the country that are being exploited for human trafficking
- Challenges faced in securing cooperation from technology firms

Section 5: Best Practices and Technological Solutions to Combat CEHT

4.2 The United States Of America

With the support of the U.S. Consulate General Hyderabad[56] and facilitated by the U.S. State Department,[57] virtual consultations were held with officials who had a varied range of expertise and skills, to contribute to the findings on understanding the prevalence and responses to CEHT in the U.S. The contributors to this chapter represented the Centre for Countering Human Trafficking, the Department of Homeland Security,[58] the Homeland Security Investigations (HSI) Cybercrime Centre,[59] and the Department of Homeland Security Policy Shop. Discussions were also held with Protect All Children from Trafficking (PACT),[60] the first U.S. organization to focus on the commercial sexual exploitation of children.

4.2.1 Trends and Patterns of CEHT: Role and Usage of Cyber Technologies

4.2.1.1 Purpose of Exploitation, Modus Operandi, and Cyber Technologies being used

Highlighting the prevailing situation in the United States, experts emphasized that human trafficking was predominantly centered around **commercial sexual exploitation**, with the primary modus operandi employed being deception, fraud, force, and coercion. While sexual exploitation is predominant, investigations have shown that online platforms are also being used for **labor**

56 U.S. Consulate General Hyderabad - U.S. Embassy & Consulates in India (usembassy.gov)

57 U.S. Department of State – Home

58 Center for Countering Human Trafficking | Homeland Security (dhs.gov)

59 HSI Cyber Crimes Center | ICE

60 About Us — PACT (wearepact.org)

trafficking, where victims were promised specific wages and jobs but ended up in exploitative conditions.

It was shared that CEHT took place mainly on social media due to the availability of encryption on the platforms and websites were also involved in facilitating CEHT. Victims were lured with enticing work offers, such as opportunities in the modelling industry. Experts noted that the traffickers manipulated the dreams and aspirations of individuals, luring them with promises of luxurious lifestyles in the United States. In one such case, women were lured from Russia and other Eastern European countries to travel to the United States and then coerced to work as women in prostitution for an illicit prostitution enterprise, **XO Companions.** Individuals seeking a better life often become victims of these transnational trafficking syndicates.

Experts also shared about CSAM, where children and young adults who were victims, were exploited by the traffickers/predators with their sexually explicit content. Several online mediums such as dating sites, online games, and apps such as Pinterest, were exploited to spot vulnerable children who were then groomed for CSAM. Experts also shared that individuals who were once victims of sexual exploitation may become involved in further exploitation by taking on roles managing day-to-day operations in such illicit activities.

4.2.1.2 Victim Profiling

Human trafficking victims come from diverse backgrounds, with no specific demographic exempt from susceptibility. Regardless of age, race, ethnicity, gender identity, national immigration status, cultural background, or socioeconomic class, anyone could fall prey to traffickers operating on online platforms. While the experts stated that everyone is equally vulnerable, they mentioned that traffickers target people experiencing loneliness and desperation. Giving an example of "*casting a net for catching fish*", one of the experts stated that traffickers impersonating affluent individuals tried to reach as many people as possible and then filtered out the most vulnerable who can be easily exploited.

As seen in the case of XO Companions, the profile of the victims generally included poor women from Russia and East European countries. These were usually young women who were in their early 20s, lured with promises of luxurious lifestyles in the United States. However, the experts highlighted instances where successful professionals such as models, doctors, etc. were also lured by the prospect of traveling for work. Experts also emphasized a rise in male child victims involved in online gaming, being groomed and coerced into sharing explicit content and facing blackmail.

4.2.1.3 Nature of exploitation

Experts concurred that the nature of exploitation was both virtual and physical, with acts of sexual exploitation occurring both on and off the digital medium. Sexual exploitation could take place in brothels, and it could also be completely online, said one of the experts.

Traffickers were increasingly utilizing dating apps and social media to identify and groom victims. The progression from physical to virtual trafficking was observed in cases where traffickers initiated contact on dating apps and then groomed victims on social media platforms. Through

enticing stories and promises of a lavish lifestyle, victims were persuaded to meet the trafficker, leading to physical exploitation, curtailment of movement, etc. Videos of sexual activity were captured and posted on pornographic websites. Additionally, the use of live streaming platforms, including Zoom, and applications like Telegram, played a significant role in facilitating trafficking.

4.2.1.4 Revenue Models

The evolution of human trafficking into a $160 billion industry surpassing narcotics accentuates the magnitude of the issue. Speaking about the revenue model, experts shared that, "*it used to be a cash-based thing to maintain anonymity*", but digital transactions were gradually increasing. Services like Cash App, PayPal, and Venmo (digital wallet) were also being used for transactions. However, the experts noted that there was minimal usage of crypto currencies in their experience.

Peer-to-peer transfers and bank statements played a pivotal role in establishing probable cause for seizing assets. An expert shared that as profits rapidly moved overseas, they went after the assets of traffickers such as their houses, cars, boats, etc.

The International Justice Mission (IJM), a U.S.-based non-governmental organization dedicated to human rights, law, and law enforcement, released a report on the Philippines that focused on examining payments made to streaming services within the country. The report found that a significant portion of CSAM streaming services originated from the Philippines. These services were being accessed by individuals in the United States and the payments for such services were traced back to the Unites States as well. However, as per their knowledge, the experts stated that the U.S. Government has not yet carried out any such studies.

4.2.2 Legal Framework to Combat CEHT

4.2.2.1 Legal Framework and Challenges in Application

Providing an overview to the existing legal framework, experts shared that in the 2000s, after the Palermo Protocol, the *Trafficking Victims Protection Act of 2000* (TVPA) was introduced. It defined human trafficking as, "*the recruitment, harbouring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act*." It extended to commercial sex acts performed on children who have not attained 18 years of age. An expert shared that challenges were faced with enforcement against people who were in the process of '*obtaining*', and it proved difficult to act against the *demand / clientele*.

Notably, CEHT was not covered under this Act. Furthermore, discussing the alternate forms of exploitation, an expert shared that in the United States., organ trade did not fall under the category of human trafficking and is covered under other laws as a separate crime. Similarly, forced marriage was a crime, but not categorized as human trafficking.

To address the challenges surrounding crimes of CEHT, in 2018, the U.S. Congress passed FOSTA-SESTA (Fight Online Sex Trafficking Act-Stop Enabling Sex Traffickers Act). FOSTA and SESTA were U.S. Senate and House bills that became law on April 11, 2018 and challenged immunity to knowingly promote sex trafficking by companies.

Citing an example, the experts spoke about ***Backpage.com,*** which was running an illicit sexual marketplace where children as young as 12 years were forced into prostitution by criminals peddling them through classified ads. The Site is supposed to have made $ 500 million over a period of 4 years. On registering of cases against this site and the victims coming forth and sharing their harrowing experiences, *Backpage* had since been banned from the internet and assets worth about $ 200 million was seized.

Another such site, Craigslist**,** was forced to shut down its personals section in the wake of the Fight Online Sex Trafficking Act, passed by Congress. Until 2009, the site had a section titled "Erotic Services", where people openly advertised sexual services. This was later changed to "Adult Services", and till recently was camouflaged under its personals section.

Experts highlighted that due to this new law, any advertisement that promotes child sexual activities is illegal. While the focus of *Backpage* was on advertising and not on the content of CSAM, the law made it illegal to advertise selling children for sex and labor. The law did not cover visuals on such websites. There are bills, still pending, that regulate what can be published by websites. **There has been a backlash by advocates for the First Amendment for freedom of speech. Although CSAM does not come under the purview of freedom of speech, yet there has been a pushback from the sex workers lobby which constitutes adults, who claim they are now prevented from making sexual content for their livelihood.**

Despite the existence of SESTA and FOSTA since 2018, challenges in their implementation persist. Challenges persist in enforcing these laws, particularly in proving the knowing assistance, facilitation, or support of trafficking by online platforms. Prosecution under FOSTA-SESTA encountered difficulties when perpetrators switched servers for illicit activities. Challenges also arose when attempting to prosecute technology companies, as they often promptly took down the site before legal action could commence. Thus, prosecutors often hesitated to use these laws, opting for more familiar charges like money laundering or interstate commerce.

Due to these challenges, experts highlighted the limited use and implementation of FOSTA-SESTA. The laws generally used are:

- Section 1591 of Code 18 (Criminalizes sex trafficking of children or adults through force, fraud, or coercion)
- Wire Fraud Laws (Prohibits the use of electronic communications to execute a scheme to defraud someone)
- Mann Act (Outlaws the transportation of individuals across state lines to engage in illegal sexual activities)
- Travel Act (Criminalizes travel or use of interstate commerce facilities with the intent to promote or carry on unlawful activities, such as prostitution or illegal gambling)
- Money Laundering Act (Targets the process of disguising the origins of illegally obtained money, typically through complex financial transactions, to make it appear legitimate)

On the critical issue of consent in CEHT cases, experts emphasized the need for detailed questioning of victims to elicit informative responses. Many cases go unnoticed when direct questions about coercion and fraud are asked. Since the definitions of these terms are not standard,

victims may not give affirmative responses. Throughout this process, victims frequently chose to remain silent, fearing repercussions, criminalization, loss of income, and, in some instances, deportation. The experts emphasized that victims felt secure and comfortable once organizations involved in trafficking were dismantled, alleviating concerns about backlash.

The Communications Decency Act (CDA) and the First Amendment in the United States offered strong protection for speech. This came about in the backdrop that if online platforms were responsible for the content placed, they would not be able to function. In a case involving *Oracle*, the company faced a lawsuit for removing offensive material. The U.S. Congress responded by passing Section 230 of the CDA which provided:

1. Websites are not to be held liable for taking down offensive material.
2. Websites are not to be held liable for keeping offensive material online.

The outcome of this section was that service providers started keeping the offensive material on the website. Pages like *Backpage* and *Craigslist* which were meant for selling furniture, also started selling children under the tags of "barely legal", "Lolita" etc. They are protected under Section 230 of CDA.

Victims of CSAM and human trafficking often invoked the defense of lack of agency in crimes committed under duress. The law treated adult victims the same as children in cases of exploitation. Earlier, coercion lacked a clear definition, and mental coercion was not explicitly acknowledged. While existing laws aimed to provide equal protection to adults and children, adults often faced a greater burden of proving trafficking. They were frequently subjected to various forms of coercion, including drug addiction and this aspect could be used as a defense in cases where victims were compelled to engage in certain criminal activities.

4.2.2.2 Support System for Victims

Experts reiterated that in theory, victim protection was a key aspect of law enforcement efforts. Restitution for victims was embedded in sentencing, ensuring that they receive financial support. To enhance victim protection, LEAs focused on seizing traffickers' assets (house, car, boat etc.) early in the investigation, ensuring that victims receive restitution even when the trafficker was incarcerated. For victim assistance, the U.S. Department of Justice had the Office for Victims of Crimes that maintains funds. This included monetary help, protection in a safe space with basic amenities and legal aid. However, how much was achieved in practice, varied across the country, experts opined.

When it came to aid from technology companies for victims, their support was limited to the removal of explicit material, addressing the immediate concern of eliminating harmful content from online platforms, shared experts.

4.2.3 Challenges in Investigation and Prosecution of CEHT Cases

4.2.3.1 Preparedness of Criminal Justice System to deal with CEHT

Experts stressed the need for skilled and trained interviewing skills required in investigating cases of CEHT. The experts emphasized the complexity of exploitation, noting that victims may not immediately realize they have been trafficked. Although commercial sexual activities may seem consensual on the surface, when one digs deeper, it is non-consensual, and elements of exploitation unravel. Building trust and rapport with victims is a time-consuming process before they feel comfortable sharing their real-life experiences with others.

Although training was occuring regularly, experts stated that yet there was no uniformity throughout the country, and not all the officers are well-trained on aspects of CEHT. An expert shared that although not everyone has specific training, yet basic knowledge exists.

The specialized units within the U.S. Attorney's Office, well-versed in various laws, played a crucial role in accepting and prosecuting human trafficking cases. Their expertise enhanced the effectiveness of criminal investigations. The synergy between investigative agencies and legal entities was critical for successful prosecutions. Prosecutors aided law enforcement in giving legal support. The Department of Justice provided prosecutors with special training for Cyber-crimes and Human Trafficking. This training under the Computer Crime & Intellectual Property Section (CCIPS) informed the prosecutors of the latest rulings and explained the newest technology to them.

Ensuring the criminal justice system's readiness involved continuous training for investigators and prosecutors. While victim-centric training was common, challenges persist in bridging the knowledge gap in technology-related aspects. Collaboration with cyber agents highlighted the interdisciplinary nature of CEHT and the need for ongoing education within LEAs.

There was a protocol for training law enforcement officers to deal with cyber-crimes regularly. Citing the example of child exploitation cases, an expert stated that the prosecutors and judges were tech-savvy and trained to deal with cyber-crimes on par with the law enforcement officer.

4.2.3.2 Collection and storage of digital evidence and status of digital forensics

The admissibility of digital evidence, even without the victim present, underlined the evolving legal landscape in the United States. Compliance with the federal definition of CSAM was essential, showcasing the legal adaptability needed to address technological advancements in criminal activities. Under ordinary circumstances, law enforcement officers typically obtained a warrant from the courts to seize digital evidence, and the courts generally acknowledged the validity of the evidence. However, in the context of an international border port of entry, the officer is authorized to inspect and, if deemed necessary, seize the device without requiring a court order. It was clarified that warrants were based on probable cause, requiring articulable facts to prove a crime's occurrence. The timeframes for responses to court orders or notices were discussed with a 10-day norm set by judges and variations in cooperation observed among different tech companies.

Regarding the collection and storage of digital evidence and the capabilities of the first respondents to address this, it was seen that the first respondent contacted the specialized team

required to assist the officer in the collection of digital evidence and took custody of the material by following due procedures as established by law and sent the evidence for analysis. The court relied on digital evidence if the chain of custody was properly established, and there were several instances where the court relied on the digital evidence while deciding the case.

Experts shared that the HSI field offices employed Computer Forensic Analysts for on-site device previews during search warrants. Advanced forensics at the Cybercrime Centre addressed issues like encryption, enhancing the ability to access critical evidence. Adherence to legal processes ensured the admissibility of digital evidence in court, strengthening the overall investigative process.

4.2.3.3 Victim dependence for prosecution

Speaking on the role of victims in securing prosecution, investigations seemed to rely heavily on victim testimony, emphasizing the importance of victim protection and support. NGOs played a vital role in providing comprehensive assistance, and addressing housing, medical care, and psychological needs. The delicate balance between victim assistance and legal integrity was a key consideration in securing justice.

In cases where the victim didn't appear in court, the case may be deemed invalid, as the suspect has the right to confront the victim during court proceedings. However, under certain circumstances, a case could proceed in court without the victim's presence, provided there is substantial evidence linking the accused to the crime involving the victim. Various agencies and NGOs are dedicated to supporting the victim throughout the trial process. These organizations offer essential services such as shelter, medical and psychological assistance, training, and in some instances assistance with employment opportunities.

4.2.4 Cyber Technology as an Enabler: Challenges and Responses

4.2.4.1 Various technologies present in the country that are being exploited for human trafficking

Novel operating systems, such as Graphene, posed challenges for law enforcement due to their enhanced privacy features. Traffickers often utilize **jail-broken phones** to access encrypted data and circumvent security measures. An **automated kill switch** was programmed which required a password to be entered every few hours or it would self-destruct.

When asked about the various technologies that were being exploited by traffickers, one of the experts exclaimed that, "*anything can be used*". Criminals were always on the lookout for new ways of using technologies for their purposes. One of the experts stated that, *"technologies are not bad on their own, it is more about how it is used. It has created ease of misuse through anonymity as you can impersonate another individual.*" When asked about specific examples they mentioned the use of encrypted apps like Kick and Telegram.

4.2.4.2 Challenges faced in securing cooperation from Technology Firms

The level of cooperation from technology firms who developed these technologies varied, reflecting the complex relationship between law enforcement and private entities. An expert stated, "*It appears as though for some companies, client privacy is more important than citizen safety.*" While some were cooperative, responding promptly to court orders, others posed obstacles, emphasizing the ongoing challenge of balancing privacy concerns and law enforcement needs. Timely responses to court orders are essential for the swift progression of investigations. There were obstacles they faced while trying to pin international perpetrators like tech companies located in another country, as serving subpoenas to an overseas company was not possible. They generally followed the money trail and talked to victims to understand the cases. For a U.S. company, law enforcement would serve a subpoena, and in most instances, they would comply. The difficulty was compounded when diplomatic relations with the concerned country were severed and, in many instances, officials relied on personal informal contacts and communication.

Typically, LEAs secure a court order and forward it to technology companies to obtain necessary information. The response deadline varied from case to case, generally spanning from 10 to 30 days. Instances arose where certain technology companies disregarded this time frame, prompting law enforcement to gather information from alternative sources.

Technology firms were criticized for lacking the intent to address human trafficking issues. The experts commented on the perceived lack of honesty among technology enablers, emphasizing their prioritization of personal interests over broader social good or law enforcement interests. There have also been instances where banks closed accounts of suspected perpetrators if it were known these were being monitored, thus stalling the investigation. The experts noted varying responses from different companies, citing *Booking.com* as more supportive than others, with some companies only responding to subpoenas and warrants issued by the courts, and not always in the first instance.

Experts were unanimous in the opinion that, on their own, the technology industry did not want to invest in improving screening mechanisms. The technology industry's interest in screening and responding to offensive material stemmed from a need to comply with legal frameworks that govern content moderation. There are two reporting mechanisms in place, the first was for reporting online to service providers, and the second was for service providers to remove the content immediately. Despite the existence of such mechanisms, implementation was slow and ineffective. Although the social media platform, Facebook, removes any explicit material that may be posted, yet there are no mechanisms in place to prevent circulation of that material.

In the United States, civil remedies were intricate, with few lawsuits against technology companies before FOSTA. Judges' limited understanding of technology led to the interpretation of Section 230 of the CDA as providing internet immunity, and hindering technology companies' content regulation. As a result, the judges dismissed lawsuits against websites.

While there have been bills made by the Judicial Committee to make screening of ISPs to be stringent, they have not been passed yet, and the United States is nowhere close to the UK or EU countries when it comes to screening of CSAM material, due to the existence of CDA. Owing to these glaring gaps, the United States has emerged as a major consumer for CSAM content being streamed

from countries such as the Philippines. Tracking payments has revealed that a significant amount of the revenue gained from such sources is also coming into the United States.

One of the issues faced by investigators in relation to companies with U.S. servers was that it was difficult to verify age in CSAM content, and this made it difficult to take action against them. It can often take multiple subpoenas for companies to respond to, or sometimes they redirect it to their legal teams. *Telegram***,** based in Russia, is notorious for not responding to notices.

A notable challenge arising from technology companies' retention policies is the limitation of access to older information. To address this, investigators deployed preservation requests to the respective technology companies, seeking to immediately safeguard necessary information. These requests played a crucial role in preventing the loss of pertinent data and were particularly important in cases where older information was essential. Additionally, investigators examined user backups as part of the process to ensure the retrieval of relevant data for their inquiries.

4.2.5 Best Practices and Technological Solutions to Combat CEHT

Experts shared tools like Spotlight (free) and Traffic Jam (paid) that illustrated law enforcement's proactive stance in leveraging technology for mapping and identifying potential trafficking ads and victims.

Traffic Jam used AI to help law enforcement find the victims and enabled them to take down organized criminal networks. Spotlight, on the other hand, was a web-based application that helped LEAs to identify potential leads in their sex trafficking investigations. Holding platforms accountable and encouraging reporting through campaigns demonstrated a multi-pronged approach to combating exploitation, integrating both technological and awareness strategies.

Social media posts, advertisements, and other online content could be analysed to identify patterns and indicators of potential human trafficking activities. Web scraping tools were used to compile data etc. in the context of CEHT. Traffic cams were also used to identify hotel rooms linked with sex trafficking.

Experts suggested that the victim-centric approach, wider operations focusing on potential victims, and increased communication with victims, as recommendations for countering CEHT. They emphasized collaboration with specialized entities such as Google and Microsoft, closing bank accounts associated with human trafficking, and international cooperation with platforms like Booking.com.

Contributors

Lori L. Cohen, Chief Executive Officer, PACT

Special Agent Mark Niegelsky, Diplomatic Security Service

Special Agent David Paik, Human Trafficking Investigations Coordinator, Diplomatic Security Service

Robert C. Bartolo, Senior Advisor, DHS Center for Countering Human Trafficking

Special Agent Albert Ordonez, National Program Manager, DHS Center for Countering Human Trafficking

Special Agent Raymond Abruzzese, Program Manager, HSI Cyber Crimes Center, Child Exploitation Investigations Unit

Bethany Eberle, Acting Director, DHS Office of Strategy, Policy and Plans/Counter Transnational Organized Crime/Crimes of Exploitation Policy Group

Profile of Organizations

Center for Countering Human Trafficking:

The Center for Countering Human Trafficking, a part of the Department of Homeland Security, is an inter-agency coordination center that brings together 16 agencies. It focuses on countering human trafficking through law enforcement operations, victim protection, and prevention efforts.

Homeland Security Investigations (HSI) Cybercrime Centre:

The HSI Cybercrime Centre, located in Fairfax, Virginia, specializes in online child exploitation investigations. Its principal focus is identifying and rescuing child victims, apprehending offenders, and conducting forensics on seized devices. In the year 2022, they successfully rescued over 1100 children globally.

Department of Homeland Security Policy Shop:

The Policy Shop plays a crucial role in policy development and strategic planning related to crimes of exploitation. They actively contribute to the White House National Action Plan, the DHS Strategy to Combat Human Trafficking, and the National Strategy for Child Exploitation Prevention and Interdiction.

Protect All Children From Trafficking (PACT):

Founded in 1991, PACT was the first U.S. organization to focus on the commercial sexual exploitation of children.

4.3 Austria

Facilitated by the Asia Department of International Projects and Programs, DKA Austria,[61] virtual consultations were held with senior officials from the Federal Ministry, European and International Affairs, Division for Border Issues, and the Fight against Trafficking in Human Beings,[62] and the Joint Operational Office against Human Smuggling, and Human Trafficking, Federal Bureau of Investigation, Austrian Ministry of the Interior.[63] Discussions were also held with a member of staff from the University of Vienna, who had research experience in this specialized area of work.

61 DKA Austria - Dreikönigsaktion, Hilfswerk der Katholischen Jungschar

62 Migration and Home Affairs - European Commission (europa.eu)

63 Austria | Europol (europa.eu)

4.3.1 Trends and Patterns of CEHT: Role and Usage of Cyber Technologies

4.3.1.1 Purpose of Exploitation, Modus Operandi, and Cyber Technologies being used

Speaking on the patterns and forms of human trafficking in Austria, **experts spoke on the connection between illegal migration and human trafficking**, shedding light on the vulnerabilities that arose from the socioeconomic status of illegal migrants. Highlighting the prevalent purpose of human trafficking in Austria, the expert emphasized two primary dimensions: labor exploitation and sexual exploitation, of both adults and children.

Foremost among these was the trafficking of girls and women for sexual exploitation. While Austria permitted prostitution within certain legal frameworks, the experts also shared the existence of a parallel, illicit domain where women and girls were coerced into sexual activities against their will.

Experts also emphasized the grave issue of child trafficking, predominantly for sexual exploitation, which manifested in both tangible realms and the digital sphere, with children being subjected to live-streamed abuse and the proliferation of CSAM. Additionally, children were trapped in activities like begging, pickpocketing, and shoplifting, further exacerbating their vulnerability and exploitation.

Secondly, there was an increasing trend of human trafficking for labor purpose, in which a pivotal role was played by subcontracting agencies in perpetuating this form of exploitation. Delving deeper into the intricacies of labor trafficking, the experts alluded to the phenomenon of migrant smuggling, where individuals were exploited as a reservoir of inexpensive labor. There was exploitation of victims in labor intensive sectors such as agriculture and farming, and they were made to live in harsh conditions.

Furthermore, speaking on the pervasive role of digital technologies in human trafficking, the experts shared that online platforms, virtual spaces, and other digital tools had seamlessly integrated into every facet of trafficking operations. From the initial stages of pre-crime planning and coordination to the subsequent control over victims post-trafficking, technology remained a central enabler for traffickers.

Elaborating on the **modus operandi** being used, experts highlighted the extensive use of social media sites such as Facebook in facilitating human trafficking whereby the platform was used largely for recruitment where the traffickers tried to gain the trust of potential victims by being friendly and acting as a confidant. The experts also spoke of the "*lover boy technique*" being used to lure victims. After gaining control over the victims, social media and encrypted applications were also used to maintain continuous control and there were instances where explicit content was used as a leverage to threaten and silence the victims.

Expanding on the broader context, experts noted the compounding effects of global events on trafficking patterns. An expert attributed the rise in child trafficking instances to the challenges posed by the Covid-19 pandemic. Furthermore, in the wake of the conflict in Ukraine, Austria witnessed an alarming surge in victims from Ukraine.

4.3.1.2 Victim Profiling

The experts provided a demographic perspective on human trafficking victims, noting that approximately two-thirds of the victims originated from European Union countries such as Romania, Hungary, Ukraine, and Bulgaria. In contrast, the remaining one-third came from non-European countries like Serbia, Thailand, Turkey, and Venezuela, among others. Speaking on the profile of the victims, migrant women and children, especially girl children are seen to constitute a majority of the victims. Historically, the focus of anti-trafficking efforts in Austria has been on vulnerable populations, centered on children from marginalized ethnic communities, like the Roma, in neighbouring countries. These victims are systematically transported into Austria, where they fall prey to forced criminal activities and organized begging. The intricate networks facilitating these operations utilize covert routes, adding layers of complexity to these exploitative schemes.

A crucial factor was the lower incidence of Austrian victims, attributing it to their awareness of legal rights and safeguards. Austrians, being informed about their rights, are less likely to fall victim to exploitation, as they are more inclined to report such incidents to LEAs.

A significant challenge, pointed out by an expert, was associated with the legality of commercial sexual activities in various parts of Europe, which often contributed to the concealment of exploitation.

4.3.1.3 Nature of exploitation

Experts delved into the nuanced landscape of exploitation, noting a blended manifestation involving both virtual and physical dimensions. While certain forms of exploitation, such as CSAM and live video streaming, predominantly occur in the virtual realm, other forms like labor exploitation, sexual exploitation through prostitution, and begging primarily manifest in the physical domain.

As noted by experts, cyber technology is known to facilitate the interconnectedness of these distinct manifestations. It was highlighted that employing digital tools and platforms made coordination and communication among traffickers more efficient. The experts highlighted that along with recruitment, planning, and coordination between traffickers also took place via technology. Traffickers were thus using social media sites like Facebook and Instant Messaging apps for this purpose.

4.3.1.4 Revenue Models

Experts provided insights into the diverse revenue models associated with human trafficking, emphasizing that these models were situational and lacked uniformity across cases. Traditionally, cash transactions have been central to the trafficking economy, often intertwined with money laundering activities.

The role of travel agencies was highlighted in subjecting illegal migrants to debt bondage in exchange for facilitating border crossings. Victims often repaid these debts through various means, including engaging in cheap labor and enduring physical and sexual exploitation.

Expanding on contemporary financial trends, experts delved into the realm of crypto currency and blockchain technology. Since transactions recorded on the blockchain cannot be concealed or erased, this characteristic could be leveraged by LEAs. The immutable nature of the blockchain offered invaluable insights and provided trails for investigators, aiding in tracking and understanding the intricate flow of illicit funds.

4.3.2. Legal Framework to Combat CEHT

4.3.2.1 Legal Framework and Challenges in Application

Experts highlighted that while Austria's criminal code encompassed various forms of cyber criminality, it lacked specific provisions directly targeting CEHT. However, victims of human trafficking, including non-EU individuals, were afforded legal protection under **Article 57 of the Austrian Asylum Act**. This ensured that victims had rights and support during investigations, contributing to their safety and well-being.

It was evident that Austria had made significant strides in combating human trafficking, but as technology evolved, legal challenges emerged, and the country faced hurdles in adapting existing legal frameworks that could effectively address the cyber dimensions of human trafficking.

The prevailing criminal code in Austria is comprehensive, encompassing various offenses. However, it applied uniformly to both traditional, physically committed crimes, and those assisted by technology. This uniform application posed challenges in addressing the unique aspects of CEHT. Although references to the Palermo Protocol were made, yet nuances related to technology, especially CEHT, seemed to be at a nascent stage. The absence of explicit laws posed challenges, prompting the exploration of the strengths and weaknesses inherent in the legal landscape.

4.3.2.2 Support System for Victims

There appears to be a notable absence of specific legal measures tailored to individuals subjected to CEHT within Austrian law. Instead, existing human trafficking laws are identified as the primary recourse for addressing cases intertwined with technology.

Victims grappled with the weaponization of technology in the trafficking scenarios they endured, with psychosocial hurdles being a significant challenge. The process of victims failing or being reluctant to recognize themselves as victims of human trafficking was identified as a potential obstacle, which impacted their access to crucial support services and legal avenues. Furthermore, an additional layer of challenges arose as perpetrators employed technology to contest victims' accounts, presenting images to suggest that the victims were not being trafficked. These challenges extend beyond the legal spectrum, emphasizing the need for holistic support frameworks that address the psychological and social dimensions of victim experiences.

Despite the challenges, Austria remains dedicated to refining victim-centric approaches. This ongoing commitment reflects the recognition that the recovery and well-being of those affected by trafficking require comprehensive and tailored support. By continuously refining its strategies and approaches, Austria aims to create an environment within these intervention centers that fosters healing, empowerment, and a path toward reclaiming agency for survivors of human trafficking.

NGOs play a pivotal role in combating human trafficking by providing support to victims and cooperating with LEAs. NGOs identified and addressed a significant number of human trafficking incidents in Austria, with reports indicating approximately 50 percent of such cases reported by them. Their involvement strengthens the collaborative efforts between civil society and law enforcement in combating human trafficking.

An expert highlighted the ***Mariposa Case***, which involved a perpetrator challenging the integrity of the victims based on their online activities. The Mariposa case stood as a landmark legal battle against CEHT. It brought to light the importance of victim-sensitive practices, collaborative efforts, and comprehensive legal measures to address the challenges posed by human trafficking in the digital age. The success of the case sets a precedent for future prosecutions in similar contexts.

The case involved victims who were primarily citizens of Venezuela and two Cuban nationals who were recruited in Venezuela, both in person and through social media. The defendants organized the victims' travel to Austria, picked them up at the airport, and were then coerced into providing escort services, under exploitative conditions. All 17 victims received psychosocial and legal support, with LEFÖ-IBF[64] providing a lawyer and psychosocial assistance for each victim, and there was early involvement of financial investigators and close cooperation between law enforcement and LEFÖ-IBF. **This was a path-breaking case, as digital evidence was collected by the case worker, the psychosocial worker, and the NGO. They all worked hard to convince the police to look at the digital evidence and to take action as the culprits were all in Venezuela and the victims were in Austria.**

As mentioned above, victims of human trafficking, including non-EU individuals, were provided legal protection under Article 57 of Austria's Asylum Act. Article 57(2) of the 2005 Asylum Act stated, *"a special protection residence permit shall be granted ex officio or upon a well-founded application to third-country nationals resident in the federal territory, in particular to witnesses or victims of human trafficking or the cross-border prostitution trade, for the purpose of guaranteeing the prosecution of acts punishable by the courts or with a view to the submission and enforcement of civil-law claims in connection with such punishable acts."* This provision ensured that victims had access to rights and support during investigations, including protection from further exploitation. Coordination by the Intervention Centre for Trafficked Women, with support from NGOs and specialized police units, further enhanced victim protection efforts. In rare cases where victims were at heightened risk, measures such as providing new identities and relocating them abroad could be undertaken to ensure their safety and security.

4.3.3 Challenges in Investigation and Prosecution of Cases of CEHT

4.3.3.1 Challenges faced in investigation and prosecution

The following were the challenges expressed by all the experts:

- The digital contents of the victims remained on the social media platforms / websites long after trafficking had ended. i.e., taking down the contents was often a challenge.

64 LEFÖ IBF– is a non-profit, non-governmental organization founded in 1985 by a group of politically exiled Latin American women living in Vienna.

- The online monitoring of suspicious accounts by the investigators was limited due to the strong privacy protection regulations. Access to certain websites that were deemed inappropriate was blocked. However, among these were also the websites that the investigator would need to access in order to investigate the crime, hindering effective investigation.
- Prohibiting/stopping illegal activities on/using technology platforms were not possible without the cooperation of the service provider of the platform. There is currently no provision in Austria to assign attributability to technology platforms.
- It had been observed that traffickers often used AI enabled manipulation of the contents of victims, e.g., to slow down speech, etc. When confronted by law enforcement agencies (LEA) they claimed that the video/content was a deep fake, and they were not involved.
- Live streaming through webcams now permitted separation of origin of human trafficking and its destination in the manner that victims need not be physically transported across borders, making it difficult to monitor and control movement.
- Further, it was difficult to ascertain the location of servers which were providing services at a particular instance/case. As a result, LEAs face problems in presenting their case to the judiciary.
- Taking down a technology platform/website/service and closing of a suspicious account was ineffective in countering CEHT, as new/alternative service/account could be hosted/opened/used very easily by the traffickers.
- When a victim was made to transfer money from their account, LEAs faced difficulties in reaching culprits in such cases of coerced cooperation.

4.3.3.2 Collection and storage of digital evidence and status of digital forensics

Regarding the process of collecting digital evidence by first responders, an expert explained that in normal situations, first responders notified a team of Cyber Experts who assisted in collecting digital evidence. However, in some cases, if the first responder felt capable, they would handle the seizure themselves and present the evidence to the prosecuting officer. While first responders received training in collecting digital evidence, specialized skills were required in certain scenarios, prompting experts to be called to the crime scene.

In response to inquiries about the admissibility of digital evidence in court, the expert stated that if a suspect challenged the authenticity of the evidence, the court could call an independent expert for evaluation. The judge then decided the weightage of the digital evidence based on the expert's opinion, emphasizing the independence and merit-based nature of the decision. Text messages between the victim and the perpetrator were considered by the court as proof of evidence, in addition to victim testimony.

4.3.3.3 Preparedness of Criminal Justice System to deal with CEHT

An expert highlighted that there were training programs for first responders in handling digital

evidence, and specialized training for second-level officers in data extraction using tools like Cellebrite/UFED. Additionally, young officers were deployed to monitor online gambling activities, swiftly responding to unlawful behaviour. These officers actively participated in online gaming platforms to deter illegal activities ensuring users were aware of police presence and could report unlawful activities. Within the police department, there was a separate unit to deal with cyber-crimes which was sufficiently trained to deal with such cases.

4.3.4 Cyber Technology as an Enabler: Challenges and Responses

4.3.4.1 Various technologies present in the country which are being exploited for human trafficking

Experts emphasized the escalating role of technology in facilitating human trafficking within Austria, with the internet and social media platforms as pivotal tools for criminal activities. Mainstream platforms such as Facebook, Instagram, and TikTok were labelled as the "most important tools" in enabling human trafficking and other criminal endeavours. Particularly noteworthy was the mention of the extensive use of social media, instant messaging, and dating apps like Tinder during the Covid-19 lockdown period, where traffickers exploited these platforms to lure and trap victims. These channels, typically designed for communication and contact, became conduits for illicit activities.

Experts emphasized the dual-edged nature of technology, asserting that while it offered numerous benefits, it could also be exploited by criminals to advance their illicit objectives. Highlighting the adaptive nature of traffickers, the tendency was to continually evolve their methods, ***"Once a particular approach is identified and countered by law enforcement, traffickers swiftly devise alternative strategies",*** an expert opined.

Perpetrators used different technology platforms at various phases of the trafficking process like social media apps i.e. Facebook, Kik, Telegram, Instagram, TikTok, WhatsApp, and Omegle. To communicate with victims, even job sites are used to identify, contact, and recruit the victims. Omegle, a free web-based online chat service, operated from 2009 to 2023, and allowed users to socialize with others without the need to register. The service randomly paired users in one-on-one chat sessions where they could chat anonymously. On November 22, 2023, the BBC published an extensive report on the role of a lawsuit and out-of-court settlement that resulted in shutting down the site. Among the technologies used to distribute the profits/proceeds of the crime, Bitcoin was predominant. While digital payment transfers were used, victims were also compelled to carry out these transfers through their account.

Typically, any app that facilitated contact and communication between two or more people could be used. During the Covid-19 pandemic, several such apps emerged, and with an extra feature like a button, participants could express an interest in sex, and the same was thus abused by the traffickers. The traffickers could open an account on behalf of victims on these platforms and offered services. Criminals were using X (formerly Twitter) to post links of pornographic sites and to offer adult services, and easily searchable with known keywords. Further, online gambling platforms were also found to be used for communication with criminal intent.

4.3.4.2 Challenges faced when securing cooperation from the technology firms

Experts shared that a significant challenge faced by prosecutors was the requirement for specific information during investigations, making it difficult to obtain cooperation from platforms hosting illicit activities. Despite these challenges, victim protection laws, such as Article 57 of Austria's Asylum Act, provided essential legal rights and support to victims throughout investigations, underscoring the strength of legal provisions in safeguarding victims' interests.

When it came to seeking information from technology companies operating outside of the EU, law enforcement officers would initiate an investigation and obtain an arrest warrant from the court. The warrant was sent to their counterparts in the respective countries where the server was located. Typically, these counterparts cooperated by instructing the technology companies to provide the requested information. In case cooperation was not forthcoming, the matter was escalated to the EU forum and pressure was applied. However, experts acknowledged limitations in the laws, which prevented prosecution in case the company did not comply. One of the experts provided an example of a specific case involving victims in China, wherein their counterparts facilitated the examination of the victim at the Austrian Embassy.

European LEAs have an agreement to share information to resolve crimes. Various networks, backed by EU agencies such as Europol and local police, collaborate to ensure justice and prosecution. Additionally, mutual networks supported by EU agencies, police, and officials help facilitate justice in cross-border crimes.

4.3.4.3 Role and Accountability of the Technology Enablers

Addressing the accountability of technology companies had become a central focus, particularly in discussions at the European Union level. The primary objective was to establish mechanisms that encourage reporting and collaboration between these companies and investigating agencies. This recognition stems from acknowledging the significant role that technology companies could play in facilitating and combating criminal activities on their platforms. Notably, there has been a shift in the willingness of technology companies to cooperate, reflecting an increased acknowledgment of corporate responsibility when it comes to combating crime.

Moving beyond the scope of technology companies, Austria had extended its collaborative efforts to various private entities, including both technology and money transmitting companies. This broader collaboration was essential in recognizing the financial aspects of human trafficking. Entities involved in financial transactions played a crucial role in understanding and tracing the monetary aspects associated with these criminal activities. Cooperation from such entities becomes indispensable in unravelling the financial networks that support human trafficking operations.

Blockchain technology has emerged as a potential game-changer in this realm. While it presents its own set of challenges, it offers a transformative solution for investigating and intervening in human trafficking cases. Blockchain provides a traceable system for financial flows, creating a transparent and permanent record of transactions. This feature becomes particularly valuable in tracking the movement of funds related to human trafficking, providing LEAs with a promising avenue for investigation and intervention.

While discussing the role of technology enablers, the experts highlighted that data protection laws and ethical concerns become a hurdle when seeking support from the intermediaries and monitoring web-activities of the users.

Ensuring the accountability of technological platforms in combating human trafficking posed challenges. One of the foremost was when platforms were unwilling to censor illicit activities or with servers located outside Austria. International cooperation becomes crucial in holding such platforms accountable, especially when engaging with platforms like Facebook and Telegram to address human trafficking activities. Cooperation from these platforms is vital for effective law enforcement action against human trafficking facilitated through online platforms, opined the experts.

4.3.5 Best Practices and Technological Solutions to Combat CEHT

Austria has constituted Cyber Units specializing in cyberspace, which monitor the web traffic for specific keywords that are typically associated with human trafficking. Austria has also constituted a 'Cyber Competence Centre', which assists the prosecution in analyzing digital evidence and presenting findings to the court. Usage of blockchain technology was suggested to secure the financial transaction trails.

Austria uses Web-Crawlers on surface web, to identify potential services of sex-trafficking. The tool was fine-tuned using a careful selection of keywords, for example, Ukrainian women/ girls, sex services, marriage, wedding, etc.

Interestingly, as shared by an expert, Austrian authorities are using technology to spread awareness among Ukrainian women refugees, who are a vulnerable group. Anticipating that these war refugee women could be targeted by the traffickers, Austrian police hosted awareness materials on their website since February 2022. The campaign aimed to make these women aware of safety practices such as asking the name of person/ agent, asking the destination, noting down car number, etc. Furthermore, Austrian LEAs carried out proactive intervention on finding mention of Ukrainian women/ girls (potentially vulnerable targets for the traffickers) on adult service websites, by warning the operators not to exploit / offer sexual services of these women if it was not voluntary.

Police are using OSINT analysis to identify and monitor as to who is behind a social media account / activity. The 'Dark Net Unit' of the police also monitors traffic on the dark net and assist in monitoring the activities related to known cases of CEHT on the dark net.

An expert shared that the 27 member countries of the EU had agreed to cooperate in dealing with CEHT. They take action to close the social media/ online accounts of those suspected to be involved or reported to be involved in human trafficking. As per statistics, in 2022, approximately 2700 accounts were identified as involved in suspicious activities. Europol was requested to close these. Approximately 400 accounts were closed within a month of reporting.

On 06 September 2022, a one-day hackathon was organized wherein experts from 20 countries in the EU assembled to investigate the online platform to identify/ confirm their usage for human trafficking, identify the traffickers, and the victims. The event marked a significant initiative of multiple international authorities coming together to address the problem of human trafficking.

The experts suggested the need to educate/ spread awareness to the potential victim group/ marginal groups, especially children, regarding the dangers of the technology platforms, healthy online usage, and dress codes to be kept in mind while using these technology platforms.

Police believe that the mobile phone gives vital information about a person and their activities. However, it often took months to obtain the forensic report of the mobile phone data from the labs. To address this issue, the Austrian Police developed a software called **Law Enforcement Analysis Project** (LEAP) with an Austrian company after two years of research. LEAP gave a detailed report of a mobile phone within minutes (5-10 minutes). It gave a report about contacts, also listing the frequently contacted, contacts with longest cumulative call durations, etc. It also analyzed emails and messages. It supported multiple languages and dialects and could plot on a map showing the native places of the dialects used in conversation found on the phone. It analyzed location data and plotted it on a map. The software analyzed 6000 photos per minute. It also analyzed the documents on the phone and could flag terrorist symbols, radical papers, child porn, etc. available on the phone. The content analysis features could be customized by the investigating agency.

Austrian police, in cooperation with an adult services provider (a German website/ app kaufmir.com i.e. Buy me.com), added an emergency button to the interface. This button could be used by the service buyer to raise a silent alarm along with sending a short message to the legal department of police. The button was to be used when a buyer suspected that the girl/ woman offering sex services was possibly doing so under coercion and was likely a victim. The legal department thereafter alerted the police unit on the hotline.

In order to police the online gambling space more effectively, the Austrian police were able to get the game/app modified to allow the virtual presence of police on these platforms. The gamers/ gamblers could give information/report an incident to these virtual police, when needed.

Contributors

Dr. Wolfgang Spadinger, Director, Deputy National Anti-Trafficking Coordinator, Federal Ministry, European and International Affairs, Division for Border Issues and the Fight against Trafficking in Human Beings

Brigadier Gerald Tatzgern, Head, Joint Operational Office against Human Smuggling and Human Trafficking, Federal Bureau of Investigation, Austrian Ministry of the Interior

Ms. Konstantina Stavrou LLM, University Assistant, Fellow of the Austrian Academy of Sciences, Department of Constitutional and Administrative Law, Faculty of Law, University of Vienna, Program Human Rights & International Criminal Law, Ludwig Boltzmann Institute of Fundamental and Human Rights

Profile of Organizations

Division for Border Issues and the Fight Against Trafficking in Human Beings

The Division for Border Issues and the Fight Against Trafficking in Human Beings in Austria is a significant part of the country's efforts to combat human trafficking. Austria has been actively

working on this issue since the establishment of the Task Force on Combating Human Trafficking in 2004.

Joint Operational Office against Human Smuggling and Human Trafficking

The Criminal Intelligence Service Austria (BK) was established in 2002 and is part of the Directorate-General for Public Security of the Federal Ministry of the Interior. In 2016, the BK opened a new Joint Operational Office (JOO) combating human smuggling and human trafficking in Vienna. The JOO serves as a regional operational platform for international investigations into migrant smuggling organized crime groups. JOO can also serve as a contact point for third parties in the source region of migration.

Ludwig Boltzmann Institute of Fundamental and Human Rights

The Ludwig Boltzmann Institute of Fundamental and Human Rights (LBI-GMR) is the largest extramural research institute in its field in Austria. It advances human rights research, fosters a human rights-based approach, and contributes to improving the human rights realities of individuals in Austria and abroad. Its interdisciplinary outlook and commitment to applied research and the third mission set it apart. The institute conducts basic and applied research which is current, international, inter-disciplinary, and translational.

4.4 The United Kingdom (UK)

Facilitated by the British High Commission, Hyderabad, discussions were held with the Modern Slavery Unit of the UK Home Office to understand the manifestations of CEHT in the UK. This chapter also includes the contributions of a leading British expert with vast experience on online child sexual exploitation, currently serving in various capacities with the UK Council on Child Internet Safety, UK Children's Charities' Coalition on Internet Safety, London School of Economics and Political Science, ECPAT International (Ending Child Prostitution in Asian Tourism) and the United Nations ITU.

4.4.1 Trends and Patterns of CEHT: Role and Usage of Cyber Technologies

4.4.1.1 Purpose of Exploitation, Modus Operandi, and Profile of Victims

Experts in the UK shared that while sexual exploitation was prominent, labor exploitation also played a significant role, often facilitated through social media and marketplace platforms, whereas sexual exploitation was perpetuated through adult service websites.

The use of technology in human trafficking within the UK has become increasingly prevalent, with online platforms serving as significant enablers for such criminal activities. Specifically, adult service websites had emerged as hubs for sexual exploitation, where individuals advertise, negotiate, and facilitate sexual services. These websites provided a platform for exploiters to manipulate, coerce, and force individuals into selling sexual services. Social media (e.g. Facebook) sites, classified advertisements, and user generated posts on social media, were suspected to be used for labor exploitation, though the expert reiterated that this was based on anecdotal evidence.

The expert who had experience of working on CSAM, in his opening remarks stated that, unlike in the United States where CSAM is considered as child trafficking, in the UK it is seen as sexual exploitation of children. In terms of CEHT, the expert stated that in the UK**,** Employment sites were the major avenues for traffickers to trap individuals for servitude, prostitution, and slavery. Modelling agencies targeted young boys and girls with promises of fame and wealth in their modelling career. Traffickers exploited this process to gain access to compromising content, subsequently using it for blackmail and coercion. These pictures were most often advertised on adult sex services sites indicating a chain of physical to virtual networks that controlled the sex trafficking syndicate.

Expressing concern about the **lack of reliable data on human trafficking** in the UK, the expert shared that only a fraction of the cases came to light, thus, if one relied only on the available data, it would not correctly represent the scale and magnitude of the problem in the country.

While specific data regarding online trafficking cases may require further analysis, it is to be noted that victims, comprising mostly women and girls, encompassed UK nationals and individuals from other countries. It was highlighted that a significant portion of trafficking cases in the UK involved children who enter or are smuggled into the country illegally through boats and subsequently go missing. **Human traffickers actively sought out these vulnerable children, taking advantage of their undocumented status, making them untraceable.** Even when placed under the care of Local Authorities, these children remain at risk, as traffickers persistently lurked around the facilities where they are housed, and often disappear, ending up in situations of domestic and sexual exploitation.

Poverty constituted the most significant vulnerability for individuals being trafficked. These children often came from impoverished backgrounds, attempting to escape violence in their home countries.

4.4.1.2 Nature of Exploitation and Revenue Model

Discussing the online nature of human trafficking, **the link between CSAM and CEHT** was highlighted whereby traffickers arranged for children to perform live sexual acts on camera. Countries such as the UK and many other countries in Europe and the United States constituted the demand for such content.

Giving the example of the Philippines, **organized gangs** arranged for children in small villages to be brought to a place where they were groomed to live stream sexual acts with viewers from the United States, UK, and other countries having the option to dictate the nature of sexual acts they prefer. Such activities were also seen in Cambodia, Thailand, and Sri Lanka. It was the poverty of such nations that often led the families of these children to engage in these criminal activities, and in many instances, it was also by the use of force, coercion, and blackmail.

The revenue model varied, as in some instances it was just a nominal amount of USD 50 -100 (₹4,000 - 8,000/-) to subscribe to online platforms. This was indicative of the huge number of subscribers to such platforms.

"Skype" emerged as the major platform for such live streaming. Since the streaming was encrypted, it was difficult to track and trace the scale of such exploitation by Microsoft. Facing extreme backlash, Skype temporarily ended its operations in the Philippines pending enquiry.

Self-generated live streaming was another phenomenon where young children were groomed to stream live, where it was difficult to identify the perpetrators facilitating such nefarious activities.

4.4.2 Legal Framework to Combat CEHT

4.4.2.1 Legal Framework, Challenges in Application and Proposed Changes

In the legal framework of UK, it is notable that the acts of buying and selling sex in England and Wales was not inherently illegal. However, activities associated with prostitution and sex work, especially those linked to exploitation, such as controlling prostitution for gain or paying for sexual services from exploited individuals were considered offenses under the law.

Adult Service Websites (ASW) host vast amounts of intelligence about modern slavery and human trafficking, making it a critical focal point for law enforcement efforts. This legal context highlighted the importance of regulating online platforms, particularly ASWs, where sexual services were advertised and facilitated.

The expert shared that while there was currently no special legislation in force in the UK to address CEHT, there were general laws to address human trafficking such as *The Modern Slavery Act, 2015*, was used in all cases of human trafficking. Interestingly, the expert when speaking of technology as an enabler mentioned that the UK for many decades believed self-regulation was the ideal option. It was only in recent times that the country recognized the need for accountability of Technology Firms as well as putting in a legal framework, which could act as a deterrent. It was this understanding that led to the ***Online Safety Act of 2023*** which represented a critical legislative step in addressing the multifaceted challenges of ensuring the safety of children in the digital realm. It would be the first of a kind legislation that covered comprehensive threats to children, and focused on the health and safety of children. **It is currently under review and has to complete several steps before it is enforced as a law.**

The Online Safety Act is a comprehensive piece of legislation that aims to deliver crucial protection for children, prevent the dissemination of illegal content, and uphold the principles of free speech. It imposed obligations on companies operating online platforms to actively protect users, enforce clear terms of service, and promptly remove illegal content. These responsibilities were essential in ensuring that online platforms prioritize user safety and take proactive measures to prevent the spread of harmful material.

A notable aspect of the Online Safety Act was its emphasis on holding tech enablers accountable for the content hosted on their platforms. Under this legislation, online platforms were required to take measures to mitigate the risk of illegal activity, including human trafficking and exploitation. This accountability stressed the significant role of platform operators in combating online exploitation and creating a safer digital environment for all users.

Under this proposed Act, companies would be mandated to implement robust measures aimed at protecting children in online spaces, particularly from CEHT. **The legislation emphasized**

the importance of proactive risk assessment for Child Safety within digital platforms and services. Companies operating in the online space would be required to conduct comprehensive risk assessments to identify, evaluate, and mitigate potential threats related to child exploitation and trafficking. One instance of the kind of threats it covered was the Modelling agencies or Employment service portals, which would be legally obliged to survey and present Risk Assessments of threats to children. These assessments would be submitted to the Regulator, and if the Risk Assessment was high, they would be legally obliged to mitigate this Risk.

The challenge here was with self-generated images of children that appeared that they were voluntarily taken. But the question remained of the consent of a child having that knowledge and its consequences, though those grooming them were seldom seen or caught. The images made children more vulnerable to multiple exploitations.

Furthermore, a significant challenge posed by AI or deep fakes related to encryption. Between the years 2019-2022, approximately 100 million reports of CSAM were received by the NCMEC, out of these 864 were identified by Apple. While the number may seem small, these were the only ones that were detected, and there may be many more, if not identified by Apple in time due to the robust encryption and protection of data provided by the company. This encryption prevented scanning and accessing material of a person, even if it was explicit. Hence, there needs to be a mechanism to look into the encryption policy of such companies and scan the encrypted data they store.

There is also a new law required to regulate payments for such CSAM images. Currently, the UK Anti Money Laundering Law i.e., The Proceeds of Crime Act (POCA), 2002 had made banks wary about whom they were providing financial access to for carrying out transactions. POCA could be used to combat CEHT. By prosecuting traffickers and seizing their assets, the government could disrupt trafficking networks and thus prevent traffickers from profiting from such crimes.

Challenges in Application

Ensuring that the Online Safety Act effectively safeguards users without unduly restricting legitimate online activities, does require careful consideration. Efforts were underway to address these challenges and ensure the effective implementation of the Online Safety Act. This included developing clear guidelines, providing adequate resources, fostering collaboration between stakeholders, and remaining vigilant against emerging threats in the online space.

4.4.2.2 Support System for Victims

Victim protection and compensation in the UK is not robust, as pointed out by the expert**.** Although some protection mechanisms were in place on paper, i.e. victims do not have to come to court, they cannot be re-interviewed, etc., yet implementation varied across the country. Compensation mechanisms were very weak in the UK.

There is the existence of the National Referral Mechanism (NRM), a process that serves the victims of slavery in the UK to access support. Additionally, Independent Trafficking Child Guardians play a crucial role in providing support to child victims of trafficking. However, these aspects require further exploration.

In contrast, the expert shared an example from the United States, the case of *Paroline v. Unknown Amy*. In this case, the U.S. Supreme Court had ruled that defendants could be held liable for a child pornography victim's loss. The decision emphasized individual contribution to harm and a compensation of USD 3.4 million was paid to the child victim, which was mutually agreed upon by both parties.

4.4.3 Challenges in Investigation, Prosecution, and Cooperation from Technology Firms

4.4.3.1 Challenges faced in investigation, prosecution, and cooperation from Technology Firms

The cooperation of Technology Firms in investigating cases and providing immediate response mechanisms to take proactive action, was reported to be varied and in most instances poor in cases of CEHT. Regarding the time taken by Technology Enablers to respond to such requests, experts shared that if the matter pertained to matters of life and death the response was immediate, but in other cases it could take many months. Often it also depended on personal relations with the Technology companies to expedite cooperation. Citing a live case scenario where a girl from Birmingham tried to commit suicide online, this was noticed by a viewer living in the United States who informed the local police, who in turn informed the FBI, and the FBI alerted their counterpart. Because of this swift action the girl was prevented from committing the act of suicide.

While there was no time requirement fixed by the law to take down CSAM by the technology companies, yet a good practice followed by them was taking the material down upon receipt of legal notice by LEAs. In Britain especially, companies took down the material within a few hours. For example, when payment gateways like MasterCard and Visa sent a notice to MindGeek, a Canadian adult entertainment conglomerate; the company removed all CSAM content within 72 hours upon receiving the legal notice to remove CSAM. However, this was not always the case as some companies ignore the notices.

It was observed by the experts that Technology companies do not want to spend time and money on safeguarding protocols as it would mean investing on engineering that would not generate profits. The new OSA law addressed this whereby Technology companies would have to obey the law, even though they might find room to save money from surveillance mechanisms. The requirement to undertake Risk Assessment meant that if the companies lied about the risks, the heads of such companies would be imprisoned. The history of such a law could be traced to the financial crash, where the banking laws evolved to jail company heads for lying. Similar punitive provisions under OSA provided for fines and threat of jail to Technology companies and could serve to act as a deterrent once the law is implemented. Against this backdrop, the expert stressed on the need to build a narrative where safer internet made for better business practice. The OSA proposes to make all technology platforms responsible for content on their platform. It is aimed to ensure child safety, protect the users, and delete illegal contents on priority or minimize the duration for which such content remains hosted on their platforms.

Some technology solutions or practices shared by the experts included a tool developed by the National Crime Agency while working with some ASWs, wherein, ASWs helped them by giving certain information, for viewing/searching contents on their platforms. These web crawlers were able to scan the difference between voluntary and involuntary sexual services.

AI based content moderation, hash scanning algorithms, etc., are also being used alongside systems ensuring multi-layered safety verification, strong KYC, and secure payment methods that are being developed. Campaigns have been undertaken to make people aware of possible harms online.

4.4.3.2 Collection and storage of digital evidence and status of digital forensics

The expert shared that the Regional Organised Crime Units (ROCUs) played a significant role in handling such cases, with highly trained professionals having technical expertise. While they specialized in various aspects of law enforcement, including cyber-crime, their expertise ensured the effective collection and handling of digital evidence in cases involving cyber-enabled crimes. The court's perception of digital evidence varied depending on the specifics of each case. For instance, in cases where traditional evidence such as the victim's testimony was lacking, digital evidence could play a crucial role. An illustrative example involved building a case around information provided on the ASWs. Despite the absence of the victim's testimony, successful convictions have been obtained based on such digital evidence.

4.4.3.3 Preparedness of criminal justice system to deal with CEHT

Experts shared that there was an ongoing effort to enhance awareness and skills within the criminal justice system, and collaboration with the Crown Prosecution Service (CPS) was underway to address these concerns.

Contributors

Ms. Sam Lee, Public Safety Group, Modern Slavery Policy Unit, UK Home Office

Mr. John Carr, OBE (Order of British Empire)
Member, Executive Board, UK Council for Child Internet Safety
Secretary, UK Children's Charities' Coalition on Internet Safety
Visiting Senior Fellow, London School of Economics and Political Science
Advisor, ECPAT International (Ending Child Prostitution in Asian Tourism)
Senior Expert Adviser, United Nations ITU

Profile of Organizations

Modern Slavery Policy Unit

The Modern Slavery Policy Unit, co-led by Justice and Care and the Centre for Social Justice, has been created with the core mission – to keep modern slavery at the top of the British political agenda. This means better understanding of the nature and scale of modern slavery, increased investment, and sophisticated national response to fight it appropriately.

UK Council for Child Internet Safety

The UK Council for Child Internet Safety (UKCCIS) was set up in 2008 and charged with bringing together government departments, LEAs, academia, private industry, and third-sector representatives such as charities and voluntary groups to collaborate on strategies to ensure child internet safety.

Ending Child Prostitution in Asian Tourism (ECPAT)

ECPAT's global campaign to end child sexual exploitation was launched in May 1990 when a small group of concerned individuals gathered in Chiang Mai in Northern Thailand. Since then, ECPAT has worked to better understand the web of child sexual exploitation through research and pushed for the critical systemic and social changes necessary to eliminate this scourge together with governments, intergovernmental institutions, the private sector, civil society and the general public, including children themselves.

International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is a specialized agency of the United Nations responsible for many matters related to information and communication technologies. It was established on 17 May 1865 as the International Telegraph Union, significantly predating the UN and making it the oldest UN agency. The ITU was initially aimed at helping connect telegraphic networks between countries, with its mandate consistently broadening with the advent of new communications technologies.

4.5 Thailand

Facilitated by the Royal Thai Embassy, Chennai, discussions were held with the Special Case Officer and Head of the Centre for International Cooperation, Bureau of Human Trafficking Crime, Department of Special Investigation (DSI) in Thailand. Drawing on his personal experiences in handling such cases, the expert provided deep insights on the scenario of CEHT in the country.

4.5.1 Trends and Patterns Of CEHT: Role and Usage of Cyber Technologies

4.5.1.1 Purposes of Exploitation, Modus Operandi, and Victim Profiling

Highlighting poverty as a significant driver of human trafficking in Thailand, the expert emphasized that financial despair often compelled individuals into vulnerable situations, and traffickers exploited this economic need and the resulting vulnerability of potential victims. Moreover, **Thailand played a complex role in human trafficking, serving as an origin, transit, and destination point**. Thai women, seeking economic opportunities, travelled to various countries such as the UAE, Japan, and Korea, and engaged in the sale of sexual services. This encompassed both consensual and forced sexual exploitation. **Additionally, the expert brought attention to Thailand's position as the second-largest producer of CSAM globally, following the Philippines.**

Interestingly, it was shared that while 90 percent of the local population constitutes poor people, everyone has a device and is connected to the internet and social media. Most of the unskilled labor in search for money are easily lured into going abroad and once they reach the destination they are forced into exploitative situations. Thailand has emerged as a major destination for luring people into being the victims of and, carrying out **cyber scamming**. Perpetrators targeted vulnerable individuals, including young men from India, Pakistan, Ethiopia, etc. by offering lucrative job opportunities in Thailand. False promises of high-paying jobs and opportunities for career advancement convinced victims to travel to Thailand on tourist visas, unaware of the exploitation awaiting them. Upon arrival in Thailand, they are made to cross over into Cambodia and Myanmar, and coerced into participating in cyber scamming activities, including fraudulent schemes conducted online. Perpetrators employed various tactics to control and manipulate victims, including threats of physical harm and exploitation of vulnerabilities. Last year alone, more than 2,000 victims were identified in Thailand.

In the context of technology, the expert outlined how online platforms were exploited for illicit purposes. Social media platforms, such as Facebook and TikTok, were used to post job advertisements, creating a digital space for the recruitment of individuals for sexual and labor exploitation. This brought out the multifaceted role of technology in contemporary human trafficking, both as a tool for exploitation and a means of recruitment.

The expert shared that prior to Covid-19 pandemic, there were three prominent forms of human trafficking in Thailand. Firstly, minors from neighbouring countries such as Myanmar, Laos, and Cambodia were brought to Thailand and forced into prostitution. Underage sex tourism is a major activity in human trafficking where minors are exploited. Secondly, those over 18 years, who enter Thailand illegally from Cambodia or other places are exploited for sexual purposes, and thirdly, exploitation for the purpose of labor exploitation. Traditionally, this had been done for labor in the fishing industry and children are also forced into begging.

During and after the Covid-19 pandemic, this has transformed to other purposes of exploitation such as forcing people to carry out cyber-scamming, loan frauds, cyber-crimes, CSAM, etc. In such instances, victims were also forced to cheat and trap more victims.

4.5.1.2 Victim Profiling

The individuals were generally poor and desperate victims from Thailand and neighbouring countries. While young girls and women were trafficked for sexual exploitation, men mostly were trafficked for labor trafficking. The expert shared that victims were also being used for forcing others into cyber-crimes, including people from India, Pakistan, and Ethiopia.

4.5.1.3 Nature of Exploitation

Prior to the Covid-19 pandemic, as per the reported cases, the nature of exploitation was seen to be only physical, however, this changed during and after the pandemic, with exploitation now taking place through both mediums – physical and virtual.

4.5.1.4 Revenue Models

The expert provided insights into the financial aspects of human trafficking in Thailand, noting that in almost 95 percent of cases, transactions occurred through e-wallets and digital platforms, with cash being used in only 5 percent of instances. Drawing attention to the ease of conducting such illegal business, the expert highlighted that opening bank accounts in Thailand was extremely simple, where the process could be completed online via phone, leading to widespread banking accessibility among the population. Exploiting this, criminals engaged in purchasing "***Mule Accounts***" from unsuspecting individuals, often those facing financial difficulties, by paying a nominal amount.

The expert also spoke about the increasing use of crypto currency and digital wallets, such as "***TrueMoney***". The adoption of these technologies added a layer of complexity for LEAs, as tracing and investigating transactions conducted through these digital means become more challenging. This stressed the need for enhanced cyber security measures and adaptive investigative strategies to address the evolving financial landscape associated with human trafficking in Thailand.

4.5.2 Legal Framework to Combat CEHT

4.5.2.1 Legal Framework

On a positive note, the expert shared that in Thailand, a comprehensive legal framework was in place which addressed CEHT and associated crimes. Thailand's legal framework included statutes specifically targeting human trafficking, such as the Prevention and Suppression of Trafficking in Persons Act, which criminalized all forms of trafficking in persons, including for labor and sexual exploitation. Additionally, labor codes regulated fair treatment of workers, ensuring that labor rights are protected, and employers were held accountable for any exploitation. These laws were constantly evolving to adapt to the challenges posed by modern technology and cyber-crime and encompassed a wide range of offences, including hacking, identity theft, online fraud, and trafficking-related crimes facilitated through digital platforms. The Computer Crime Act of 2007, for example, criminalized various cyber-related offenses and provided LEAs with the legal tools necessary to investigate and prosecute cybercriminals.

Thus, Thailand's legal framework demonstrated various strengths in addressing CEHT and related crimes. The Prevention and Suppression of Trafficking in Persons Act criminalized all forms of trafficking of persons, ensuring that perpetrators were held accountable for their actions.

4.5.2.2 Support System for Victims

Furthermore, the legal framework included provisions for victim protection, including mechanisms for repatriation and support services. NGOs played a vital role in providing support services to victims and advocating for their rights within the legal system. Legal protection ensured that victims were afforded the necessary safeguards throughout the legal process, including access to legal representation and support services. Victims, both male and female, benefitted from various measures aimed at ensuring their safety, well-being, and access to justice.

The International Organization for Migration[65] (IOM) played a vital role in assisting victims of human trafficking in Thailand. The IOM worked in collaboration with governmental and non-governmental partners to provide comprehensive support to victims, including shelter, medical care, legal assistance, and repatriation services. Through its efforts, the IOM aimed to ensure that victims receive the necessary assistance and support to rebuild their lives and reintegrate into society.

Additionally, efforts are being made to raise awareness about human trafficking and educate the public about the rights of victims.

4.5.3 Challenges In Investigation And Prosecution Cases Of CEHT

4.5.3.1 Collection and storage of digital evidence and status of digital forensics

By law, LEAs had the authority to request details from technology companies for the purpose of carrying out investigations, and the time frame for getting this information varied from case to case. Whenever required they requested bank statements, call recordings, telephone numbers, or emails from the respective companies. Depending on the platform and company, if the information was required urgently such as phone numbers or email, it would usually be obtained within 24 hours.

While there were no standardized Standard Operating Procedures for obtaining or ceasing evidence from a crime scene, in some important cases LEAs took the services of NGOs to assist in collecting digital evidence. However, in court, digital evidence provided by the law enforcement officer is acceptable, but it's not accepted if the digital evidence was provided by NGOs. Furthermore, by law, this digital evidence does not require to be certified by a forensic laboratory or expert.

4.5.3.2 Challenges faced in Investigation and Prosecution of Cases

Despite the comprehensive legal framework in place, the expert opined that addressing CEHT in Thailand presented several challenges that hindered effective investigation and prosecution. Jurisdictional issues often arose in cases involving cross-border crimes, complicating coordination with other countries and delaying legal proceedings. Additionally, the transnational nature of cyber-enabled crimes made evidence gathering complex, especially when dealing with multinational technology companies and encrypted platforms that may not readily cooperate with law enforcement authorities.

A significant challenge was also the lack of awareness and understanding of cyber-enabled crimes among law enforcement officials and the general public in Thailand. This lack of awareness hampered efforts to effectively identify, investigate, and prosecute cyber-enabled human trafficking cases. Moreover, trust issues between stakeholders, including victims, technology companies, and LEAs, further impeded cooperation and collaboration in combating cyber-enabled crimes.

Resource constraints also posed a challenge, with limited human and technological resources slowing down LEAs ability to conduct thorough investigations and prosecute perpetrators

65 IOM Thailand

effectively. Additional funding, manpower, and technological capabilities were essential to support Thailand's response to cyber-enabled human trafficking and related crimes, stated the expert.

4.5.4 Cyber Technology as an Enabler: Challenges and Responses

4.5.4.1 Various Technologies Present in the Country Being Exploited for Human Trafficking

Some of the platforms listed by the expert for facilitating the crime of human trafficking included Facebook, Facebook Messenger, Tinder, TikTok and WhatsApp. Elaborating on the same the expert shared two examples on how these platforms were used to recruit and exploit victims:

Case 1: An advertisement was posted on Facebook regarding the possibility of working in Dubai, offering free air tickets and visa. However, the opting women were put into forced prostitution. On the rescue of a victim, it was revealed that they had to handle 50 customers a day and also that during periods they would be forced to have sex without condoms and not paid any money.

Case 2: Students and young people typically used Tinder and TikTok, and cases had been reported wherein they had been befriended by boys/girls and asked to share their videos, which were later used for purposes of sextortion.

4.5.4.2 Challenges faced in securing cooperation from the Technology Firms

The expert highlighted the challenge of obtaining cooperation from technology companies in addressing human trafficking. While technology played a role in facilitating these illicit activities, securing support from technology companies proved to be a complex endeavour, including compliance with Thai Law.

Tech companies operating in Thailand were subject to Thai laws and regulations governing their activities. However, enforcing accountability posed challenges, particularly when dealing with companies based in foreign jurisdictions that may not fully comply with Thai legal requirements. International cooperation was crucial for holding technology enablers accountable for their role in facilitating cyber-enabled crimes, including human trafficking.

4.5.5 Best Practices and Technological Solutions to Combat CEHT

The expert highlighted how technology was being used to collect digital evidence. Victims were asked to deposit their mobile phones when they filed their complaint. The data was extracted as evidence from mobile phones and the investigating officer asked the service provider to provide information based on phone number, etc. to determine how the trafficker contacted the victim or how the victim talked to the trafficker, etc. Further, campaigns have been conducted on Facebook and TikTok to educate people and raise awareness on the issues of cyber-scamming, as a prevention measure against CEHT.

Contributor

Mr. Thapana Bhasathiti Sanyabutra

Special Case Officer and Head of the Centre for International Cooperation, Bureau of Human Trafficking Crime, Department of Special Investigation

Profile of Organizations

Department of Special Investigation

The Department of Special Investigation (DSI) is a department of the Ministry of Justice of Thailand. It operates independently of the Royal Thai Police and is tasked with the investigation of certain "special cases". These include complex criminal cases, those affecting national security, those involving organised criminal organizations and those potentially implicating high-ranking government officials or police officers.

4.6 Spain

Facilitated by the Counter Extremism Project,[66] this section draws on contributions by one of Spain's leading researchers and jurists in matters of human trafficking. This expert is also responsible for the Data Culture in Human Trafficking project,[67] which aims to raise awareness and train professionals and experts to generate, analyse, and manage data on human trafficking for the identification and assistance to victims of this circumstance.

4.6.1 Trends and Patterns of CEHT: Role and Usage of Cyber Technologies

4.6.1.1 Purposes of Exploitation, Modus Operandi, and Victim Profiling

The expert mentioned that the major purpose of human trafficking in Spain included sexual exploitation of women and children, labor exploitation in the agriculture industry, and CSAM, with several apps and platforms being used for grooming, and sexual exploitation of children.

As per the Home Affairs Ministry,[68] the number of human trafficking victims identified in Spain during the year 2020 was 269. Persons identified in sexual trafficking processes were 160, of which 90 percent were women (145) and 7.5 percent were men (12). In this modality, the most identified trafficking situation in Spain, recognized minors who represented barely 2 percent of the total number of victims: 2 girls and 1 boy.

In a labor trafficking situation, 99 persons were identified: 65 women, 33 men, and one girl. For the commission of criminal activities, 5 female and 2 male victims of trafficking were identified. Finally, two girls and a woman were identified as victims of forced marriage trafficking, and

66 About CEP | Counter Extremism Project

67 What we know and how we tell it: data culture in human trafficking (comillas.edu)

68 WHAT DO WE KNOW AND HOW WE TELL IT_FINAL_12.05.22.pdf (comillas.edu)

no victims for the purpose of begging were identified. National and international authorities, professionals, researchers, and experts who work with this complex problem agreed that the available data did not accurately reflect the social processes that facilitate the trafficking and exploitation of people in Spain.

Most of the victims of the cases under investigation in Spain were trafficked by criminal organizations or criminal groups, usually for the purpose of sexual exploitation or to commit petty crimes. But sometimes trafficking was carried out by "individual traffickers" such as paedophiles who surf the internet, family members in the sphere of domestic exploitation, or relatives of the victims themselves.

The forms of recruitment were inherently linked to the nationality of the victims and the offenders. The ways of operating changed substantially depending on whether the networks were Nigerian, Chinese, Romanian, or South American.

Among the victims from Eastern Europe, the "*lover boy*" method continued to be the most common. The recruiters approached their victims, usually from poor backgrounds and low educational level, and managed to establish a relationship with them and later on convince them and their families to travel to Spain. In order to convince them, they offered the victims work in the hotel or restaurant sector, caring for the elderly or children, etc. Sometimes, the deception was not in the type of activity but in the working conditions. Some victims knew the activity they would carry out, mostly prostitution, but did not know the semi-slavery conditions and even the real debt they would have towards their traffickers.

Social media and the internet are now one of the top means to recruit new victims. During the Covid-19 pandemic the use of online technologies reached an outstanding increase. The figures of child victims identified continue to be limited compared to the total number of victims identified. This did not mean there were no child victims, but rather the children were hidden, and it was difficult to detect them.

Given Spain's popularity as a tourist destination, the expert shared that this posed unique challenges related to tourist-related trafficking. In areas with high tourist traffic, such as coastal regions and major cities, there was an increased risk of trafficking for sexual exploitation and forced labor. While some individual hotels and enterprises took steps to address this issue independently, there was a lack of systematic efforts and awareness on the connection between tourism and trafficking and this posed a significant challenge in effectively combating trafficking in tourist areas and protecting potential victims. The expert stressed the need for greater collaboration between the tourism industry, law enforcement, and civil society organizations to raise awareness, identify potential trafficking situations, and provide support to victims. Additionally, more comprehensive policies and strategies were needed to address the root cause of tourist-related trafficking and prevent exploitation in tourist destinations.

Victim Profiling

It was shared that most of the people vulnerable to trafficking and exploitation were in search of employment. Spain also had a huge number of "children in poor situations" and these children were also prone to getting trafficked and abused.

Furthermore, people from various Latin American countries could easily get entry into Spain without a visa, and ended up getting trafficked for sexual and labor exploitation.

4.6.1.2 Nature of Exploitation and Revenue Models

While the expert shared that as per her knowledge the exploitation was mostly limited to physical places, she stated that there may be instances where there was a recording made of the exploitation and that could be shared online, and this was permanent and could be viewed multiple times.

The expert shared that as prostitution was legal, payment could be in any form. It could be found on many websites which have a very secure/guaranteed form of payment portal. It was difficult to know the exact amount of money being transferred, and the police could only have an estimation or rough idea of the amount.

4.6.2 Legal Framework to Combat CEHT

4.6.2.1 Legal Framework and Challenges in Application

While there was no single comprehensive law dedicated solely to trafficking, Spain's legal framework was used to address trafficking through a combination of laws and regulations covering different aspects of prevention, prosecution, and victim protection. These included provisions within the Penal Code, the Organic Law on Comprehensive Protection Measures against Gender Violence, and other relevant legislation related to immigration, labor rights, and victim protection.

The introduction of trafficking into Spain's criminal law is relatively recent, dating back to 2010. Before this legal amendment, trafficking cases were often categorized as smuggling offenses, leading to a lack of clarity and understanding regarding trafficking as a distinct crime. This lack of clarity posed challenges in effectively addressing trafficking and educating the public about its nuances and implications, as mentioned by the expert.

Additionally, Spain had legislation specifically targeting violence against women and children, the Organic Law 8/2021 on the Comprehensive Protection of Children and Adolescents against Violence. This law included provisions aimed at protecting victims within these vulnerable groups, while acknowledging the intersectionality between trafficking and gender-based violence. By addressing the unique challenges faced by women and children, these laws contributed to a more comprehensive approach to combating trafficking and supporting victims.

Despite the existence of comprehensive laws, Spain faced challenges in effectively applying them to combat trafficking and support victims. One challenge was the relatively recent introduction of trafficking into the criminal law in 2010. This resulted in cultural and knowledge gaps within LEAs and other relevant stakeholders, hindering efforts to identify and address trafficking effectively.

Moreover, there was a need for improved coordination among LEAs, ministries, and NGOs involved in anti-trafficking efforts. Additionally, raising public awareness about trafficking and victims' rights remained a significant challenge, further complicating efforts to combat trafficking effectively.

4.6.2.2 Support System for Victims

Victims of trafficking, particularly women and children were provided with various forms of support and assistance under Spain's legal framework, the expert shared. These provisions included access to shelters, legal representation, medical care, and psychosocial support. Additionally, victims were entitled to temporary residence permits and other forms of protection to ensure their safety and well-being.

However, challenges remained in fully implementing these provisions. Victims often faced barriers in accessing support services due to language barriers, fear of reprisals from traffickers, or lack of awareness about available resources. Moreover, there was a need for greater coordination among relevant agencies and stakeholders to ensure a more holistic and victim-centered approach to supporting trafficking victims.

4.6.3 Investigation and Prosecution of Cases of CEHT

Interestingly, the expert shared that the evidence as per the Spanish legal system was the testimony from the victims. While the prosecutor could start investigation based on other evidence, they would not be able to get a final decision until they had testimony from the victims regarding the traffickers. The expert was not aware of any human trafficking case where digital evidence was used. Further, due to the fewer number of reported cases, the Spanish police were not trained in human trafficking, let alone CEHT, the expert asserted.

4.6.4 Cyber Technology as an Enabler: Challenges and Responses

On the role of technology in facilitating the crime of CEHT, the expert discussed that technology was being used to lure people though digital spaces. But this posed a challenge to ascertain the location of the perpetrators. The LEAs could not be sure if it was in their jurisdiction or not. Anonymity provided by cyber technology made it difficult to identify the trafficker and link them to a case. The platforms commonly used in Spain were WhatsApp, Instagram, TikTok (common among children and youth), gaming apps such as Minecraft, etc. However, the expert reiterated that these were *possible* platforms for abuse but there were no reported cases so far.

While there was recognition of the role of technology companies in facilitating human trafficking, in the absence of specific laws targeting CEHT, efforts to hold enterprises accountable for trafficking-related activities were limited and primarily focused on isolated cases rather than systemic issues involving technology enablers.

Greater awareness and collaboration among stakeholders were identified to address the intersection of technology and trafficking effectively. This included efforts to raise awareness among technology companies about their responsibilities in preventing and addressing trafficking, as well as collaboration with law enforcement and other stakeholders to identify and disrupt trafficking networks operating online.

Contributor

Ms. Maria Jose Castano, Jurist and Lead Researcher for Data Culture in Human Trafficking Project

The "Data Culture in Human Trafficking" project in Spain is an initiative that emphasizes the importance of data as a tool to better understand the reality of human trafficking and exploitation. It operates on the hypothesis that preventing and protecting victims of trafficking requires knowledge of the scope and magnitude of the problem. The project has undertaken numerous actions to highlight the significance of data in making informed decisions in the fight against human trafficking.

4.7 The Philippines

The landscape of CEHT in the Philippines was gleaned from discussions held with the International Justice Mission. The experts represented the Regional Forced Labor Program, and the Centre to End the Online Sexual Exploitation of Children, having on ground experience in handling cases of CEHT in the Philippines.

4.7.1 Trends and Patterns of CEHT: Role and Usage of Cyber Technologies

4.7.1.1 Purpose of Exploitation, Modus Operandi, and Cyber Technologies being used

Noting the concerning trend of inflation in the Philippines, resulting in a decline in the financial status of the population in recent years, experts highlighted that the financial hardships experienced by individuals had created conditions conducive to exploitation, as perpetrators exploited the desperation and economic struggles of vulnerable populations.

The experts highlighted several reasons for human trafficking prevalent in the Philippines, and reflecting the diverse forms of exploitation faced by individuals in the region. The major purposes identified were **forced labor trafficking, sex trafficking, and cyber-scamming/forced criminality**, which continued to pose significant challenges. Local vulnerable populations were being trafficked to Cambodia and Myanmar for carrying out forced cyber-scamming. The Philippines is emerging as a destination country, whereby foreign nationals from Myanmar, Taiwan, Mainland China, etc. are lured with attractive IT offers and are then held hostage for ransom payments or are forcibly made to recruit more victims for carrying out cyber-scams.

While sometimes these were seen to operate as solo enterprises but in actual fact, they were well-organized syndicates running out of compounds with hi-speed internet, etc. One such compound even housed a brothel, showing the scale at which these criminal networks are operating.

Technology had also made young children vulnerable, who were earlier safe inside their homes. Experts spoke on the alarming prevalence of trafficking for OSEC, as well as the production and distribution of CSAM.

Moreover, experts addressed the deceptive recruitment practices employed by traffickers in labor trafficking, affecting both children and adults. Victims were coerced into various industries,

including plantations, sugarcane agriculture, and other such activities. Additionally, the discussion shed light on trafficking for armed conflict, where individuals from certain tribes were recruited to participate in armed conflicts, which highlighted the intersection between trafficking and broader sociopolitical issues. One of the experts raised the issue of trafficking for illegal organ trade, where traffickers promoted the trade as a lucrative avenue without disclosing the risks involved.

Experts mentioned that the primary role of technology was present in the stage of recruitment, relationship building, and exploitation. Along with social media platforms, online gaming apps were also used by traffickers to trap children. Even when children were not direct users of the internet, the adults who had access to children transacted through cyber technologies. Platforms like Facebook, Telegram and WhatsApp were extensively used by the traffickers.

For the purpose of exploitation, anything with video capability could be used and Facebook Messenger, Skype and WhatsApp were identified by the experts as the most widely used applications for the purposes of such exploitation. Technology was being increasingly used for recruitment in forced labor and cyber scamming. Victims who were tech-savvy and knew multiple languages were profiled and targeted with the help of social media and job portals.

4.7.1.2 Victim Profiling

Most of the victims belonged to the lower socioeconomic background, and while the Philippines was seen traditionally as a source country, it was now transitioning into a destination country as well. Victims from other countries like Myanmar, Taiwan, Indonesia, and Mainland China were being targeted by the traffickers as the Philippines has a high internet penetration and social media usage.

4.7.1.3 Revenue Models

Various forms of transactions were used by the traffickers. Apps and services such as MSB, Western Union, PayPal, and bank transfers were used for carrying out such transactions. At the surface level, these transactions appeared to be legitimate. It was discussed that traffickers often operated as solo entrepreneurs, but there were also organized syndicates operating too. Many such places where exploitation took place operated like properly established businesses. Experts equated it with Multi-Level Marketing schemes where people were given targets of recruitment.

4.7.2 Legal Framework to Combat CEHT

4.7.2.1 Legal Framework and Challenges in Application

The Philippines has a comprehensive legal framework aimed at combating human trafficking and related crimes. These laws encompassed various aspects, including traditional trafficking, cyber-enabled offenses, and online exploitation. Below is the overview of the key laws and regulations as mentioned:

1. The Republic Act 9208 (Anti-Trafficking in Persons Act of 2003): This was the flagship law addressing human trafficking in the Philippines. It followed the Act-Means-Purpose framework outlined by the United Nations to define and prohibit trafficking in persons. The law criminalized trafficking for various purposes, such as sexual exploitation, forced labor, slavery, and servitude. It provided measures for prevention, protection, and prosecution of traffickers, as well as assistance and support for victims.
2. The Republic Act 10175 (Cybercrime Prevention Act of 2012): This law covered cyber-enabled offenses, including those facilitated by information technology or computer systems. It enforced penalties for crimes committed using digital platforms, such as online scams, cybersex trafficking, and exploitation of children. The law aimed to address emerging cyber threats and protect individuals from online exploitation and abuse.
3. The Republic Act 11930 (Anti-Online Sexual Abuse and Exploitation Act): Enacted in 2018, this law specifically targeted online sexual abuse and exploitation of children. It provided legal measures to combat the proliferation of CSAM and the online exploitation of minors. The law criminalized the production, distribution, and possession of CSAM, as well as online grooming and solicitation of children for sexual purposes.
4. The Philippine Offshore Gaming Operators (POGOs) Regulation: The Philippine Amusement and Gaming Corporation (PAGCOR), a government-controlled corporation, licence and regulate POGOs. PAGCOR oversees the operation of POGOs and issue licenses to offshore gaming operators. The regulation of POGOs includes licensing requirements, compliance with anti-money laundering regulations, and measures to address potential risks, such as criminal activities and exploitation.
5. Other Cyber-crime and Gaming Regulations: The experts mentioned the challenges of regulating online platforms, including gaming and dating sites, which could be used for illicit activities such as scamming and exploitation. While specific laws address cyber-enabled offenses and online exploitation, enforcement may be complex due to jurisdictional issues and the transnational nature of online crimes.

Strengths in Law

The strengths in the legal framework of the Philippines, as discussed by the experts, highlighted several key aspects that contribute to the effectiveness of anti-trafficking efforts and victim support:

- **High-Level Political Will:** A significant strength was the consistent support from successive administrations towards combating human trafficking. This sustained support provided momentum for enforcement efforts and policy improvements, ensuring a cohesive approach to combating trafficking across different administrations.
- **Trauma-Informed Care:** A further strength lay in the focus on trauma-informed care for trafficking survivors. This approach recognized the complex needs of survivors and aims to provide support that is sensitive, empathetic, and tailored to their individual experiences.
- **Victim Identification and Support:** The legal framework in the Philippines allowed for victim self-identification without requiring extensive legal processes. This provision

enabled victims to access support services promptly, without unnecessary bureaucratic hurdles. Additionally, the inclusion of foreign nationals in victim support provisions stressed on the commitment to providing comprehensive care to all trafficking survivors, regardless of nationality.

- **Inter-Agency Collaboration and Resource Linkages:** The ICAT played a central role in coordinating efforts and ensuring seamless service delivery to survivors. Victims were provided with links to additional resources, including psychosocial services, coordination assistance, and repatriation funding, facilitating their access to comprehensive support.

Challenges in the Application of Law

- **Bodies and Budget Constraints:** LEAs often faced significant limitations in terms of personnel and financial resources. Without an adequate number of trained personnel and sufficient funding, they struggled to conduct thorough investigations, coordinate rescue operations, and prosecute traffickers. Additionally, bureaucratic hurdles and restrictions on budget allocation further impeded their efforts.
- **Training and Specialization:** Due to limited training opportunities and a lack of emphasis on specialization for such crimes, there is often a scarcity of skilled professionals that could significantly impact the quality of investigations and legal proceedings, potentially leading to inadequate outcomes in trafficking cases.
- **Coordination and Cooperation:** Different agencies operated in silos, lacking seamless communication and coordination mechanisms. This lack of cohesion resulted in inefficient resource utilization, duplication of efforts, and delays in victim assistance. Additionally, cooperation between local and international entities presented challenges due to jurisdictional complexities and differing legal frameworks.
- **Resource Allocation Challenges**: While budgetary constraints are a significant concern, even when funds are available, there may be restrictions on their allocation. LEAs may encounter difficulties in accessing allocated budgets for specific operations, particularly those involving victim rescue or international cooperation. Additionally, competing priorities within government agencies may lead to inadequate prioritization of anti-trafficking efforts, further exacerbating resource allocation challenges.
- **Legal and Procedural Hurdles:** Complex legal processes, lengthy court proceedings, and stringent evidentiary requirements may hinder swift action against traffickers. Moreover, gaps or ambiguities in existing laws and regulations may create loopholes that traffickers exploit. Addressing these legal and procedural hurdles required comprehensive legislative reforms and streamlined judicial processes to ensure timely and effective prosecution of traffickers.
- **Legal Interpretation and Adaptation:** Another challenge lay in interpreting and adapting existing laws to address emerging forms of exploitation facilitated by technology. While laws like the Cybercrime Prevention Act and the Trafficking in Persons Act provide a framework, ensuring that they are effectively applied to cyber-enabled crimes required

continuous interpretation and adaptation. This included clarifying jurisdictional issues and determining appropriate legal remedies for crimes committed online.

4.7.2.2 Support System for Victims

The Philippines' government has ensured various measures to cater to the unique needs and challenges faced by survivors of trafficking.

- **Non-Deportation and Blacklisting:** Victims of trafficking, including foreign nationals, are not subject to deportation or blacklisting under the Philippines' law. Victims are not penalized for their exploitation but instead are ensured protection and support by this provision.
- **Aftercare and Shelter Services:** Victims of trafficking are provided with shelter and support services through the efforts of the ICAT. This includes immediate placement in shelters where they can access essential services and resources. Shelter facilities are managed by relevant government agencies and NGOs specializing in victim support. International guidelines on safe spaces for refugees are being used to ensure that transitory spaces are made safe for victims.
- **Trauma-Informed Care:** This approach recognizes the psychological and emotional impact of trafficking and aims to provide tailored assistance to address survivors' needs. Trauma-informed care includes access to mental health professionals, counselling services, and other forms of psychosocial support.
- **Resource Linkages:** These resources may include access to legal aid, medical care, educational opportunities, vocational training, and employment placement services. Coordination efforts between government agencies, NGOs, and other stakeholders ensure that victims have access to a comprehensive range of services to address their individual needs and circumstances. Victims may also receive assistance with repatriation, including transportation arrangements and financial support to facilitate their return to their country of origin, if desired.
- **Legal Framework and Standards of Care:** The legal framework for protecting victims of human trafficking places the best interest of the child as the paramount consideration in all legal proceedings affecting them. During legal processes, measures are implemented to ensure that children are not further harmed, as required by this standard of care.
- **Defining Victory in Prosecution:** In prosecuting cases related to human trafficking, there were two primary goals that defined success. The first was obtaining a conviction to restrain the offender and protect the child from further harm. The second was to ensure that the child was psychologically or emotionally not harmed throughout the legal process. Achieving these objectives involves implementing child protective measures within the courtroom and legal proceedings.

Collaborative efforts between different stakeholders are the keys to providing a comprehensive support network for victims, opined the experts.

4.7.3 Challenges in Investigation and Prosecution of Cases of CEHT

4.7.3.1 Preparedness of Criminal Justice System to deal with CEHT

In the Philippines, experts shared that there is a Judicial Academy to carry out trainings and roughly 60 percent of judges have basic understanding to deal with such cases. Operations are conducted by Anti-Human Trafficking officers along with the assistance of cyber experts.

However, one of the key challenges in the application of laws related to CEHT and online exploitation was the need for capacity building and ensuring that officers have a deep understanding of the complexities of cyber-related evidence and the unique challenges faced by victims.

4.7.3.2 Collection and storage of digital evidence and status of digital forensics

With regards to the procedure on seizure of evidence from the crime scene, experts shared that one has to apply for a warrant to seize data and enter the premises. The cyber experts would assist the team in conducting the seizure and capture of data to conduct online forensics onsite on the computer and mobile devices. In the absence of direct evidence, if the chain of custody is proven, the court relies on digital evidence. Forensic labs were present to authenticate such digital evidence, and the person who conducts the test would depose evidence in court by authenticating the material.

4.7.3.3 Victim dependence for prosecution

An expert shared that in the Philippines, the court considered the victims of CSAM/Sex Trafficking as special cases. The victim's statement, in video form or affidavit form, would be considered along with other evidence to decide these cases qualified for granting certain privileges. In some cases, if the defence lawyer insisted on cross-examination of the victim, the court would allow the person who interviewed the victim and video-record her statement to face the cross-examination. Special provisions exist for child witnesses, allowing video testimony with the condition that the specialists who conducted the interview are subject to cross-examination. This maintains fairness while prioritizing the protection of vulnerable witnesses.

Prosecutors may choose to focus on evidence other than direct testimony, such as transaction records to establish a case, and minimize the necessity for survivor testimony. This approach meant that a case could be proven without relying solely on live witness testimony. Judges recognized that in many cases, crucial evidence can be presented without the need for direct victim testimony. Analogies to murder cases where victims could not testify directly highlighted this understanding.

4.7.4 Cyber Technology as an Enabler: Challenges and Responses

4.7.4.1 Various technologies present in the country being exploited for human trafficking

Experts shared that the Philippines had a high internet penetration with 70 percent of the population having access to the internet. There were 80 million social media accounts of Filipinos out of the total population of 110 million. Interestingly, the Philippines had a legal regulatory

framework known as, 'Philippines Offshore Gaming Operators (POGO)', which regulated Filipino businessmen who collaborated with foreign technology companies to provide their gaming services in the country. However, there is no fool-proof method of stopping services of online gaming service providers whose POGO license had been revoked.

Some technologies listed by the expert included:

- Facebook, Instagram, Telegram were used for recruitment for forced criminalization and to search young children by the buyers.
- Online gaming and dating sites were being used to recruit men and women, especially by the victims who are forced into cyber-scamming.
- Commonly available/used messaging apps having video transmission (WhatsApp, Facebook Messenger, Telegram, Skype, etc.) capability were used to connect young children to buyers of online (sexual) streaming services. Typically, access to children was provided by an adult who has trusted access to the children. The exploitative acts were directed by the buyer of livestream service and facilitated by the adult guardian in explaining/translating it to the victim children.
- Gaming platforms were used to directly connect with the children. Roblox, Minecraft, etc. were popular online games in the Philippines.
- Facebook, WhatsApp, Telegram etc. were also used to recruit job seekers through deception, offering generic IT jobs such as Customer Service Representative, Data Encoder, etc. Such people are forced into committing cyber-crimes/cyber-scamming.
- Crypto currencies were used for accepting ransom payments by fraudsters to release the victims entrapped for cyber-scamming. The inflow of funds through crypto currency was estimated to be several million USD.
- Legitimate fund transfer services of banks, Western Union, etc. were used to receive payments by the adult facilitator.

4.7.4.2 Challenges faced in securing cooperation from Technology Firms

The business model of Technology platforms is to promote more interaction among users. More users and more data mean greater revenue to them. Compliance with regulations puts them at risk of losing certain users and hence revenue, thereby making them reluctant to abide by regulations.

In the context of filtering out CSAM, the Philippines' legal machinery is working with technology companies to maintain the preservation of content and acquire a court order to release the content. They respond immediately to notices if the request is in the proper format. The Technology companies provide a platform to post requests by LEAs, for example - Meta has a dedicated portal to post queries.

4.7.4.3 Accountability of Technology Enablers

While there were provisions within the Philippines' law to hold technology enablers accountable, the specific mechanisms for enforcement and regulation required clarification and implementation. The present provisions are given below:

- **Legal Framework and Accountability**: The legal framework in the Philippines provided avenues to regulate and hold technology enablers accountable for facilitating cyber-enabled crimes, including human trafficking. Laws such as Republic Act 10175, covered cyber-crime, outlined provisions for addressing offenses facilitated by information technology or computer systems. Under the legal framework, technology enablers, such as ISPs and online platforms, had responsibilities in combating human trafficking. This includes implementing measures to prevent the spread of exploitative materials and ensure the safety of users, particularly children, on their platforms.
- **Regulatory Oversight**: Regulatory agencies played a crucial role in overseeing the compliance of technology enablers with legal requirements and standards. However, there may be challenges in effectively enforcing regulations, particularly in cases where technology companies operate from outside the Philippines or utilize encrypted platforms.
- **Compliance and Liability**: Technology enablers are expected to comply with regulations aimed at preventing and detecting illicit activities, such as child sexual exploitation and trafficking. Failure to fulfil these obligations could result in legal liability, including penalties and sanctions.
- **Platform Accountabilit**y: Under the Philippines' law, the platforms could be held accountable if they were complicit or negligent in allowing their services to be used for human trafficking or exploitation. Provisions within relevant laws empowered law enforcement to take action against such platforms. Platforms played a responsible role in preventing and addressing online exploitation and providing recourse for victims affected by platform-facilitated crimes. These provisions ensured that such actions were taken.

4.7.4.4 Suggestions for holding Technology Enablers Accountable:

While the Philippines' law provided a framework for holding technology enablers accountable for facilitating CEHT, the experts stated the need for robust enforcement mechanisms and clear guidelines to ensure compliance and address regulatory challenges. These are listed below:

- **Implementing Rules and Guidelines**: The development of implementing rules and guidelines was essential to clarify the responsibilities and expectations of technology enablers in preventing and addressing cyber-enabled crimes. These rules should outline specific compliance requirements and mechanisms for monitoring and reporting illicit activities.
- **Regulatory Challenges and Recommendations**: Despite the existence of legal provisions, challenges remained in effectively regulating technology enablers and holding them accountable. There is a need for regulatory bodies to address gaps in enforcement and

ensure that technology companies fulfil their obligations in combating human trafficking and related offenses.

- **Collaboration and Coordination**: Collaboration between regulatory agencies, law enforcement, and other stakeholders was crucial in addressing the complex challenges posed by cyber-enabled crimes. Effective coordination can facilitate information sharing, enforcement efforts, and the development of targeted strategies to combat trafficking in the digital space.

4.7.5 Best Practices and Technological Solutions to Combat CEHT

Experts mentioned the following Technology solutions to address the problem:

Technology companies had been directed to filter contents related to CSAM.

- There were certain watch groups which kept searching for CSAM and other inappropriate contents on the internet and maintain a record of their URLs. The companies subscribe to these watch groups' bulletin to block the URLs reported by them.
- Further, they preserve the evidence based on letters from LEA. Certain technology companies have provided a portal for the LEAs to post requests/ contact their nodal officers regarding evidence preservation. However, the evidence is produced only when a court order is given, which may take more time.
- LEA uses a pen drive-based tool for onsite forensics. The pen drive contained hashes of known CSAM materials. It was used to detect the presence of these CSAM materials on the suspect's computer.
- LEA uses a suite of tools for gathering open-source intelligence and social media intelligence with a focus to detect online exploitation of children.
- Certain agencies and NGOs have set up hotlines to facilitate reporting. Certain local government bodies have also set up platforms to receive complaints.

Experts also shared Technology solutions to improve safeguarding within the existing systems:

- Certain large and reputed technology companies operating online gaming had disabled direct chatting to players on their platform based on the age of player.
- Kumu, a social networking app popular in the Philippines, which also supports live video streaming/sharing has stopped its operation/ services after the makers realised that their platform was prone to be misused. Makers were trying to secure their app against potential misuse and have suspended operations until the security gaps are plugged.
- A solution to prevent the distribution of known CSAM materials by blocking its transmission to devices is being worked upon.
- SafetoNet.com is an initiative by the IJM, IWF, and others, which is developing a tool that leverages advanced AI to block harmful and illegal visual content in real time while

preserving user's privacy. The Philippines intends to use the same for protecting the children.

- Agencies have reached out to technology companies such as Meta to develop algorithms to detect malicious advertisements on their platform and block them.
- Burden to proactively detect and report/prevent the harmful contents are being placed on the companies.
- Interpol is trying to negotiate with WhatsApp to provide backdoor access to LEAs to monitor chats and files on the platform.

Contributors

Mr. Andrey Sawchenko, Regional Vice President, Forced Labor Programs, Asia Pacific at International Justice Mission

Mr. Gideon Cauton, Law Enforcement Development Specialist, Regional Forced Labor Program, International Justice Mission

Mr. Benjamin Lawrence Patrick Aritao, Director, Prosecution and Aftercare, Center to End Online Sexual Exploitation of Children, International Justice Mission

Profile of Organization

International Justice Mission

The International Justice Mission (IJM), is a U.S.-based NGO dedicated to human rights, law, and law enforcement. Founded in 1997, IJM works to combat sex trafficking, child sexual exploitation, cybersex trafficking, forced labor slavery, property grabbing, and police abuse of power, and addresses citizenship rights of minorities. The bulk of IJM's work focuses on sex trafficking.

4.8 Recommendations by Global Experts for Regional and Global Cooperation to Combat CEHT

Global experts from the six countries highlighted the recognition of the challenges being faced regionally and globally with the increasing usage of cyber technologies in ways and means, which were unprecedented and unrecognizable. In light of these challenges and difficulties encountered in effectively preventing and combating the transnational nature of CEHT, the experts shared their recommendations to improve regional and global cooperation to combat CEHT, summarized herewith. These recommendations draw from their experiences of fighting CEHT in their respective countries and are also learnings from these efforts.

1. Securing global consensus for an **International Convention on Countering Transnational CEHT**, and making it mandatory on member states to coordinate international efforts to

combat this pervasive criminal enterprise. This should entail international cooperation, joint investigations, mutual legal assistance, extraditions, collection of digital evidence, and the regulation of proceeds of the crimes, in cases of cyber-enabled trafficking in persons.

2. Through collaborative efforts put in place **Regional Cooperation Mechanisms** to enhance coordination and facilitate joint investigations into transnational criminal networks, entailing multi- stakeholder collaboration with a victim centric approach.

3. Create an **International Regulatory and Enforcement Framework for Securing Cooperation from Technology Platforms** and to hold them accountable for their role in the use of cyber technologies that recruit, control and exploit victims.

4. Establish a **Global Observatory to track CEHT globally,** improve data collection, and research on the scope and nature of the misuse of cyber technologies, and find global solutions, with India playing a lead role.

4.9 The Lessons Learnt from Global Experiences

Discussions with the global experts provided insights on the prevailing global trends and manifestations of CEHT, but also drew attention to the challenges faced and lessons learnt that could provide useful knowledge and an evidence base for developing any plan of action. Globally, while there are similarities in both the nature of the problem and solutions adopted, it is also interesting to note the variations depending on the geopolitical conditions in the country and region.

1. Human Trafficking and Cyber Technology

Traditional forms of human trafficking continue both as a domestic and transnational problem. Cyber technology has only accelerated the same and brought in additionally some newer forms of exploitation that are unique to its nature such as human trafficking for cyber scamming, and generation and dissemination of CSAM. CEHT has minimized direct contact of the traffickers with the victim, and also opened virtual exploitation as a new form of intimidation and control of victims.

2. Misuse of Cyber Technologies

All virtual mediums such as social media, instant messaging apps, job sites, dating sites, and live streaming apps, have been exploited by traffickers by taking advantage of loopholes in the technology. Traffickers are using technology at every stage of the crime, from identification, recruitment, control of victims, to the laundering of the proceeds of the exploitation. Certain technologies offered by technology firms provide a favourable ecosystem for the traffickers to operate.

3. Concerning rise in CSAM and the Issue of Consent

Increasing presence of children as those involved in generating CSAM with consent has emerged as a global concern. The usage of gaming apps to potentially identify vulnerable children and grooming them for crimes brings out another worrying modus operandi which effectively conceals the traffickers. This calls upon the need to incorporate a gender-and-child-

sensitive perspective into responses being developed to address the nexus between technology and trafficking in person.

4. Challenges posed by AI

   The potential misuse of encrypted AI, particularly in generating CSAM images which are hyper realistic and indistinguishable, poses a major challenge and requires a mechanism to look into the encryption policy of companies, and scan the encrypted data they store.

5. War, Unrest, and Human Trafficking

   In the wake of wars, civil unrest, and crisis situations a global proliferation of transnational trafficking syndicates emerges across countries and regions. These organized criminal networks target victims whose heightened vulnerabilities arise from their socioeconomic and undocumented status, for various purposes of exploitation.

6. Impact of Covid on Human Trafficking

   Information and communications technology has become an indispensable element of our lives, accelerated by Covid-19, leading to its gross misuse by criminal networks. With the global onset of the Covid-19 pandemic, traditional modes of exploitation faced disruptions due to movement restrictions and this period witnessed a shift in traffickers' modus operandi. With victims no longer being physically transported across borders, they are subjected to exploitation directly in their countries of origin through sophisticated online means, presenting challenges in detection.

7. Legalization of Commercial Sexual Activities

   Legalization of commercial sexual activities in various parts of Europe has fostered concealment of exploitation making it more complex to detect the crime and identify the victim.

8. Securing Cooperation and Accountability from Technology Platforms

   Most Technology platforms lack the intent to address human trafficking issues. In the absence of a well-defined legal framework outlining the responsibilities of technology enablers the timeliness and efficacy of their cooperation faces challenges in enforcement.

9. Lack of Specialized Investigation and Prosecution Skills

   There is a need to strengthen the expertise and the capacity of law enforcement and criminal justice agencies in conducting efficient investigations and operations in cyberspace.

10. Partnership Model with NGOs in Fighting CEHT

    Collaborative efforts in combating human trafficking placing prevention at the forefront is going to play a critical role in all counter trafficking efforts and the role of NGOs is pivotal in both prevention and protection.

11. Victim Protection and Services

    There is a need for uniformity in the victim protection measures across countries through effective partnerships and coalitions between various sectors and stakeholders, with NGOs

playing an important role, to enhance innovation and cooperation in providing trauma informed holistic services for victims.

12. Leveraging Technology to Combat CEHT

Best practices and technology-based solutions in the detection, investigation, and prosecution of CEHT cases, the protection of victims and witnesses, and the removal of harmful or exploitative materials online, offers the possibility of adoption and replication in the global and national context.

4.10 Inputs for the National Plan of Action to Combat CEHT

The recommendations made by the global experts and the lessons learnt from the global experience are useful insights which will contribute to the drafting of the NPoA to combat CEHT. Some major components drawn from these expert inputs that will be adopted are listed below:

1. A comprehensive National Legal Framework which defines CEHT and encompasses all the aspects of this crime, provides for inter-state and international cooperation, provides holistic trauma informed victim services, and makes technology firms liable for their role as an enabler.
2. Amendments in the existing law to ensure that usage of technology is to be viewed as an aggravated form of crime in such circumstances.
3. Develop technology-based solutions to both prevent and fight the crime.
4. Establish specialized Cyber Competence Centers for all jurisdictions who will assist the local law enforcement mechanism to deal with crimes that are cyber-enabled.
5. Need for specialized forces with the requisite skills, resources, and capacities to fight CEHT.
6. Need for specialized training and refresher courses for law enforcement and criminal justice practitioners to effectively deal with the new and emerging dimensions of CEHT.
7. Develop regional and international cooperation framework at the SAARC, ASEAN and global level.
8. Drawing up of a minimum protocol for technology firms to operate in the country that should include risk assessment on the dangers posed by CEHT, appointment of an accessible nodal person, encryption policy and prioritization of user safety.
9. Mandate websites hosting adult sexual services to introduce emergency response mechanism for customers/buyers to report on in suspected cases of human trafficking including that of minors.
10. Forge a formal partnership with civil society for victim protection services and crime detection.
11. Develop targeted awareness-raising campaigns in collaboration with all stakeholders including technological firms, particularly focused on the new and emerging dimensions of CEHT i.e. online sexual exploitation of children, cyber-scamming, etc.

12. Ensure the appointment of a nodal person/department within the Central Government. This person will be responsible to support the fight against human trafficking, with specific focus on CEHT.
13. Establish Inter Ministerial Committee Against Trafficking (IMCAT) to facilitate inter-agency collaboration and partnership in counter trafficking efforts.

Chapter

05

Indian Context - Insights From Data Collection

Chapter 5

Indian Context - Insights From Data Collection

5.1 Introduction

While the global context was necessary to position the problem of CEHT as a borderless crime this national research was carried out to understand the trends and patterns of CEHT in different regions of India. The study aimed to ascertain the usage of technology by the traffickers in the 'act, means, and purpose' of human trafficking and also to examine the role of technological platforms/companies in enabling CEHT. The scope of study included to identify gaps in Indian legal framework to tackle CEHT and assess the preparedness of law enforcement mechanism to deal with CEHT within the existing legal framework. In order to develop the national perspective of the problem of CEHT, the study planned to collect data from a fairly large sample set of states which can adequately represent the country. Even though, cyber-crimes/CEHT is borderless in nature, in order to understand regional differences, Indian states were clubbed into the four broad regions - north, south, east, and west. To ensure representation of each region, three states from each region were selected as samples, with the exception of eastern India, where six states were selected noting that the North-Eastern states of India often exhibit distinct patterns from rest of India.

The 15 sample states from where the study collected data are, Punjab, Rajasthan and Madhya Pradesh from the north; Kerala, Telangana and Andhra Pradesh from the south; Bihar, Jharkhand, Odisha, West Bengal, Assam, and Meghalaya from the east; and Gujarat, Maharashtra and Goa from the western region of India.

Interaction with police officers handling human trafficking and cyber-crimes of each state to discuss/record the CEHT cases they have handled/ observed was considered as the appropriate and feasible means to understand the trends and patterns of CEHT in India. Further, states were requested to nominate a mix of officers from AHTUs, cyber investigation and CID for the discussion, so that a diversified and balanced view on the subject could be obtained. Data was collected by means of FGDs with the participant police officers followed by administration of a detailed questionnaire. While the FGDs were largely qualitative in nature, the questionnaire included both quantitative and qualitative components.

This chapter presents the compilation of data collected both from the questionnaire and the FGDs under the following headings:

1. Nature of cases - human trafficking
2. Application of the law
3. Technology usage in CEHT

4. Revenue and transactions
5. Difficulties in gathering digital evidence
6. Difficulty with technology firms/intermediaries
7. Challenges in prosecution
8. Support for law enforcement mechanisms
9. Victim protection and challenges faced
10. Recommendations

5.2 Nature of Cases – Human Trafficking

The study found that participants were not familiar with the term 'CEHT'. One of the preliminary tasks was to orient the participants to the objectives of the study conducted through a simulation session, where the definition of human trafficking with all its components (act, means, and purpose of exploitation) were discussed in the context of cyber technology being an enabler with anecdotal local and international examples. The simulation session helped the participants to relate to CEHT and enable them to share information about cases. Interestingly, after the concept was demystified and the participants were able to correlate their field level experience, they were able to elaborate on how various cyber technologies like social media, instant messaging apps, payment apps, and other encrypted services were used in suspected cases of human trafficking.

5.2.1 Dealing with CEHT Cases

Of the participants present, 14 percent of participants had actually registered cases as CEHT, as was revealed by their response to the question, if "they had encountered a CEHT case" (see figure 5.2.1).

The data reflects that even though the elements of cyber technology were present in the cases of human trafficking, it was never treated as a case of CEHT. This could also be because, currently the legal framework does not explicitly acknowledge CEHT as a form of crime, nor does it distinguish it from conventional human trafficking.

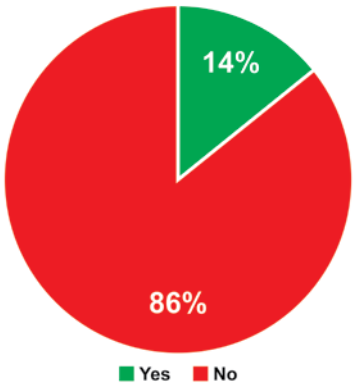


Fig 5.2.1: Officers having handled CEHT cases

5.2.2 Major Purpose of Trafficking

The participants were asked as per their knowledge, what was the major form of human trafficking that is enabled by cyber technology. A majority of participants cited **Commercial Sexual Exploitation** (72 percent) as one of the main purposes of human trafficking that could be enabled by cyber technology. The participants also cited **labor exploitation** (56 percent), **production of CSAM** (50 percent), **organ trafficking** (37 percent), **forced marriage** (36 percent), **coercion to commit cyber-crimes** (36 percent), **surrogacy** (19 percent) and **adoption** (17 percent) as other purposes of human trafficking that could be cyber-enabled.

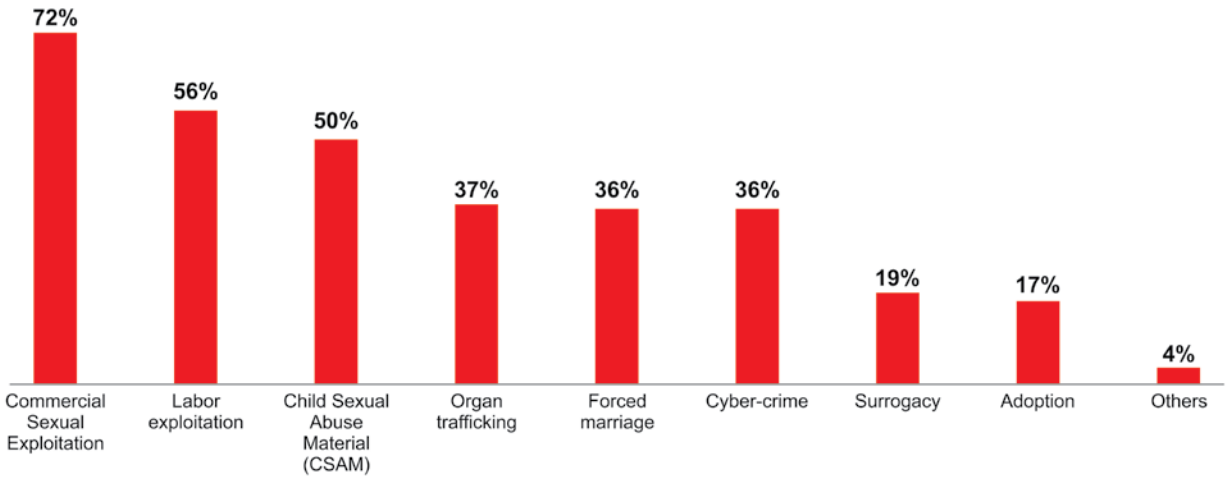


Fig 5.2.2: Major purposes of CEHT/ human trafficking

5.2.3 Sources of Information

The study sought to understand the various sources from which police could get information about CEHT cases.

A significant majority of respondents i.e. 71 percent identified **complaints by victims or their families** as the primary source of information. Nearly half of the respondents (45.6 percent) also mentioned **online portals** or **cyber tip-lines** as sources of information. Another 24 percent of respondents said that **tip-offs** from anonymous sources or concerned individuals were their information sources. According to 18 percent of the respondents ***Suo moto* action** by the police, based on suspicion or patterns identified during investigations enabled them to detect human trafficking cases.

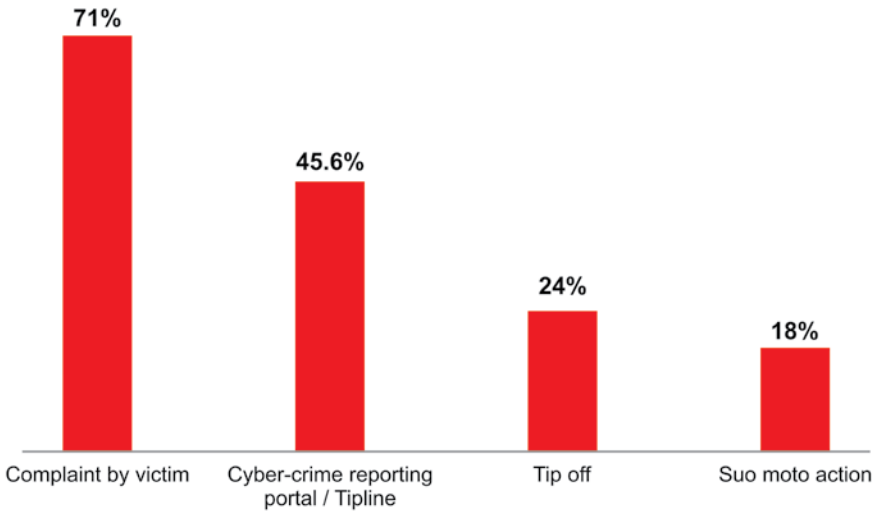


Fig 5.2.3: Source of information of a CEHT/ human trafficking case

During the FGDs, participants discussed that complaints are often not filed due to lack of awareness, stigma, and lengthy legal processes.

5.2.4 Modus Operandi and Means in CEHT Cases

An effort was made to understand what, in the opinion of the respondents, would be the modus operandi that would be used in CEHT cases.

A majority (75 percent) felt false promises of employment would be the most common means that traffickers will employ in cyber space to trap potential victims. Other means such as fake marriage proposals (61 percent), financial allurement (59 percent), threats and intimidation/ blackmailing (47 percent), sextortion (46 percent) deceit/cheating (43 percent), abduction and kidnapping (31 percent) and grooming (26 percent) figured as other tactics that could be applied by traffickers in cyber space.

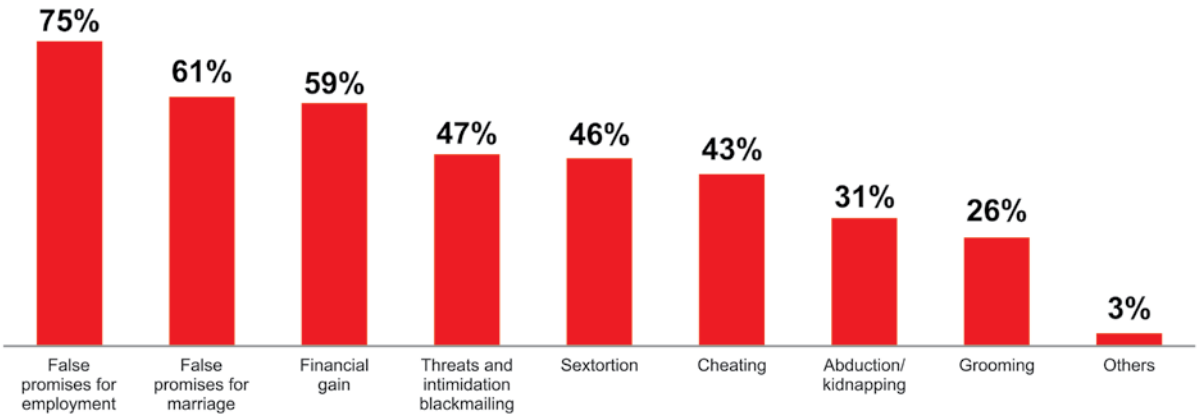


Fig 5.2.4: Modus operandi in carrying out CEHT

This was further corroborated during FGDs where the respondents highlighted how traffickers lure victims through false promises of employment, marriage prospects, or financial stability, sharing several case studies. In their experience, deceit often begins innocuously, with victims falling prey to scams involving part-time jobs, fraudulent loan apps, or matrimonial fraud schemes. Acts of grooming is specifically employed in trapping women with fake promises of marriage and in exploitation of children. Participants elaborated that traffickers prey on vulnerable individuals, particularly women and girls from marginalized communities. Spotting them on social media and using tactics of false promises of love and marriage, they are lured to elope from their homes, thereby moving them outside their ecosystem into a new environment where they do not have any kind of support and safety nets. They are then trapped in a cycle of abuse and coercion, with few avenues of escape. Participants from the Eastern region extensively spoke on how instant messaging apps were used to facilitate labor trafficking. The participants who actually registered the CEHT cases highlighted the emerging pattern where young professionals well versed with cyber technologies are being trafficked internationally with lucrative job offers, to carry out cyber-crimes and various online frauds. They also pointed out that these individuals were not only victims of human trafficking but are also vulnerable to commit crimes due to their involvement in various illegal activities that they are forced to carry out.

In the course of FGDs, participants through various case studies highlighted how victims were spotted on cyber space through various means such as social media, online gaming apps, matrimonial or job sites, and how they were groomed via instant messaging and then exploited physically either for commercial sexual exploitation or for labor exploitation.

In cases where there was production and circulation of CSAM, the virtual medium was adopted both for trapping the potential victim and for exploitation. For instance, the perpetrator used an online gaming app such as 'truth or dare' for connecting with the victim, grooming her to share her nude photos and videos online, and thereafter using this shared material to blackmail and exploit her using Instagram. Participants also shared that internet enabled video calling/conferencing services facilitate virtual exploitation, where victims are coerced and forced to perform inappropriate acts in front of the camera.

A few cases were also mentioned where the victim was physically engaged in the early stage of contact building and cultivating a trust-connect to shoot/ record nude photos/sexual acts with consent. These private contents were subsequently used for virtual exploitation.

Participants also discussed that financial frauds and extortion further aggravate the plight of victims. Malicious loan apps, identity theft, and online scams prey on the desperate and vulnerable, siphoning off their hard-earned money or coercing them into further exploitation. Involvement of parents in certain cases adds another layer of complexity, when, in financial distress, they sell their own children for forced marriages or labor exploitation for small sums of money.

5.2.5 Nature / Medium of Exploitation

The respondents were asked regarding the nature/medium of exploitation in the cases of CEHT. The majority of respondents (75 percent) indicated that exploitation involves a **mix of both physical and virtual aspects**. Nearly 26 percent of respondents observed that exploitation **starts and remains entirely virtual**. On the other hand, 18 percent of respondents mentioned cases where exploitation **began with physical coercion but transitioned largely into the virtual domain.**

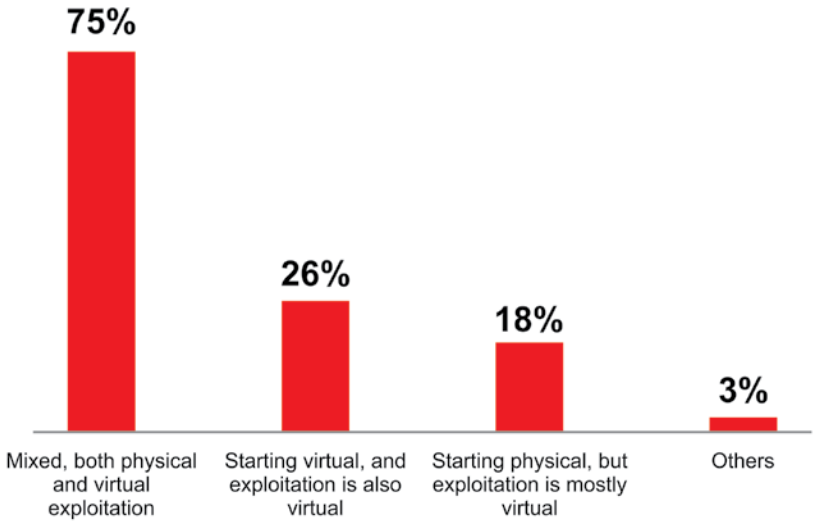


Fig 5.2.5: Nature of exploitation in CEHT

5.2.6 Profile of the Victims

The profile of the human beings trapped in CEHT is an important component to be understood in order to evolve and design specific strategies to address the problem at the grassroots level. The gender, age, and vulnerability factors were the three variables taken to understand the profile of victims.

5.2.7 Gender Profile of the Victims

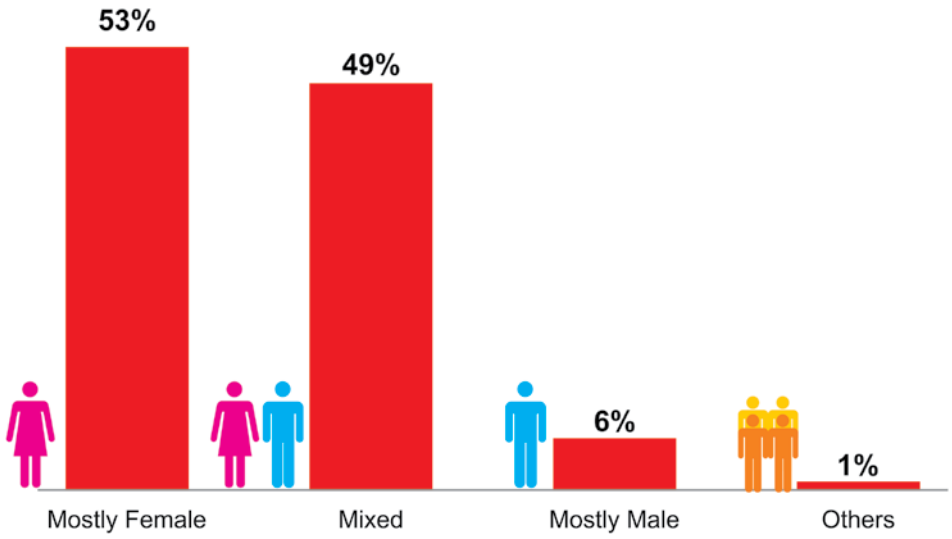


Fig 5.2.7: Gender profile of the victims of CEHT

Based on the cases that the respondents had seen on the ground 53 percent stated that most of the victims of CEHT are females. While 49 percent had observed the victims of CEHT cases as both males and females, only 6 percent of the respondents mentioned that they had mostly observed male victims.

During the FGDs it emerged that prostitution and commercial sexual exploitation continues to form the larger chunk of human trafficking cases that are cyber-enabled, and mostly target women and girls. The visible and significant number of male victims was largely for labor exploitation such as cyber scamming.

5.2.8 Age Profile of the Victims

Regarding the age ranges of victims, 9 percent of respondents indicated the victims are **below 10 years** while 36 percent had observed them to be in the age range of **11-15 years**. A vast majority of respondents (64 percent) stated that the average age of the victim is between **16-18 years**.

5.2.9 Key Vulnerability factors among Victims

The study also tried to ascertain the key vulnerability factors of victims and their families in the

cases that the participants had observed. The vast majority of respondents (76 percent) identified **poverty** as a major vulnerability factor. A significant portion of respondents, i.e. 60 percent, indicated **illiteracy** as a vulnerability factor. Nearly half of the respondents (49 percent) highlighted **emotional vulnerability** as a factor. It also emerged that social factors like caste also play a role, with 43 percent of respondents mentioning **low social and caste status** as a vulnerability factor. 33 percent of respondents **reported violence or abuse in the household** as a vulnerability factor. Additionally, a similar percentage (33 percent) mentioned **separation/divorce** as a potential vulnerability factor.

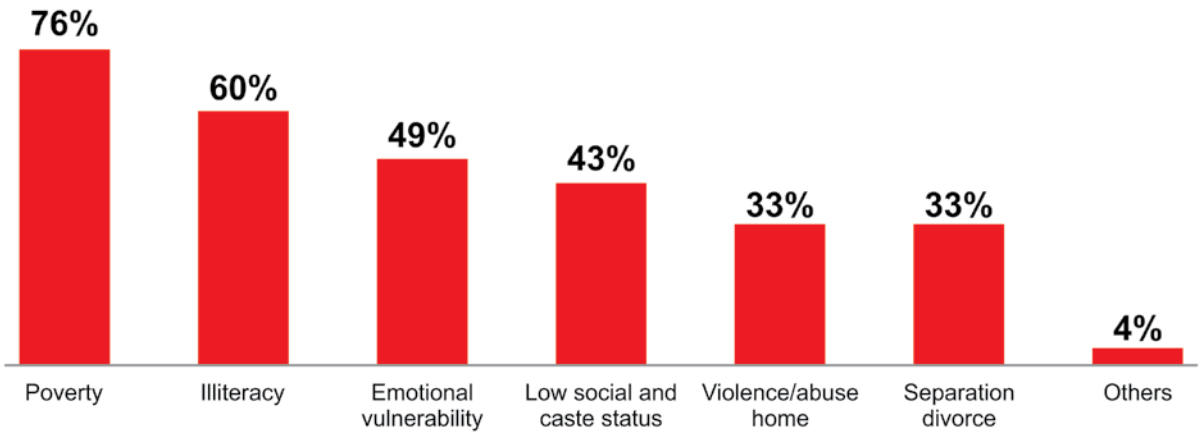


Fig 5.2.9: Vulnerability factor of the victims of CEHT

Corroborating these factors are the facts shared by participants during the course of FGDs where they elaborated case studies of widows or divorced women being the prime targets of predators through matrimonial sites or dating sites. The emotional vacuum expressed on social media such as Facebook or Instagram was cited by many as the primary reason for being spotted by traffickers on the online space. Multiple vulnerability factors such as poverty and illiteracy combined with low social status (attributed to caste and other sociological factors) was seen in many cases where the victims unable to bear their socioeconomic conditions were easily lured online with promises of a better future.

5.2.10 Age Profile of the Traffickers

As all the respondents were police officers who dealt with crime on a day-to-day basis, the study sought to understand the age profile of traffickers who were identified/arrested.

Over half of the respondents (51 percent) indicated traffickers to be between **25 to 30 years** old. Nearly 40 percent of respondents mentioned traffickers to be in the **31- 40 years** age range, and over one third (34 percent) reported traffickers in the age range of **18 to 24 years old.**

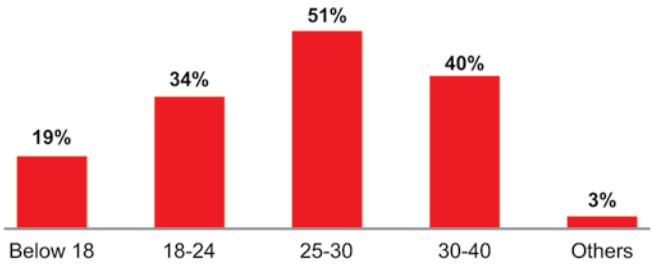


Fig 5.2.10: Average age of Traffickers in CEHT

Nearly one-fifth of respondents (19 percent) reported traffickers were under **18 years of age.**

5.2.11 Location of the Traffickers

Delving deeper into the operational framework of the traffickers the participants were asked about the likely locations of the traffickers. A significant 78 percent of respondents said that traffickers are **within India, but located in states other than in which their targets belonged.** Over one third of respondents (38 percent) reported traffickers to be located **within the same state** where the crime occurred. About 31 percent respondents mentioned that the traffickers were operating from **outside** India.

A few, yet a significant number of respondents (18 percent) were unable to speculate the location of the traffickers.

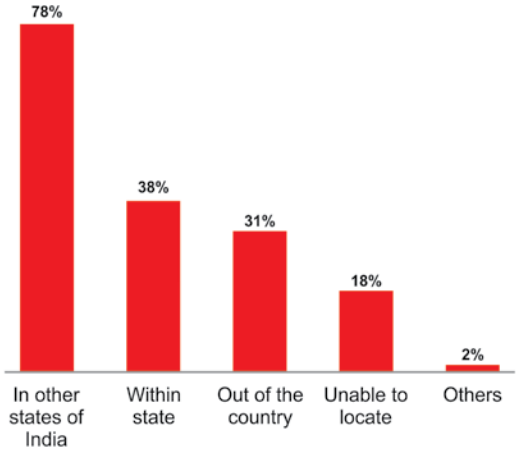


Fig 5.2.11: Location of traffickers

5.2.12 Trends and patterns in CEHT and Human Trafficking

During the FGDs, several case studies shared by the participants brought out specific trends and patterns in India that are common nationally and are reported across all regions. The summary of technology use for different purposes of exploitation as mentioned by the participants of respective states is given below:

a) Sexual Exploitation:

i. Telangana and Maharashtra: WhatsApp was used for communication and payment transactions. Photo editing apps were used to modify or morph victim images to make them look good to post on online advertisements for selling sexual services under the garb of escort services.

ii. Andhra Pradesh: WhatsApp and Telegram were commonly used for communication due to their encrypted reachability.

iii. Punjab: Telegram was used for sharing photos, videos, and porn materials.

iv. Bihar: Facebook and Instagram were used for extortion based on morphed pictures, and Instagram was used for spotting vulnerable victims.

v. Assam: Clubhouse, lottery apps, dating apps, and matrimonial apps were used for spotting victims, whereas messaging apps such as WhatsApp and Telegram were used for recruiting and transportation.

vi. West Bengal: Facebook, Instagram, Locanto, and dating apps were used for spotting and recruiting; IMO and WhatsApp were used for transporting and harbouring victims.

vii. Meghalaya: Instagram, Facebook, Telegram, WhatsApp, and Messenger were used for spotting and recruiting, whereas WhatsApp and Telegram were used for recruiting and transporting.

b) Labor Exploitation:

i. Rajasthan: Facebook, Instagram, WhatsApp, Telegram, and gaming apps like PUBG and Blue Whale were used for spotting victims.

ii. Jharkhand: WhatsApp was primarily used for communication and circulation of information among agents.

iii. Rajasthan and Madhya Pradesh: WhatsApp was used for communication and circulation of information among agents.

iv. Punjab: Malicious loan apps were advertised on Facebook/Instagram. Social media platforms such as WhatsApp, Snapchat, and Share chat, were used for recruiting and communication. Payment and revenue transactions were facilitated through UPI apps like Paytm and GPay.

c) Trafficking of Child Brides:

i. Bihar: Facebook was commonly used to extort money based on morphed pictures and to advertise for recruiting victims, and Instagram was used for spotting vulnerable victims through reels.

d) Cyber Scamming:

i. Assam, Telangana, and Maharashtra: Messaging apps like WhatsApp and Telegram were used for recruiting and communication, and Clubhouse, lottery apps, dating apps, job sites and matrimonial apps were used for spotting victims.

ii. Meghalaya: Instagram, Facebook, Telegram, WhatsApp, and Messenger were used for spotting and recruiting, and WhatsApp and Telegram were used specially for recruiting and transporting.

5.3 Existing Legal Provisions and CEHT

An attempt was made to understand how the existing legal provisions were being used in CEHT cases. The participants who were drawn from cyber-crime wings, AHTUs and CID shared their experience based on the cases they had handled **(The data collection was done from November 2023 to March 2024 when the Indian Penal Code (IPC) was still applied)**.

5.3.1 Application of Law

A majority of participants, while registering a human trafficking case, had applied Sec. 370 (75 percent), Sec. 366A &B (59 percent) of the Indian Penal Code and the relevant sections of the

Immoral Traffic (Prevention) Act,1956 (56 percent) which is a special legislation to combat sex trafficking. In cases where minors/children were victims, 65 percent had applied the Protection of Children from Sexual Offences (POCSO) Act and 30 percent Sec. 372 and Sec.373 of the Indian Penal Code. 50 percent of the participants had applied the Information Technology (IT) Act, 2000. Certain officers from the Telugu states of Andhra Pradesh and Telangana who constitute 7 percent of sample had also applied the Telangana Preventive Detention Act, 1986 in cases of human trafficking.

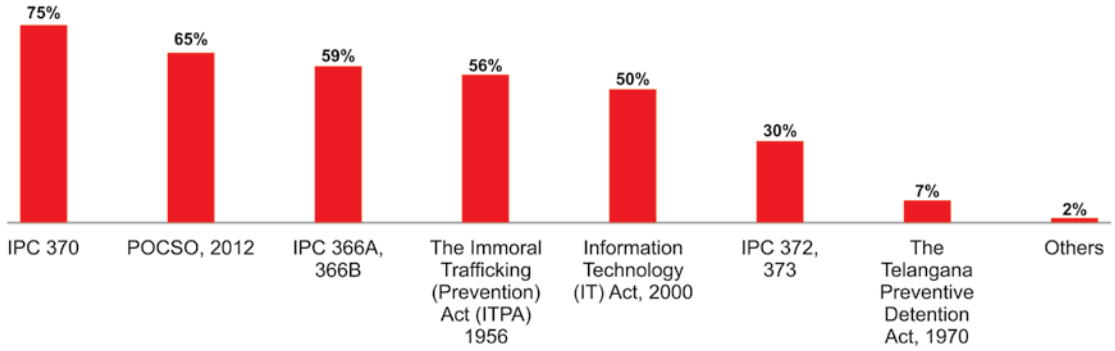


Fig 5.3.1: Acts/ sections used in CEHT/ human trafficking cases

5.3.2 Application of IT Act 2000 in CEHT Cases

On the question on what parameters could be used to decide application of IT Act 2000 in CEHT cases, over half of the respondents (54 percent) stated the IT Act can be used when cyber technologies are used by the traffickers **to communicate with victims.** A significant portion of respondents (38 percent) reported that in the cases where **exploitation itself occurred online**, such as in pornography or through video streaming via online platforms, and 34 percent of respondents stated the IT Act can be used when cyber technologies are used by the traffickers in **facilitating the movement of the victim**. Along with that, 32 percent of respondents mentioned that when there is trace of cyber technologies for making **payment and online transaction**, they could apply the IT Act. Notably, 23 percent of respondents felt a case-to-case assessment is necessary and drawing a list of parameters is not helpful.

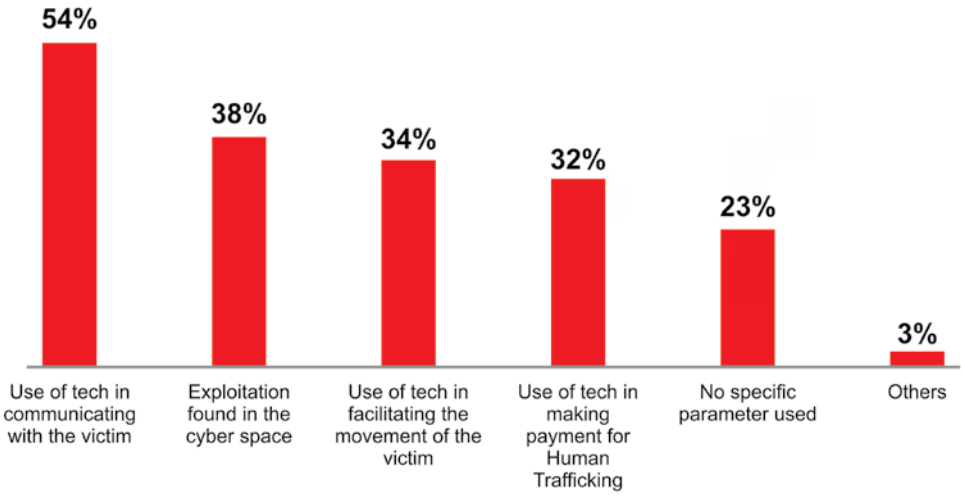


Fig 5.3.2: Application of IT Act 2000 in CEHT case

During the course of FGDs, participants were able to relate to the extensive usage of cyber technologies by human traffickers in the cases they have come across. They were able to describe various modus operandi enabled by cyber technology such as online grooming, recruitment through social media platforms, or using technology to control victim's communication with others. Many of them also pointed out that technology was being used to facilitate movement of victims by booking their tickets online, making hotel reservations, and to track victims' movements through the GPS of their mobile phones. It was also clear that most of these elements are not recognized by the existing IT Act.

5.4 Technologies Usage In CEHT

An attempt was made to understand various technologies used in CEHT cases. Participants shared their experience based on both the cases handled by them and also of those observed on the ground which could be a potential CEHT case but were never registered as under CEHT.

5.4.1 Technology Used to Entrap Victims

Participants were asked which all technologies, according to their experience, was used by the traffickers to spot, communicate and lure victims.

Social media platforms emerged as the primary communication channel, with an overwhelming 84 percent of respondents indicating their use. 59 percent of the respondents pointed at **instant messaging apps** as the primary means of communication and luring of victims. A sizeable group of respondents (36 percent) stated that traditional methods like **SMS** are used. According to 41 percent of respondents, traffickers use **online classified advertisements** to disguise their bait as jobs to lure the victims searching for jobs. 30 percent of respondents observed the use of **photo editing apps** by traffickers to create fake profiles or manipulate images to coerce victims into exploitation. Use of encryption tools like **VPNs and TOR** by some traffickers was indicated by 29 percent of the respondents. 5 percent of the respondents stated there may be other/additional tools and technologies possibly being used for communication by the traffickers.

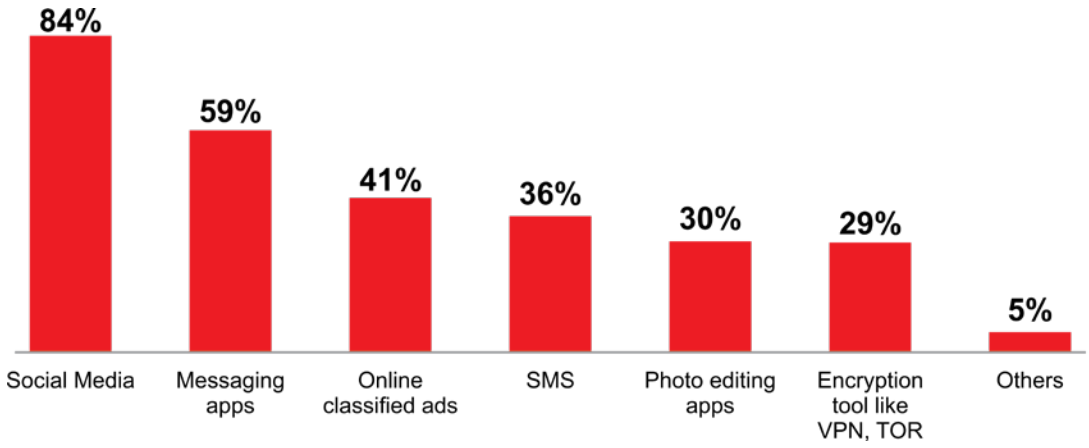


Fig 5.4.1: Technologies used by the recruiter to spot, communicate, and lure victims

Through the FGD, it emerged that communication platforms like WhatsApp, Telegram, and Facebook Messenger, serve as primary channels for recruitment, transportation, and coordination for harbouring of victims. Participants also discussed the usage of social media platforms such as Facebook, Instagram, and TikTok that serve as virtual hunting grounds for traffickers, who use them to spot vulnerable individuals. It was discussed that criminals try to profile the victims to understand them in detail and their vulnerabilities. The information shared by the victims online is subsequently used to gain trust and then coerce them into exploitation. Traffickers identify and lure potential victims through targeted advertisements, fake profiles, and grooming techniques. Matrimonial websites like 'Shaadi.com' and dating apps such as 'Tinder' are also used to target individuals seeking companionship online, offering false promises of love and marriage to win trust, before subjecting them to exploitation.

5.4.2 Loopholes in the existing technologies exploited by Criminals

Exploring the features that exist in various technologies that provide a safe haven for criminals to operate, the participants were requested to share their views based on the cases that they have come across and their understanding of the cyber space.

An overwhelming number of respondents (77 percent) stated that the ease of making **fake profiles** is the major loophole used by all traffickers, combined with the ease of usage of online platforms (49 percent), and a lack of user profile screening (44 percent) enabled traffickers to use the cyberspace with confidence of remaining undetected.

The **anonymity** provided by online platforms (36 percent) and **free availability** of many communication apps (29 percent) ensured both impunity and accessibility for the traffickers to operate.

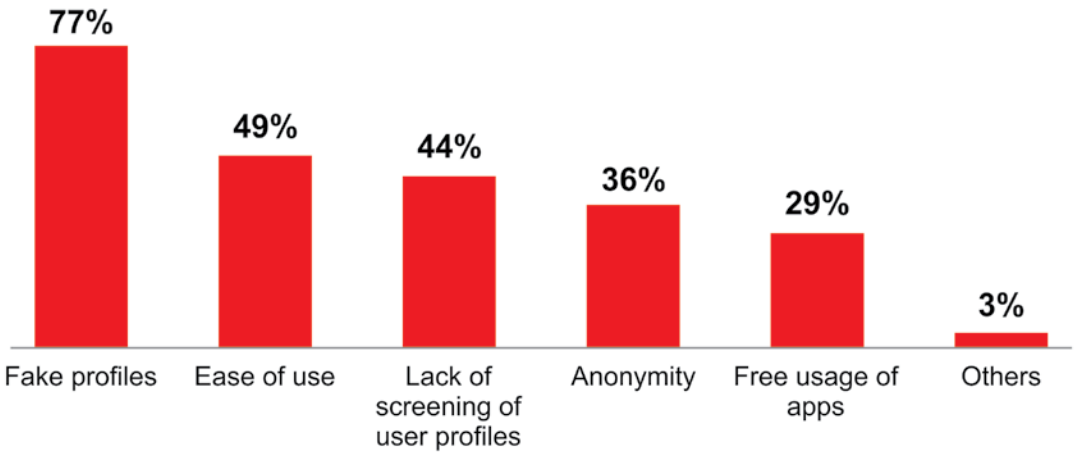


Fig 5.4.2: Loopholes provided in the apps that encourages its usage by criminals

In the FGDs, participants explained in detail how traffickers readily create accounts and utilize these platforms for communication and recruitment without facing significant technical barriers. These factors can make it easier for traffickers to establish contact and exploit potential victims.

5.4.3 Websites used for Labor Exploitation

In an attempt to understand the misuse of certain websites for labor exploitation, the participants were asked if they knew of any such websites from where vulnerable job seeking persons were exploited.

A significant portion of respondents (63 percent) identified **Naukri.com** as a platform potentially targeted for labor exploitation. **LaborNet** emerged as another major platform mentioned by 37 percent of respondents as being potentially misused for exploitation. 27 percent of respondents mentioned **eShram** and 9 percent mentioned the **NSDC** website.

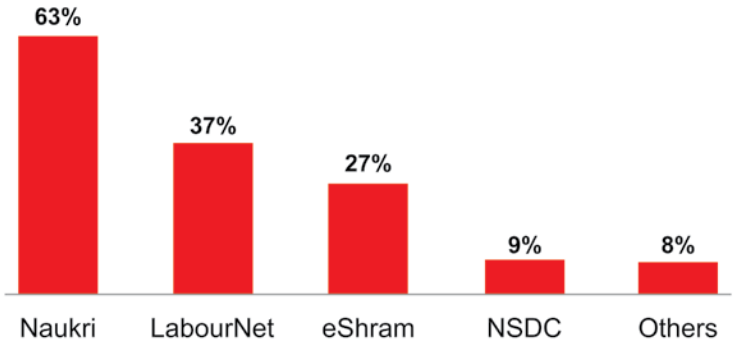


Fig 5.4.3: Websites used for labor exploitation

5.4.4 Usage of Technology to Counter Crime

As adoption of technology by traffickers and criminals emerged in previous sections, the study also sought to find out the level of adoption of technology by the LEAs to detect and counter human trafficking and other crimes.

Over half of the respondents who were mostly cyber-crime inspectors (55 percent) indicated **they use technological tools for detecting and investigating cyber-crimes.**

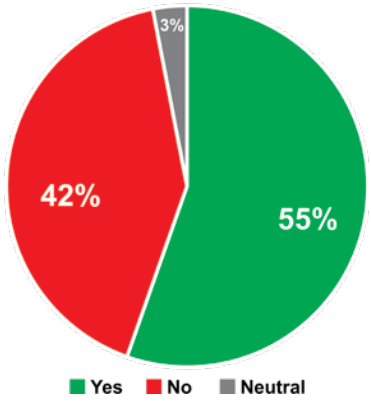


Fig. 5.4.4: Usage of technology to detect/ counter crime

5.4.5 Usage of Software and Services

Participants, mostly cyber inspectors, who had indicated that they had used technological solutions in their investigations were further probed to explicitly state the purpose of its usage.

Around 57 percent mentioned using technology for **investigation purposes**. This includes software for communication tracing, online record searches to identify victims or traffickers, or digital evidence analysis tools to extract information from confiscated devices. Nearly 54 percent of respondents reported using technology for **tracking purposes,** and 49 percent used it for evidence collection. Further 53 percent indicated that software services were used to **detect potential trafficking cases.**

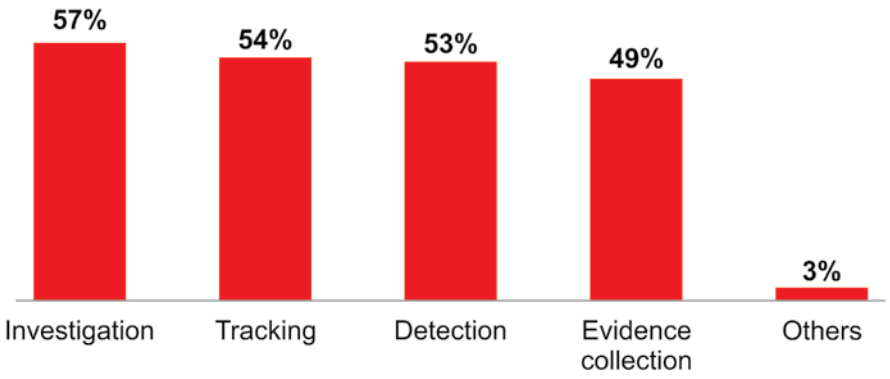


Fig: 5.4.5: Usage of specialized software in dealing with CEHT

During the course of FGDs some interesting insights were shared by the participants about older officers who were technologically challenged and have come up the ranks and who were placed in cyber-crime units as Investigating Officers. They faced immense difficulty in applying any technological solutions. The situation had a direct bearing on the prosecution as the investigating officer is also mandated with the responsibility of presenting the evidence in the court of law.

5.4.6 Awareness on software/service for dealing with CEHT Cases

Noting that the participants formed a diverse group of police officers constituted from cyber investigators, the AHTU officers and also the CID, the study attempted to know the awareness amongst the participants about technological tools in dealing/investigating CEHT cases. Participants were asked if they were aware of any specialized software or service that can be used for dealing with the CEHT cases. 73 percent of respondents said that they have no knowledge about it and only 18 percent acknowledged having known of such software/ service. 9 percent of respondents did not provide any response.

During the FGDs, it was discussed that the lack of infrastructure, absence of the latest technology, and budget constraints in procuring software were limitations in capacity building.

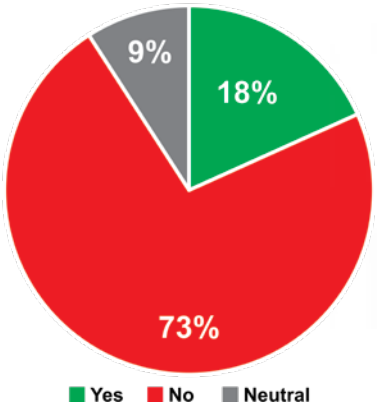


Fig 5.4.6: Awareness on software/ service for dealing with CEHT Cases

5.5 Revenue and Transactions

Human trafficking is one of the fastest growing criminal enterprises next to drugs and arms. The hundred-billion-dollar industry preys on human vulnerabilities for revenue generation. With growing digitization of all financial transactions in India an attempt was made to understand both the usage of cyber technology in facilitation of crime, and also whether the digital money trail has improved crime investigations in such cases.

5.5.1 Cyber Technology for Revenue Transactions in Facilitation of Crimes

Human trafficking for any purpose and through any means is for the sole purpose of revenue generation. In order to understand the role of cyber technology in facilitation of revenue transactions the participants were asked the specific question on how money transfers took place in such crimes.

A majority of respondents (86 percent) alluded to UPI used for money transfers, 30 percent to money transfer through western union, while 29 percent respondents mentioned crypto currencies, and 26 percent cited electronic bank transfers through NEFT (National Electronic Transfer) or RTGS (real Time Gross Settlement) as modes of payment. Only a small number of respondents (10 percent) indicated the usage of checks, and 9 percent talked about other forms of transactions such as cash.

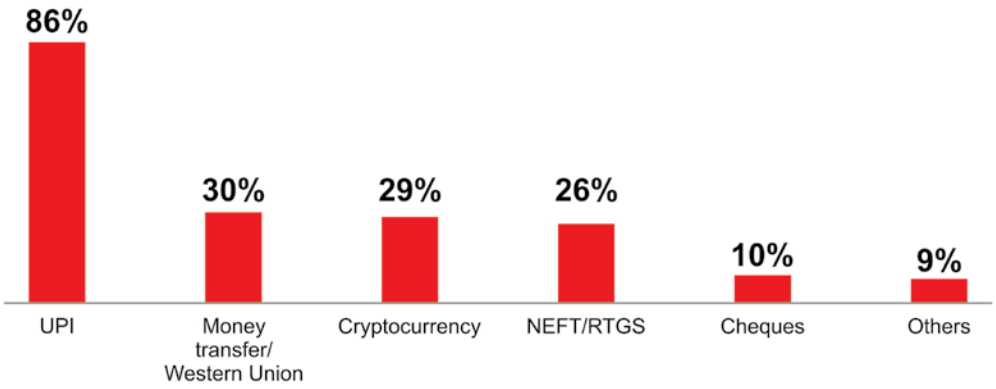


Fig 5.5.1: Primary payment modes in facilitation of cyber-crimes

In the course of qualitative discussion, the participants shared that digital payment apps like Paytm, Google Pay, and Phone Pe facilitate transactions between traffickers and buyers, providing a convenient method for exchanging money.

5.5.2 Tracing the money trail in Crime Investigation

Tracking the proceeds of the crime has been traditionally an important tool used in crime investigation involving financial frauds. As revenue generation is the core objective of human trafficking the participants were asked if the investigation of money trail was helpful in identifying the traffickers. Responses were seen to be divided with 43 percent of respondents saying that it proved helpful and an equal number of respondents (43 percent) saying that it does not help in identifying the traffickers conclusively.

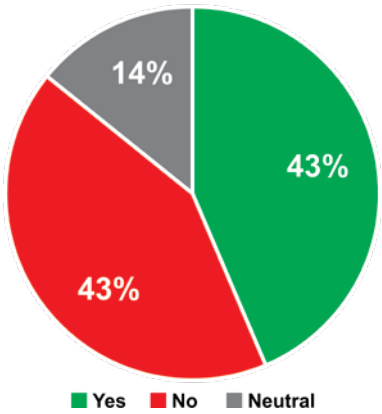


Fig 5.5.2: Are money trail helpful in investigations

During the FGDs, participants discussed about the "mule bank accounts" which are bank accounts of innocent/unsuspecting persons being used by criminals for receiving funds illegally, often by paying a small fee to the account holders. Participants shared that while investigating money trails, very often they identify the bank account in which funds of criminal proceeds were received,

that eventually turns out to be mule accounts. The account holders have no information about the actual criminals. Investigations in such cases reach a dead end and result in wastage of time and resources. Similarly, in cases where money was moved through various accounts, with account holders/banks in different states, it was difficult to coordinate with interstate stakeholders. It was also mentioned that criminals are well aware of these loopholes, and they exploit them to their advantage.

Participants from Odisha and Maharashtra mentioned several cases where current bank accounts of shell companies were used for committing financial crimes. Since current accounts have a higher transaction limit, they are preferred by criminals to be able to do transactions of high amounts. During investigations, police often find that companies were registered by providing fake details to the Registrar of Companies (ROC), thereby hitting a dead end. In Telangana, it was learned that companies are also being bought and sold just like mule bank accounts with an intention to commit financial crimes. Participants mentioned that they had encountered a case wherein 79 accounts belonging to 42 shell companies were discovered. These accounts were sold for Rupees 2 lakh per account.

5.6 Difficulties in Gathering Digital Evidence

One of the objectives of the study is to assess the preparedness of the law enforcement mechanism to respond to CEHT within the existing legal framework. Under this objective, participants were asked about their experiences in collecting, handling, storing and presenting digital evidence in CEHT cases.

5.6.1 Collection of Digital Evidence

Participants were probed about the method by which they collected digital evidence. 78 percent of the respondents mentioned that they **call a digital forensic** expert to collect digital evidence. 73 percent of the respondents declared that they **collected digital evidence under the seizure report.** It was further revealed that both the processes are carried out on a case-to-case basis depending on the requirements of the case.

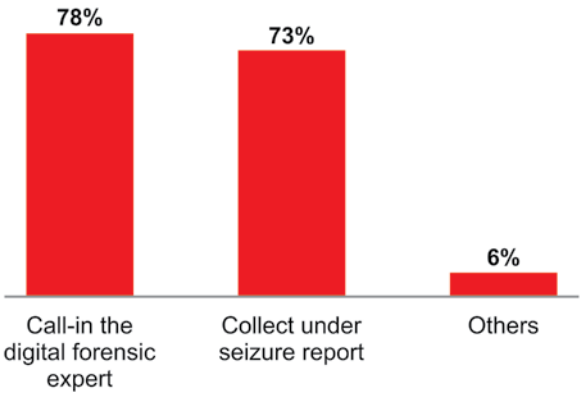


Fig 5.6.1: Method of collection of digital evidence

5.6.2 Provision to keep the custody of digital evidence without breaking the Chain of Custody

Indian laws stipulate strict procedure to handle digital evidence, wherein a lapse would render all investigation efforts as meaningless. The study sought to understand the existing capabilities and challenges that law enforcement face in such situations. The participants were queried on the provisions on the custody of digital evidence without breaking chain of custody. The majority of the respondents (47 percent) revealed that they do not have provisions for storing digital evidence without breaking the chain of custody. On the other hand, 43 percent mentioned that they have provisions to store digital evidence without breaking the chain of custody.

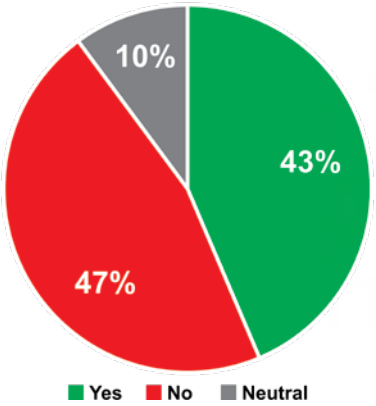


Fig 5.6.2: Do law enforcement have adequate provisions to preserve digital evidence and maintain chain of custody

During the FGDs, certain participants shared that many still rely on external expertise to assist in managing digital evidence effectively. Discussions clearly indicated lacunae in the infrastructure and procedural framework of law enforcement organizations. The specialized/dedicated units (such as cyber cells) are well aware of the procedures and are also equipped suitably, whereas other departments are neither aware of the procedures nor equipped to handle the digital evidence

5.6.3 Challenges faced in gathering digital evidence in CEHT Cases

To understand the challenges on-ground in gathering digital evidence, especially in CEHT cases, the participants were requested to state the challenges they faced.

An estimated 67 percent identified the **lack of cooperation from technology companies** as a major hurdle. This involved difficulties in obtaining user data, encountering restrictions on accessing private communications, and navigating complex legal procedures for data requests.

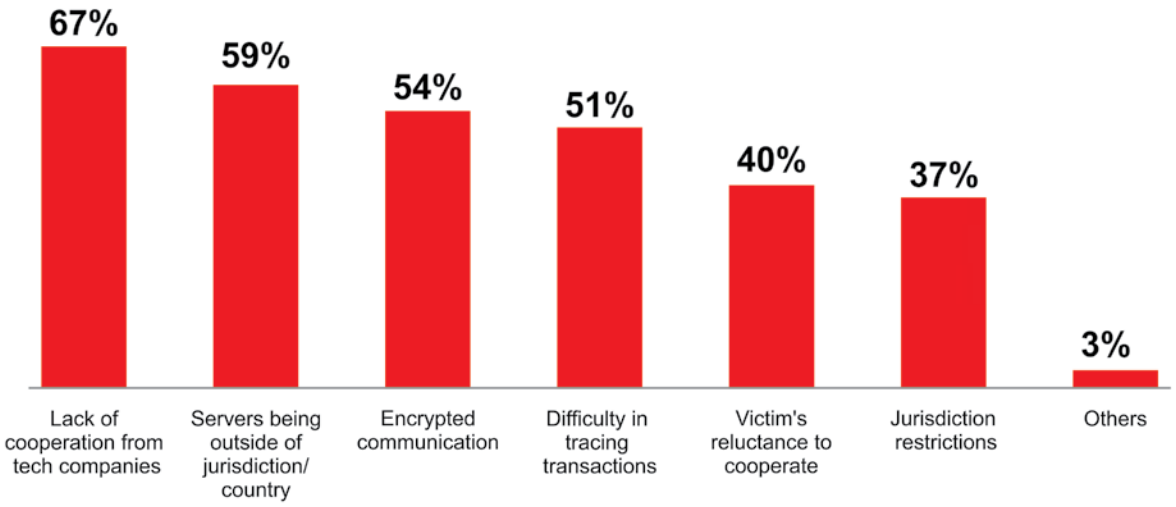


Fig 5.6.3: Main challenges in gathering digital evidence in CEHT cases

Nearly 59 percent of the respondents highlighted the challenge of **servers being located outside** the country. Difficulties are thus caused in obtaining legal authorization to access data stored on these servers, resulting in delays and roadblocks in investigations.

Around 54 percent of the respondents reported challenges due to **encrypted communication methods** used by traffickers. 51 percent of the respondents identified the **difficulty in tracing financial transactions** as a challenge. Nearly 40 percent of respondents highlighted **victim's reluctance to cooperate** as a major challenge. According to 37 percent of the respondents, **jurisdiction** issues too pose a challenge to them. Enforcing laws and gaining access to evidence can be complex when trafficking activities take place across state/national borders.

In the course of discussions, participants elaborated that victims do not come forward to complain due to fear of retaliation, trauma, or a lack of trust in law enforcement. The cases often fall flat when witnesses and victims turn hostile. It was also mentioned that in many cases victims only want immediate reprieve such as getting their money back or their inappropriate content being removed from online platforms. They do not want to go deep into the process of police cases and court hearings. The lack of cooperation by technology companies was cited repeatedly as the biggest hurdle. It includes not getting the required information, and in the cases where partial information is provided, it is delayed inordinately. The officers also described challenges occurring due to technical and jurisdictional aspects.

5.6.4 Legal Challenges in Admissibility of Digital Evidence

In response to questions concerning the admissibility of digital evidence in court and legal challenges thereto, 56 percent of respondents cited significant obstacles as lack of Clarity and Standardized Operating Procedures (SOPs) for managing digital evidence. Nearly 53 percent of the respondents identified the lack of adequately equipped and staffed digital forensic labs as a major concern. This results in delays in processing digital evidence. Nearly half of the respondents (49 percent) indicated that data encryption poses a significant challenge.

In the course of the FGDs, participants discussed that perpetrators often exploit secure communication channels and delete incriminating digital footprints making it difficult to recover evidence. The officers also lamented the lack of SOPs and skills in handling digital evidence. While certain states like Kerala and Telangana shared that they had advanced infrastructure to deal with new forms of digital evidence, most of the states are yet to upgrade their infrastructure.

Participants from Meghalaya shared that their state is in the process of setting up a cyber lab and currently they only have the capability to acquire data from a device. They send the digital device/acquired data to Guwahati for forensics. This dependence on another state adds delays. Similarly, participants from Goa mentioned that the state has only one Cyber Police Station grappling with a high volume

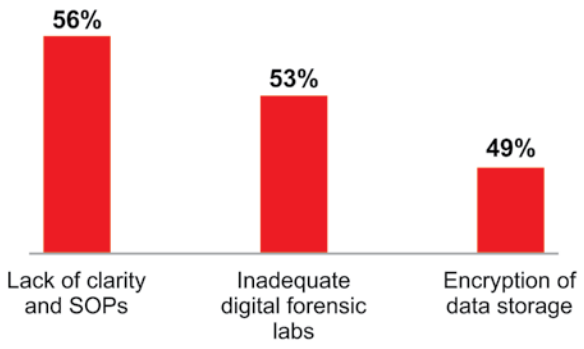


Fig 5.6.4: Legal challenges in admissibility of digital evidence

of backlog. Participants from Rajasthan, Odisha, West Bengal and Bihar also pointed to lack of infrastructure as a challenge for collecting, storing, and presenting digital evidence.

5.6.5 Investigation of Technological elements in Human Trafficking Cases

In order to understand when exactly the investigating officers look for digital evidence in a CEHT case, majority (67 percent) said that they look for digital evidence **when victims mention the usage of cyber technology** in their statement. Another 60 percent said that they explore digital evidence if it is **present at the crime scene.** And 15 percent said that whenever basic elements of Section 370 of IPC related to trafficking are met, then they do not look further for technological evidence. Just 4 percent of the respondents stated there might be other considerations for including technology in investigations, and it is done on a case-to-case basis.

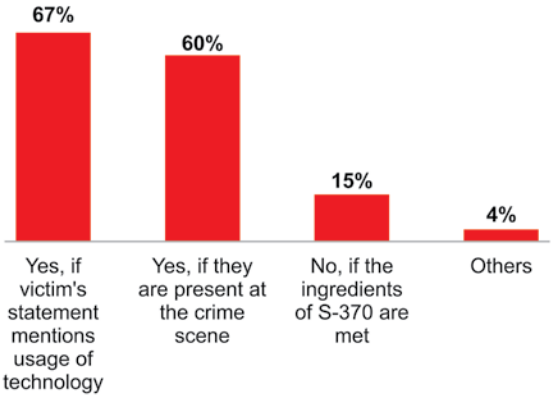


Fig: 5.6.5: When the investigating officers (IOs) look for technological elements in a human trafficking case

5.6.6 Challenges faced in investigation of CEHT Cases

For the pertinent question of challenges faced during investigation of a CEHT case, 65 percent identified difficulty in **tracing the use of technology** as a major challenge. Nearly half of the respondents (49 percent) mentioned **difficulty in seizing digital evidence**. **Under-reporting of facts by victims** emerged as another concern raised by 43 percent of the respondents, while 41 percent of respondents highlighted the challenge in **storage of digital evidence** securely and ensuring its accessibility for investigation and potential legal proceedings.

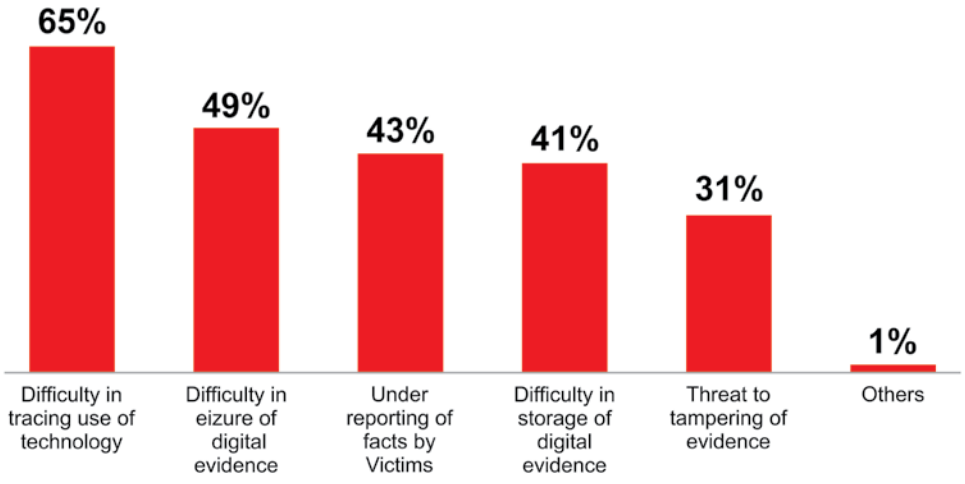


Fig 5.6.6: Challenges in investigating a CEHT case

5.7 Difficulty with Technology Firms/ Intermediaries

Technological firms are responsible for designing the software and bringing out cyber-enabled services that are used by all. For the companies which are business entities, market interests usually govern the nature of services provided. The need to attract as many consumers as possible is core to their business needs. The number of start-ups and businesses offering cyber-enabled services has skyrocketed due to increased digitization, creating fierce competition among them. Hence survival for these companies depends on building attractive packages that are easily accessible to all. In the course of such business interests, cooperating with the criminal justice system is not big on the priority list of any technology firm. On the other hand, there is stiff resistance for any compliance aspect that might affect the number of consumers. In the past decade or so, governments across the globe have systematically brought in legal frameworks to compel technology firms to become more accountable and comply with the law of the land. This section looks at cooperation by the technology firms from the lens of the law enforcement mechanism.

5.7.1 Support expected from technology firms/ intermediaries

Regarding the kind of support expected/ required from technological firms/ intermediaries, 79 percent of respondents wanted them to **provide metadata and other details in a timely manner** to facilitate investigation or timely action. Although 63 percent thought that they can help in **tracking/ tracing the accused,** 58 percent respondents wanted technology firms to assist in **tracking/tracing the victim**. Further, 56 percent of respondents felt that technology firms can assist in **removing sensitive/ abusive/ exploitative contents** hosted on their platforms.

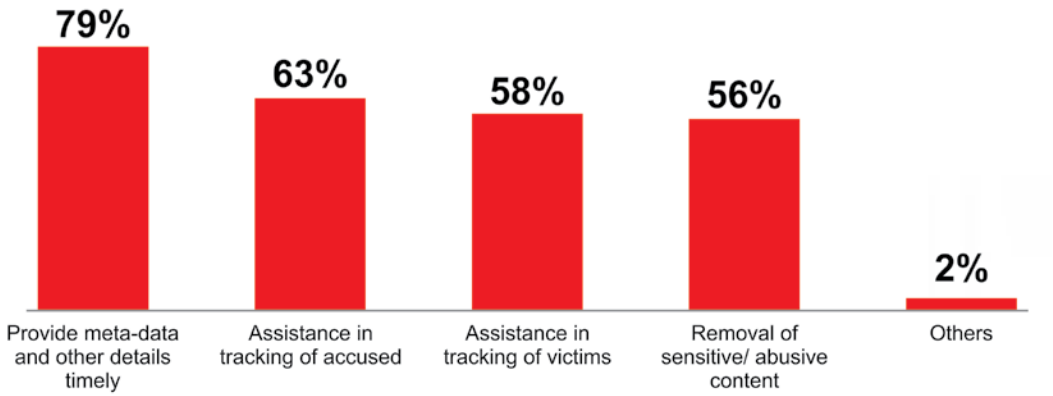


Fig 5.7.1: Support expected from Technology Firms

5.7.2 Challenges encountered in seeking information from technology firms/ intermediaries

When asked regarding the level of cooperation received while seeking information from technology firms/intermediaries through laid down procedures, 76 percent of respondents said that they face challenges in dealing with technology firms for the purpose of investigation while 18 percent said that they had received reasonable cooperation from the technology firms. It is very evident from the above data that seeking cooperation with a technology firm in matters of investigation is not an easy journey for most law enforcers. One of the major challenges with technology firms cited by them during the FGDs was delays in providing information. They shared

that 72 hours is the cooling off period wherein technology firms do not take any action, and typically take 15-45 days to respond with details, if they do so at all. Through their experience, participants were of the view that technology firms have their own yardstick in cooperation. They provide information as per their community guidelines. For example, they typically do not respond in cases of missing person, human trafficking, etc. However, in the cases related to CSAM and crime against women and children such as rape, murder, or imminent threat to life, they provide information promptly. There was a mixed response regarding the level of cooperation of Meta Inc, as few states had experienced a better response from Meta, while others had the opposite experience. As regards Telegram, every state's police said that its cooperation level in investigations is very dismal.

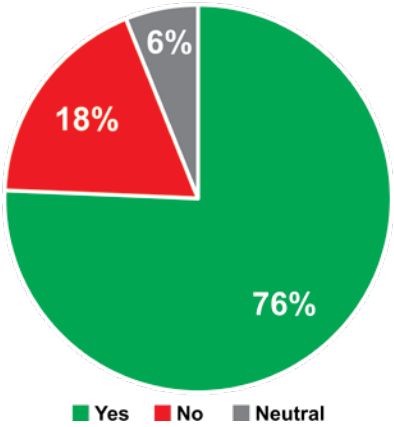


Fig 5.7.2: Challenges in Dealing with Technology Firms

5.7.3 Types of issues in cooperation with Technology Firms

Participants were asked regarding the kinds of issues that they encounter when dealing with technology firms/ intermediaries.

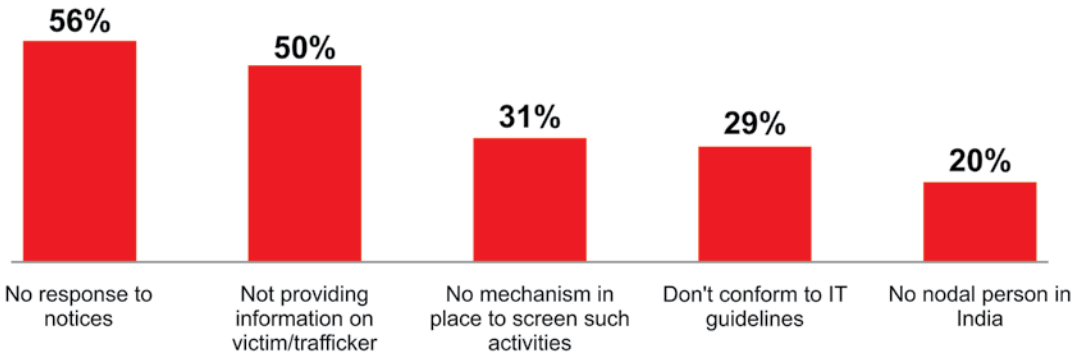


Fig 5.7.3: Cooperation issues faced with technology firms

Nearly 56 percent of respondents said that **technology firms do not respond to notices,** and the other 50 percent observed that **technology firms do not provide any helpful information** about the victim or the accused. Interestingly, 31 percent were of the view that **technology firms do not have mechanisms in place to filter malicious activities** using their platforms, and around 29 percent felt that they **do not conform to the provisions of the IT Act**. Just 20 percent of respondents said that some of the technology firms **have not appointed a Nodal Officer in India** at all.

During the FGDs the participants spoke about the lack of response from technology firms to the notices sent. It was further pointed that those who responded were reluctant to provide certificates under Section 65B (4) of Indian Evidence Act when providing data, as it would make them a witness in the case. In the absence of such a certificate, the evidential data is not admissible in the court.

Regarding lack of response by technology firms, the participants observed that there is only one nodal officer appointed by technology platforms in India as per the IT Intermediary Guidelines, 2021. They are therefore overburdened by the volume of requests from LEAs and randomly filter out two thirds of the information requests without responding. Participants also pointed out that platforms such as Locanto, Tinder, MailChimp, VPN providers, and domain providers have not even appointed a Nodal Officer in India. Certain participants also pointed out the absence of regulation for online advertisement and felt that this void needs to be addressed.

5.8 Challenges in Investigation and Prosecution

With newer forms of crimes emerging in this cyber era, the law enforcement mechanism has to rise to the situation and set up newer units to handle these specialized crimes. The fact that traditional forms continue unabated ensures that a large section of the police force is occupied to handle the same; the newer units of police are just evolving as per the need and refining their operations as they get a grip on the operational models. The enforcement mechanism, which is struggling with a lack of expertise and an uncooperative ecosystem of stakeholders, including technology firms, is far behind cybercriminals, who are ahead in this race. This disparity will undoubtedly make it difficult to investigate and prosecute cases of CEHT.

5.8.1 AHTU and Cyber-Crime Units

During the FGDs, across the states, one topic that frequently emerged was the allocation of duties among AHTU, the Cyber-Crime Unit, and regular police stations. It was brought out that AHTU lacks the jurisdiction to register complaints and conduct investigations. Their role is to solely collect information, perform raids, arrest the accused, seize the material evidence, and hand it over to the local police station for further investigation. AHTU is also not authorized to send notices directly to technology-enablers seeking required information. Only the Cyber-Crime Unit, which is a designated police station, can establish contact with technology companies to seek information for investigation. Participants voiced their belief that cases under section 370 of the IPC (Section 143 BNS 2023) would typically go unnoticed by the Cyber-Crime Unit, which would only gather information for cases registered under the IT Act.

5.8.2 Investigation of Cyber-crimes

The Cyber-Crime Unit officers shared the nature of their problems and challenges during FGDs. Firstly, as per Sec 78 of the IT Act, the power to investigate cyber-crimes is not given to ranks below Inspector. The number of Inspectors available in any jurisdiction is a handful whereas the number of cyber-crimes reported per day is overwhelming. Moreover, the number of cyber-crime cases is increasing rapidly, surpassing the capacity of investigating officers. Invariably, these Inspectors have a team of junior officers (SI or ASI) with strong technical skills supporting them while they conduct their investigations. However, problems arise when the court refuses to allow the SI or ASI, who personally conducted the investigation and is highly knowledgeable about all the technical aspects, to testify during court proceedings. The court insists that only the Inspector (the designated IO)

should present the evidence. And often it has resulted in the IO not being able to present good/ sound technical evidence to the satisfaction of the court, thereby weakening the case.

An interesting and innovative example was set by the Mumbai City Police, to overcome the challenges cited above. In the face of multiple challenges related to financial fraud through instant loan apps which were further aggravated by the suicide of a victim, Mumbai City Police innovatively tried to address the problem by setting up a converged team of all Cyber Inspectors in the city who jointly investigated this crime on par with an organized crime.

5.8.3 Collection and analysis of digital evidence

Collection/seizure of digital devices such as smartphones, computers, etc., extraction of digital evidence from them, and its analysis are crucial parts of cyber-crime investigation and prosecution. The study explored the methodologies and various tools being used by LEAs.

When asked about the various forensics tools being used in investigation by their departments, Forensic Toolkit or FTK, a computer forensic software emerged as the most commonly used tool used with 33 percent of respondents acknowledging usage. Oxygen Forensics and Write Blockers were the next most used tools with 29 percent responses respectively. Password cracking is commonly done by law enforcement as 25 percent of respondents said that Password Recovery Tool Kit is being used in their departments. However, as the participants formed a diverse group of AHTU officers, Cyber Investigators, and other police officers, nearly 23 percent of respondents were not aware of usage of any forensic tool by their department. A few participants also mentioned 'other' tools being used by them such as Cellebrite UFED, Purple Radiance, Cyniq, GPS Forensic tools, and OS INT.

During FGDs, participants also shared certain associated issues with the extraction, preservation, and examination of digital evidence. Firstly, there are very few forensic labs in the

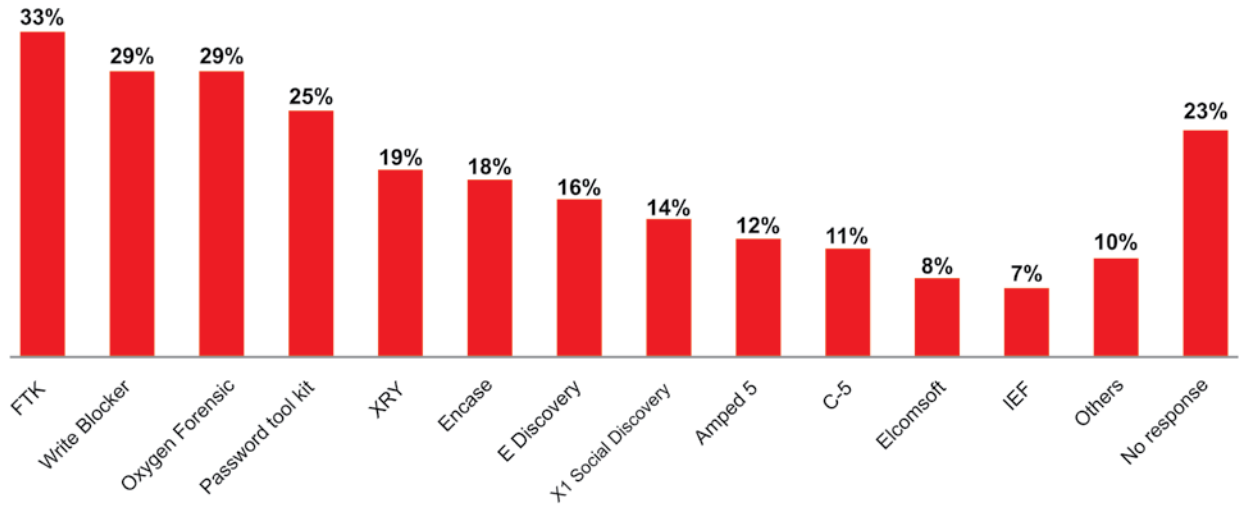


Fig 5.8.3: Software used for investigation

state that handle a large number of cases. Moreover, the time it takes to receive a report on a case submitted for forensic examination ranges from six months to over a year. Secondly, issues such as lack of training with respect to the correct procedure at the level of the officer who seizes a device, difficulties in following and maintaining correct procedure, and chain of custody throughout the examination process due to paucity of resources, etc., leads to the evidence being rendered inadmissible in court. Further, improperly trained IOs do not record the case details properly, making the requirements requested from forensic labs vague, in addition to the possibility of the case facing problems in courts subsequently.

The delay is, however, not solely attributed to the delay in getting the forensic report from the labs. During FGDs, officers expressed their helplessness over delays in responses from technology firms, which further add to the tally of pending cases with them. A participant tried to depict the enormity of the issue, giving an example that if there are 20 cyber-crimes reported per day and if technology firms take 45 days to respond to a query, the same results in 900 cases already pending with the IO by the time they receive inputs from a technology firm. Further, there is a time limit (60-90 days) for filing a chargesheet from the date of registration of a case. Due to delays in response from the technology firms, police often resort to dropping portions related to the technical evidence while filing chargesheet.

5.8.4 Challenges in investigating a cyber-crime/ CEHT

The participants of FGD discussed several challenges they faced in investigating CEHT cases and cyber-crimes. Following are the typical issues:

(a) For a variety of reasons, victims postpone reporting cyber-crimes. As time elapses, the recovery of relevant evidence becomes increasingly difficult.

(b) Money trail investigation becomes difficult due to the dissipation of funds through multiple transfers. Investigation of the money trail after the 4th level of transfer becomes untraceable. Also, within an account, there are a massive number of transactions, which compound the difficulty.

(c) In CEHT cases, police face problems due to the indoctrination through efficient grooming of the victim girl who is reluctant to give incriminating statements about the accused. Sometimes, they become hostile witnesses.

(d) Technological limitations such as no visibility of data on the VPN, encrypted chats and backups, non-feasibility of determination of the identity of a person from Telegram's user ID, inability to recover data after a certain period as it was deleted by the service providers as a routine/prevalent data retention policy were discussed.

(e) Fake SIM cards i.e. SIM cards obtained using fake identities and anonymous usage of social media/most cyber services were cited as major enablers of cyber-crimes.

(f) It has been observed that certain people offer their bank accounts as mule accounts to cyber criminals, for a fee. When their account is frozen during investigation, etc., they play the victim card claiming innocence stating that their account was misused by unknown cyber criminals.

5.8.5 Multi-jurisdiction Challenges

During FGDs, issues related to the challenges of multi-jurisdictional cases were commonly found across the states. There are major operational challenges in getting an independent witness as mandated by the law and also in obtaining the transit remand of accused when they are apprehended in another state. Issues of poor cooperation by the police of the host state emerged, to the extent that visiting officers carried the impression that host police sometimes facilitate the accused to escape arrest. There were mixed experiences, largely negative, regarding the logistical requirements such as the provision of transport, a local guide, and other resources for the visiting police team, expected from the host state.

5.8.6 Prosecution challenges

The participants were asked as to what major challenges they face when presenting a CEHT case for prosecution in collaboration with the prosecutors and the judiciary. 64 percent of participants felt that **lack of expertise**, especially related to cyber-crimes and digital evidence **among legal professionals** is the main hurdle in giving them an effective comprehension of the matter. 58 percent said that they face **challenges in presenting digital evidence** for various reasons.

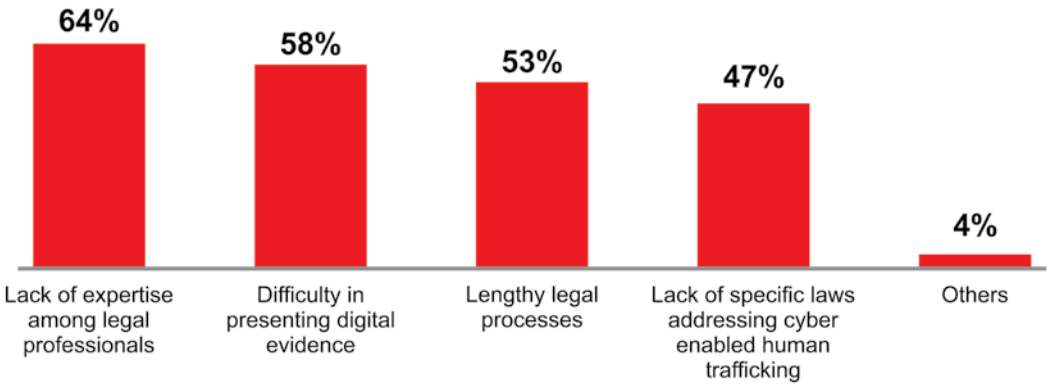


Fig 5.8.6: Main challenges in prosecution of CEHT cases

53 percent of respondents said that the **lengthy legal processes** create problems in prosecution. 47 percent of respondents observed that **lack of laws specific to CEHT** make their tasks challenging as they have to then resort to various other laws applicable to the crime in parts. 4 percent of respondents gave additional inputs such as the need to expedite CEHT related cases keeping the nature of crime in mind as delays often lead to the victims losing faith and becoming hostile.

During FGDs, it came out that challenges in presenting digital evidence in court include reasons such as IOs' inability to explain evidence/ analysis procedure properly, lower level of understanding of the nature and capability of digital evidence amongst legal authorities and lapses in stipulated procedures of seizure/ extraction/ examination of digital evidence pointed out by the defense.

The lack of an adequate number of specialized courts and a large number of pending cases in them have also been cited as legal hurdles in prosecution during the FGDs. Due to lengthy legal

processes, problems such as victims from other states/regions returning back and being unavailable to depose as a witness, continuity of an Investigating Officer, some local victims becoming hostile, etc. arise. An interesting anecdote was shared, wherein, an officer saw his case falling flat during prosecution when the critical witnesses who were employees of an NGO that provided leads for the rescue, turned hostile for they were no longer employees of the NGO at the time of hearing.

5.8.7 Administrative Challenges

The investigation process is hindered by administrative factors that are common to all states. These include insufficient funding, a lack of technological equipment at police stations, inadequate travel allowance for out-of-state investigations, no provision for drawing travel allowance in advance, excessive delays in reimbursement after submitting claims, etc. Officers also mentioned that they have to travel on short notice for operational reasons, which means they have to put up with the inconvenience of taking trains without a confirmed reservation.

Officers from certain states brought out that the training they receive is not aligned with the tasks they perform on the ground. Fewer trained cyber investigators are available and not all inspectors who handle cyber-crimes are trained for that. Frequent transfers were discussed as a problem that breaks continuity and prevents an individual from developing domain-specific skills over time. It was also revealed that although cyber police stations exist at the district level in the majority of states, they are not supported by the same resources as traditional police departments because they are not considered mainstream policing.

5.9 Support For Law Enforcement Mechanism

Preparedness of the law enforcement mechanism to respond to emerging crimes depends on several factors such as, updating knowledge and skills through in-service training, access to appropriate infrastructure, collaborative engagement with stakeholders who support prosecution, extra-jurisdictional cooperation, and specialized mandate.

Response to CEHT implies know-how of technology and various tools that can be applied to crack a case in the cyber space, engaging with technology firms for investigation, coordinating with other states within the country, and collaborating internationally.

In this section an attempt was made to understand the preparedness of the police force and their requirements to effectively handle CEHT cases.

5.9.1 Training

To establish the current status about the level and type of training being imparted to police, the participants were asked about the training mechanism and if they have received any kind of training on CEHT. Over 54.8 percent of the participants stated that they had not received any in-service training on human trafficking including CEHT. 45.2 percent had received training on various subjects including human trafficking and cyber- crimes but not on CEHT. The data also indicated

that there is no uniformity in training programs conducted in all states. Some states seem to have conducted more programs, and some others have only conducted minimal programs.

The participants who responded positively to having received training were asked for further details of training, the responses are summarized below:

(a) Only basic training is provided.

(b) All Station House Officers (SHOs) (in certain states) are provided basic training to handle cyber-crimes.

(c) Only selected officers/ personnel are trained.

(d) Regular/ quarterly training is organized by state authorities to train police personnel in a phased manner.

(e) Nominated officers are trained at National/ State Police Academy/ Institutions as well as at training facilities of other states.

(f) Training on cyber-crimes and forensics is provided.

(g) Training is provided on the application of laws in some special crimes.

5.9.2 Interdepartmental cooperation issues within a state

Investigation of CEHT cases can be complicated and involve multiple departments within a state. To examine this aspect, the participants were asked as to what kind of support/ cooperation they needed from other departments within their state. Participants shared a wide range of responses, ranging from practical to aspirational in nature.

The areas of desired interdepartmental cooperation as shared by the participants across the 15 states is summarized herewith:

a) Quicker response to any request/ query and the need for uninhibited information exchange between departments.

b) Assistance from the legal department, medical department, child welfare departments and the forensic labs.

c) Training from the IT department and provision for on-call cyber experts.

d) Additional funds for investigation especially to coordinate with other departments.

e) Coordination cell at each district with a nodal officer to facilitate coordination between various state agencies/ departments.

f) Orientation and sensitization of other departments to ensure the severity/ sensitivity of a case is understood by other departments.

g) Setting up a new inter-departmental regulatory body to monitor various mobile apps and their activities.

5.9.3 Interstate Cooperation Issues

Inter-state cooperation is critical for any crime that involves two or more states. Police officers have to routinely seek cooperation with other states when the crime involves multiple jurisdictions. Cases of human trafficking both with intra-state and inter-state manifestations involve working in other jurisdictions which is a constant struggle. In several instances such as tracking in a missing case or a kidnap case, on request of one state another state will take a proactive measure to rescue the victim but might face challenges to detain the alleged accused if the requesting state authorities do not reach the destination on time. Based on their experience of working with other states, the participants were asked about the nature of inter-state cooperation that they seek. The following issues and aspirations were put forth:

a) Need for logistical support about transport and accommodation arrangements, when in another state.

b) Need for cooperation by the local police in providing a local guide, a translator, and provision of local force wherever necessary for carrying out operation.

c) Assist in the investigation, such as in verifying the identity of the accused located in their jurisdiction, arresting the accused, and/or rescuing the victim at their behest.

d) Legal assistance in obtaining the transit remand of the accused, providing technical support through locally available resources, and also providing access to software tools to analyse the evidence obtained at the field in that state.

e) Create a centralized system that removes the communication gap between different state jurisdictions and maintains a repository of information on accused persons that all the states can access.

f) I4C should share the details of cases registered by a state with all other states, including the evidence. This would help in the investigation by facilitating IOs in corroborating evidence. As of now only the Docket Number is visible to other states and no case details are accessible.

g) Nodal officers to be placed at each district level to facilitate interstate cooperation.

5.9.4 International Cooperation Issues

As in inter-state cooperation, international cooperation is pivotal for a borderless crime like CEHT. Different countries may be required to interact together when they are either a source or destination of human trafficking. However, in the case of CEHT, a country that is home to a technology platform providing services in India that is used in some form in CEHT, also becomes a stakeholder. Although the demands for desired international cooperation may resemble those for interstate cooperation that we looked at in the previous section, the geopolitical ramifications of these requests necessitate a strong national political will as well as protracted diplomatic discussions to reach a consensus. The issues included:

a) Support/cooperation for timely response, assistance in identification and arrest of accused, logistical support, legal assistance, and help from the local cyber experts.

b) Cooperation of Interpol in the investigation.

c) Assistance of immigration officials for the arrest of the accused.

d) Countries that are home to technology firms should assist in obtaining information/ data from them.

e) Mutual sharing of new technologies that have been developed/utilized in carrying out an effective investigation.

f) Mutual Legal Assistance Treaties with countries that have to be engaged to tackle this crime.

g) Internationally agreed upon liaison units for easy communication and cooperation.

5.9.5 Requirements for Dealing with CEHT Cases Efficiently

There was near consensus among all the participants that CEHT does not get the priority it deserves, in fact, it is not even acknowledged as a real concern. Having understood the gravity of the situation the participants were asked about the nature of support they required to deal with CEHT cases efficiently. Of the participants, 72 percent wanted **training on detection and investigation** of these crimes. Another 68 percent felt that they need **training in the usage of technology** to be efficient at the mission. A further, 64 percent said that they need **training on the application of laws,** while 58 percent highlighted that **access to up-to-date technological infrastructure** is crucial for the success of their cases. Nearly 51 percent underscored the need for a **dedicated budget for investigations** and to meet the logistical requirement.

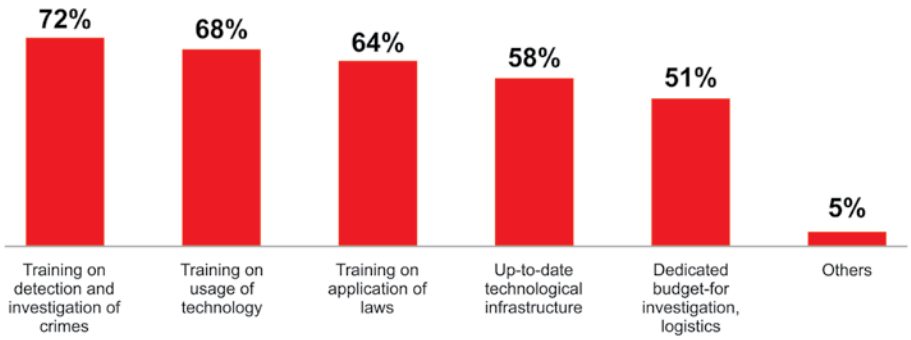


Fig 5.9.5: Requirements to be able to deal with CEHT cases efficiently

During the FGDs, the need to train prosecutors and NGOs on CEHT was discussed in detail. The participants believed training prosecutors will improve prosecution and that having trained NGOs will assist in both crime detection and victim protection.

5.10 Victim Protection and Challenges Faced

At the core of any human trafficking case is a human being who is a victim. The journey of trafficking through false promises, grooming, or coercion is also about a deep sense of betrayal,

shame, and guilt. The process of being trafficked and thereafter being exploited leaves irreversible damage to the body, mind, and soul of the human being. This multi-layered trauma combined with an acute trust deficit very often makes a victim hostile to the criminal justice system adversely impacting a case during its prosecution stage. A holistic victim protection and victim services is a neglected zone, and efforts from state and non-state players are much below the desired level.

An attempt was made to understand the participant's perspective on the challenges faced by the victims, existing support services, and what more could be required.

5.10.1 Challenges faced by victims of CEHT

Participants were asked what challenges victims face when it comes to reaching out for help or escaping their exploitative situation. While 76 percent identified lack of awareness about available support as the biggest challenge, 66 percent said that fear of retaliation is the reason for the victims' unwillingness to report the case. 39 percent participants believed coercion and control through technology was the threat that silences the victims, and 30 percent cited that limited internet access that is unmonitored forces a victim to remain in captivity and servitude.

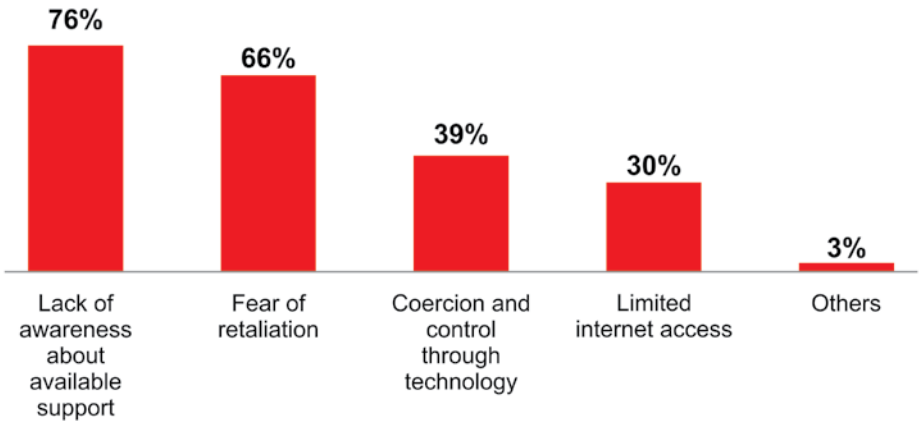


Fig 5.10.1: Challenges faced by victims of CEHT

5.10.2 Victim support services

The existing state of victim support services available in the country requires a deeper understanding. When asked, 74 percent of the participants said they were unaware of any services that were available for victims of CEHT, 19 percent said there were no specialized services available for victims, and 7 percent chose not to answer the question which could be interpreted as they had no knowledge of the same.

In response to a follow-up inquiry regarding the nature of services offered, 73 percent of participants mentioned free legal aid, 62 percent mentioned the availability of shelter homes as protection services, and 43 percent believed that the ability to request content removal is also a victim support service.

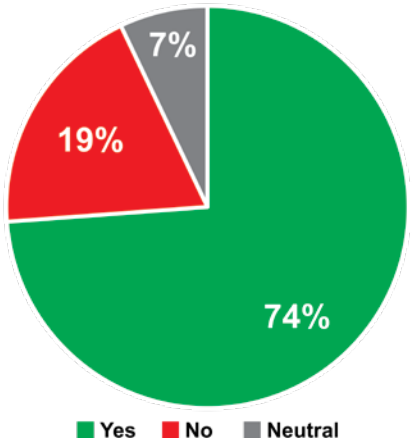


Fig 5.10.2 (a): Are there victim service provision for CEHT victims?

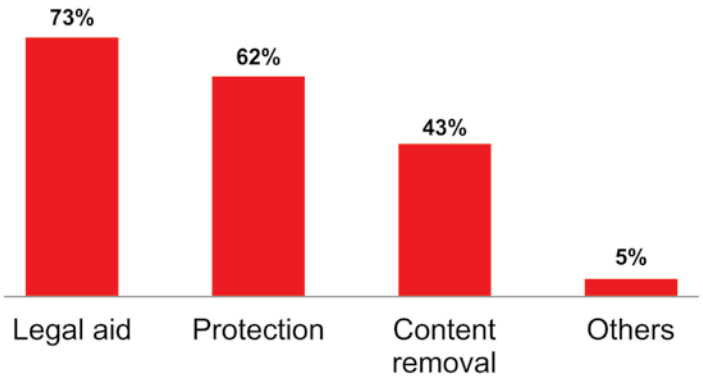


Fig 5.10.2 (b): Type of support provided to victims of CEHT

5.10.3 Improvements in victim support services

Participants were asked about their ideas for how victim protection services could be made better in order to find out if they saw any gaps in the current offerings. Several suggestions were received, which are summarized below:

(a) Victims can be supported by immediate/ earliest removal of exploitative contents pertaining to them.

(b) The identity of victims should be kept confidential and not disclosed through media, especially for minor victims.

(c) Victims should be provided with expeditious trials.

(d) There is a need to treat such cases with empathy and compassion. Moral support to the victims, especially those rescued from commercial sexual exploitation should be provided.

(e) Victims should be provided with mental and physical support through psychological counselling and medical facilities. Their confidence needs to be boosted, assuring them that their suffering wasn't their sin/mistake.

(f) Victims should be given information regarding the legal aid and protection available to them. They should also be guided about the rehabilitation opportunity and compensation provisions.

(g) Victims should be given financial aid, education, and jobs. To achieve this, there is a requirement to obtain sponsorship.

(h) Help victims feel inclusive in society.

(i) Shelter homes for victims should be established where they are provided counselling and compensation. Victims can be kept at such shelters for a certain period and apart from the above, they can be provided with some kind of vocational training, to enable them to be financially independent.

(j) Victim services can be improved through participation and coordination through various stakeholders such as the social welfare department, NGOs, etc.

(k) Spreading awareness among vulnerable groups is an important preventive measure that should be undertaken. Videos/ films on awareness content can be made and played out in remote areas to create mass awareness of the nature of crimes, so that they are better prepared to protect themselves.

(l) There should be a nodal officer appointed who is responsible for periodically tracking the rescued victims and ensuring their safety, adjustment in society, and also determining whether they need any further assistance.

(m) Laws are required to be amended to protect victims of CEHT.

(n) Special schemes like "Pari-Yojana" implemented in Odisha to spread awareness against sexual harassment along with establishing mechanisms for girl child rescue or efforts like Disha police stations in Andhra Pradesh should be replicated to improve access for the victims to seek justice.

5.11 RECOMMENDATIONS

The profile of participants, drawn from 15 states, possessed extensive experience, having served in the police force for at least 15 years. While cases of CEHT specifically were not dealt with by a majority of them, their applied knowledge in law gave them insights to suggest what could work when countering such new emerging crimes. The recommendations given are practical and can be easily adopted as a comprehensive response while evolving a national action plan to combat CEHT.

5.11.1 Improving legal and operational framework for addressing CEHT

a) Capacity building: Building the capacities of the police officers with regular training programs and empowering the police stations with adequate infrastructure will build a strong force equipped to handle any new generation crimes. The training should be practical and include different forms of trafficking and the application of law, investigation techniques on cyberspace, methods to write notices, protocols to deal with nodal officers, etc. The training curriculum should be reviewed and updated for relevance and ensure imparting of the same will not affect regular policing.

b) Specialized Units: Setting up special autonomous dedicated units to deal only with CEHT cases with personnel trained in the application of appropriate laws and cyber technology. These units should be mandated to only look at such cases and not be deployed for any purpose with officers given longer tenure to maintain continuity.

c) Stringent laws and faster trials: Existing laws to be amended to bring more stringent punishment for such grievous crimes and special courts to be set up as opposed to designated courts for the speedy trial of such cases.

d) Technical training of judges and prosecutors: Other than law enforcement personnel, those involved in trial stages i.e. the prosecutor and judges should also be trained so that they understand technology and its evidential value well.

e) Predictive Policing: Develop/ use technology tools for the predictive policing to check CEHT. Use open-source intelligence for detection of the crime of CEHT.

f) Improved inter-departmental cooperation: Special formal framework to foster inter-departmental cooperation which will also facilitate inter-state coordination.

g) Victim services: Establishing proper infrastructure for holistic rehabilitation of victims.

h) Community Awareness: Multi-media campaigns using electronic and social media to build awareness in the community targeting especially children. Community campaigns in collaboration with Panchayat and frontline workers such as Anganwadi Workers, and Asha Workers be undertaken to reach out to the rural population to make them aware of online safety.

5.11.2 Improving the investigation process of CEHT cases

a) Forensic Labs: Adequate cyber forensic labs with advanced forensics resources to be set up in all the states.

b) Technically trained manpower: The officers should be provided training on handling technological tools and investigating crimes involving technology. Officers of ranks of ASI and SI, who have the better technical aptitude to be given a mandate to investigate cyber-crimes. Technically trained manpower should be posted/ available up to the district level.

c) Cyber Experts: Enrolling cyber experts under oath to assist the local police in cases where cyber technology is used.

d) Special Task Force: Setting up special task forces routinely to investigate and crack cyber-enabled crimes operated by large criminal networks.

e) Standard Operating Procedure: Clear SOPs on seizure/ collection, custody/ handling of digital evidence should be evolved and all the officers irrespective of their posting should be trained for the same.

f) Adequate funding: Funding requirements be met for operational and administrative purposes.

5.11.3 Assistance by technology firms/ intermediaries in CEHT cases

a) Time bound simplified procedure: The procedure to seek information should be simple and the technology firms should be mandated to provide it in a time-bound manner. Firms that do not comply should be legally penalized for the same.

b) Removal of Content: Technology platforms should promptly respond to requests for removing exploitative or inappropriate content.

c) Information to be provided by Technology Firms: The firms should be mandated to share all information that will constitute evidence such as location history, chat logs, IP logs, email ID, phone numbers, etc. apart from metadata.

d) Retention of deleted data: The data related to any crime involving a deleted account should be mandated to be retained as prescribed by the law.

e) Proactive participation of technology firms: Technology firms should develop preventive technologies in the form of algorithms to detect contents that can potentially propagate crime and block/ report it. They should be made liable for failure to check the usage of their platforms for illegal/ criminal activities.

f) Online regulation of job sites: Job websites including the ones backed/ promoted by the government, should permit only legitimate usage i.e. only verified employers be provided access to the data of job seekers. There should be an audit mechanism for the employers registered on these websites and their activities.

g) State-level Nodal Officers: The firms should appoint one nodal officer per state to assist the law enforcement mechanism.

h) Banning Rogue Technology Firms: Any technology firm which does not cooperate with the law enforcement mechanism should be blacklisted and considered for ban of all operations in India.

i) Easy Access: Create a mechanism for global access to technology firms located in any country, providing data as and when required by LEAs in real-time.

5.11.4 Legal and Policy Reforms

a) Amendment of existing law: The term CEHT should be defined in the law and necessary amendment should be made in Sec.143 of BNS 2023 to include the same.

b) Institutional Regulation: Strict regulatory provision to be mandated to all institutions to restrict access to multiple mobile SIM cards, usage of bank accounts with fake credentials, and anonymous usage of social media.

c) Robust KYC procedures: There is a need to relook at the present KYC procedures to address issues like mule SIM cards, and mule bank accounts. KYC procedures should extend to the usage of technical services too. Anonymous usage of these services should be prohibited.

d) Regulations on cyberspace: A robust legal regulatory provision should be brought for online advertisements and stringent penal action should be taken for any violation.

e) Cooling off Period: Evolve policies for financial institutions to impose a cooling off period of 12 hours for transfer of large sums above Rupees one lakh to provide LEAs reasonable response time to recover defrauded money.

f) Regulation of ROC: Policies ensuring robust verification mechanism of companies registered with the Registrar of Companies (ROC), while maintaining the ease of starting a business.

5.11.5 Institutional Framework

a) Role of I4C: The central agency I4C which was established by the Home Ministry to coordinate cyber-crime should expand its scope of work to include a repository of repeat offenders and alleged accused of cyber-crimes, facilitate inter-state and international investigation, a database of social media profiles against complaints have been registered, and details of all the cases with evidence for IOs to corroborate.

b) Interstate police cooperation: There is a need to evolve a framework to address the issues in interstate police cooperation during investigations and operations.

c) International cooperation: Comprehensive efforts are needed to develop bilateral cooperation ties with other countries or a group of countries participating in a unified response to the CEHT. Cooperation areas are rescue of victims, arrest of accused, and facilitating reasonable cooperation by the technology platforms.

5.12 Conclusion

Law enforcers are at the core of tackling a crime, and there is a great need to build the right ecosystem to facilitate the same. The new and emerging challenge unlike any other crime is the huge volume of cyber-enabled crimes including that of human trafficking which is going to steadily rise in the coming years. Resolving operational issues and investing in building the right environment for officers to function will not only sustain their morale but also be instrumental in building a force that fights with all its might the war-like situation that cyber technology is going to pose as a challenge to both internal and external security of this nation.

The in-depth interviews conducted with more than 365 law enforcement officials in 15 states throughout India provide a comprehensive picture of the patterns and trends of CEHT in the country. The new terminology might be unfamiliar, but the problem is not. The wealth of experience possessed by the officers provided insights into the difficulties associated with conducting investigations and prosecutions, the necessity of institutional frameworks, the importance of training and capacity building, and the necessity of collaboration and coordination with other relevant parties. In order to combat this worldwide crime, cyber technology, cyber specialists and the technology companies that oversee cyberspace have been identified as being crucial and playing a pivotal role in combating CEHT. Comprehending the issue and the current deficiencies in addressing it offers the appropriate structure for creating a NPoA to counteract CEHT.

Chapter

06

Validation Investigations

Chapter 6

Validation Investigations

6.1 Introduction

To qualify the findings of the Action Research, it was important to validate such information through pro-active investigations. This included the need to study the profiles of the victims and perpetrators first- hand, gather information on the precise modus operandi, and mediums/ platforms exploited by the perpetrators as well as gather an understanding of the forms of exploitation and prevalence levels, the gaps and loopholes in the technological platforms open to exploitation, the enabling role played by the technological firms and various players in facilitating and committing such crimes.

While the focus of the Action Research was to understand the trends and patterns of cyber enabled trafficking in India, a critical missing element observed was the absence of authenticated case studies that actually gave a *lived perspective* on how cyber technology is misused to facilitate such an organised crime and the modus operandi being adopted.

In this backdrop, a distinct methodology was adopted in this action research by undertaking validation investigations by trained investigators who would verify the information received by conducting actual decoy investigations in cyber space. The investigations culminated with the lodging of a formal complaint with the Crime Investigation Department of Telangana Police.

6.2 METHODOLOGY

For any civil society organization, ethical considerations and adherence to the legal framework are paramount when conducting investigations. The investigative approach used in the Action Research involved an *immersive technique*. Care was taken to follow a strict code of conduct, and the operations were closely monitored at every step by the Principal Investigator.

Given the specialized nature of the subject matter and such operations, a critical aspect was the required skills and expertise to undertake such investigations. These operations were undertaken under the guidance of the Principal Investigator, having over three decades of experience in leading sex trafficking rescue operations and led by a trained Cyber Investigator, having experience of over 33 years with the Police Department, including almost a decade with the Cyber-Crimes Wing of Hyderabad.

Furthermore, to ensure that these operations were brought to a logical conclusion, a formal partnership was entered into with the Crime Investigation Department (CID), Telangana Police. The Cyber-Crime Police Station attached to the CID facilitated filing cases for further investigations based on the input received from the validation investigations.

In strict adherence to the legal requirements, care was taken to have an exclusive set up with laptops and mobile phones which were handed over to the law enforcement officer designated to handle the case as a part of filing the formal complaint. In the investigations involving CSAM content and sex trafficking of minors, care was taken to ensure no content was disseminated to any other party other than the law enforcement machinery.

Strict code of conduct and confidentiality was maintained by the investigating team even in sharing information with the rest of the Project Team.

6.3 Validation Investigation and Operations

Credible information from various sources was the trigger for all the validation investigations. For this purpose, the investigator engaged with multiple sources, conducted sustained online intelligence gathering, and scanned all the reported cases in the media. The longstanding experience of the organization working with sex trafficked victims and engaging with the victims closely in the safe homes, also provided credible leads in these investigations. Three major leads were then zeroed down for the investigation which included:

1. Sale of Child Sexual Abuse Material (CSAM)
2. Trafficking for Commercial Sexual Exploitation via Dating/Escort Adult Websites
3. Trafficking to carry out Organ Trade

6.3.1 VALIDATION INVESTIGATION I: SALE OF CHILD SEXUAL ABUSE MATERIAL (CSAM) ON TELEGRAM

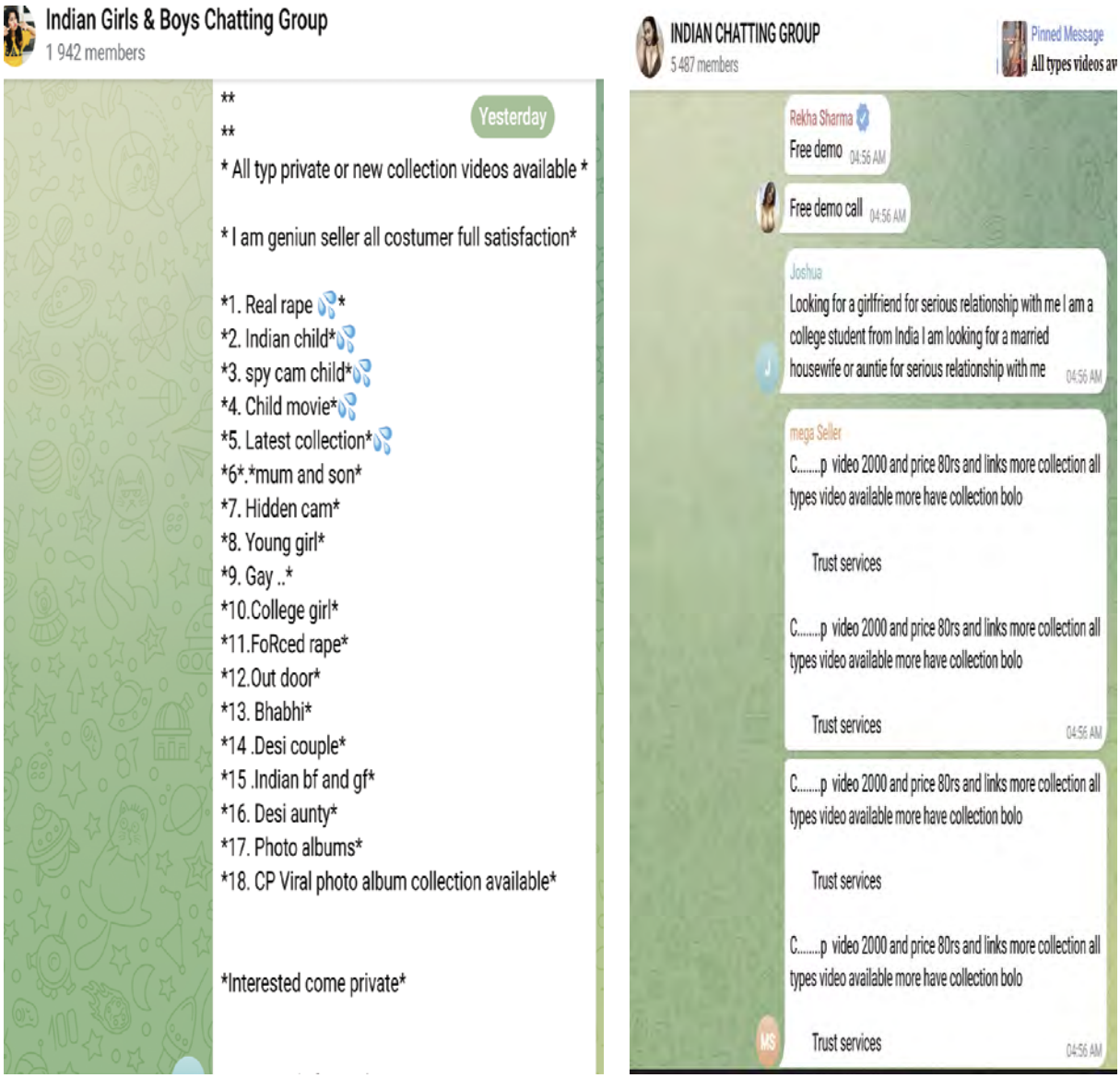
Period of Investigation: 26 October 2023 - 11 November 2023

Intelligence gathering: To understand the actual status of CSAM available online, the investigator checked on various online platforms which were being reported to have disseminated CSAM. After multiple interactions with various sources, a clear indication led to the Telegram. Telegram is a freemium, cross-platform, cloud-based instant messaging (IM) service. The service also provides end-to-end encrypted video calling, VoIP, file sharing, and several other features.

The Investigation: The investigator downloaded the Telegram and signed up with a pseudo name without requiring any identification documents. -

Upon signing up, the investigator learnt that the app has a feature of a search bar that lets you find groups/people/content with certain keywords, similar to a search engine. The app also allows users to search from the contacts list the groups hosted in the Telegram by other subscribers. Using keywords such as 'Indian boys and girls chatting' on the search engine, the investigator came across a group called 'Girls and Boys Chatting'. This was a free-access open channel where anyone could

join and post their content. On pressing the button "Join", he was allowed to join the group and he noticed that the group consisted of over **31,000** active members, and a stream of messages being sent to the group. Most of these were advertising messages in the form of a pre-made template which appeared to look like a 'menu' of the different categories of explicit material including CSAM, rape, molestation, etc. that could be purchased. The investigator then established contact with different sellers for the purchase of CSAM content as well as entry into paid private groups.



Screenshot 1- Menu of explicit content available and private group messages

One of the contacts, 'Seller 3' with the username '@pelvabb', posted promotional messages providing a menu of explicit material that was available for purchase through Direct Message (DM). The message stated, "All types of videos available such as mom – son, rape, child…". The investigator connected with 'Seller 3' through DM and enquired about CSAM content and the mode of payment. The seller instantly forwarded a QR Code of the Phone gateway and asked for payment of ₹400. Post negotiations, the investigator agreed to the amount of ₹150 and initially sent ₹50 to check

the veracity of the QR code and sent the screenshot of the payment to 'Seller 3'. Despite making this payment, when the investigator did not receive the promised content, he reached out to 'Seller 3', when he was informed that the seller was "in tuition", and two hours later the content was provided. After reviewing the CSAM content sent, the investigator informed 'Seller 3' that he had trouble unzipping one of the files, for which he was asked to make an additional payment. Simultaneously, 'Seller 3' advertised that they had new material under the category of "murder" for ₹200. The investigator refused to buy this new content and asked for more CSAM, and following negotiations paid ₹50 on the previously shared QR code.

The content comprising 6 folders of explicit material was delivered via personal chat. The folders contained CSAM depicting oral sex and intercourse with children, solo streaming of children appearing to be in the age group of 3 to 12 years, as well as adult pornography. It also contained videos of gang rape with victims and molesters who appeared to be Indian. All transactions with the first contact were completed in less than 2 hours and 979 MB+ 1.02 GB content was procured which included largely CSAM.

Contact was established with a second seller, 'Mega link Seller' with username '@megaseller345', who had sent a promotional message of links to enter private rooms on the same 'Girls and Boys Chatting' group. The message promoted access to paid private groups upon payment of ₹80. Such groups had between 2 and 100 members and allowed the owner to activate the settings of encryption, and screenshots of this group were however barred given the encryption settings.

Upon enquiry, 'Mega link Seller' sent a PhonePe QR for payment and the investigator made the payment and was given access to group links of content after transferring money to the account of "*Saleya Begum"*. After the transaction, the 'Mega link seller' deleted his account using the self-destruct feature of Telegram, which also deleted all chats with him on Telegram. The self-destruct feature allowed the sender to set a timer on the visibility of the message, which deletes itself. The investigator received over 2000 CSAM videos from five private channels of this seller.

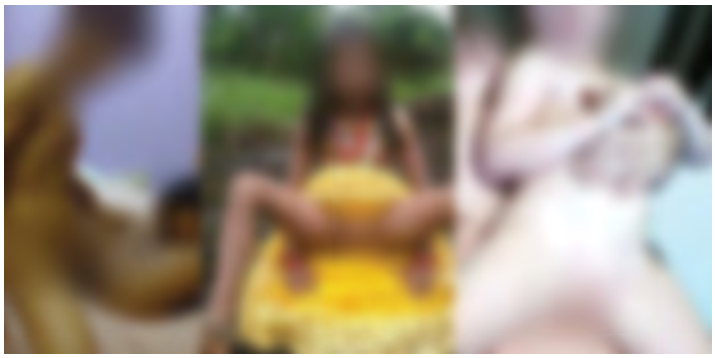
The third seller the investigator contacted was a person with the ID "SELLER" from the same "Girls and Boys Chatting" group to join other CSAM private Telegram channels for a fee of ₹100. These private Telegram channels allowed the admin to admit and remove members by choice, and not be visible in the general search engine of Telegram.

The investigator made the first payment of ₹100 by transferring the money to the account registered on the same day through a PhonePe QR code. Upon payment, the investigator was given links to 6 explicit private Telegram Channels. On the same day, the investigator again got access to CSAM for ₹50. On making a second payment on the same QR code, 'SELLER' sent a link to the folder with "URL: https://t.me/+eSs8rhh7agNINmQ1" which contained explicit content of CSAM, including adults participating in intercourse with children and self-streaming by underage girls. Through this seller the investigator got access to six private channels having more than 2000 videos each.

The fourth seller was contacted when the investigator saw a post sent by 'Dada Seller' with username "@Dadaseller02" in another group named 'Chatting Girls and Boys'. This group had 40,368 members of which 528 members were online at that time. 'Dada Seller' offered to give access to his private channel through links upon payment. After negotiating, he agreed to provide access at ₹70 and sent a QR Code to make the payment. Upon payment, he gave access to the channel

named “Heart 4”. The link he provided contained pictures of girls from ages 4 to 10 years of age, videos of people having intercourse with children, oral sex, and self-streaming of underage girls. It also had videos of gang rape with victims. A total of 30 GB and access to one private channel with 3200 CSAM videos was received from this seller.

Here the investigator also came in contact with a fifth seller with the ID ‘innocent boy’ who was a regular advertiser on the group ‘Telegu Girls’. The seller advertised selling zip files of explicit material at a cost to be discussed via messages in private. The investigator paid the seller ₹50 through a PhonePe QR Code and received a zip file of size 1.81 GB under the name ‘CP 32 295videos. zip’ (the word “CP” is often seen to be used in Telegram groups for Child Pornography). The zip files did not open due to an error, and it was observed that many times, the sellers deliberately embed malware into zip files to corrupt the receiver’s system.



Screenshot 2- Images of CSAM available

After connecting with five sellers and spending a total of ₹530/- the investigator was able to purchase 32GB of CSAM that translated to over 9 hours of content. After observing how technology is enabling such a crime and the extent and magnitude of these criminal networks using this platform, the investigator brought the operation to a close and handed over the information as a formal complaint to the Cyber-Crime Police Station at CID, Hyderabad.

Key Findings and Observations:

1. Technology providing a favourable ecosystem for criminals to Operate: Telegram provides a very favourable environment for predators/paedophiles and criminals to communicate and engage in illegal transactions for the purposes of buying or selling of CSAM.
2. Technology as an enabler: The following features in this technology acts as an enabler for such criminal activities:
    a) Ease to create a fake account - No identification verification is required to create an account on this app. The only prerequisite is a phone number that can be acquired by any means.
    b) Seamless advertising - Any content can be advertised on a private channel without any checks and balances including those for CSAM.

c) End to end encryption - Private messaging options with end-to-end encryption to carry out any transactions to purchase or sell. The encryption settings allow the admin and owner to prevent taking screenshots and copying links essentially preventing any collection of evidence.

d) Self-destruct feature - The self-destruct feature allows sellers to time-bound their messages which disappear without a trace.

e) Upload high volumes of data - The platform allows the sender to upload high volumes of data on third-party platforms like "www.mega.io" onto a zip file with time-bound access to its content post that would show as an error. Third-party cloud-based storage platforms such as "Mega" offer space of 5 GB to 20 GB free of cost.

f) No option to flag illegal content - The platform has no mechanism for any user to flag any illegal content or activity.

3. Payment gateway as an enabler: Payment Gateways such as PhonePe and Paytm have been instrumental in providing QR generation access to such sellers to distribute CSAM at nominal rates with ease.

4. CSAM content and its implications:

a) Easy access on surface web: The perception that CSAM is only available on the Darknet turns out to be just a myth. Such apps have provided easy access to such content on the surface web.

b) Normalized criminal behaviour: The volume of members in private groups investigated with over 70,000 members in two groups is indicative of the huge number of human beings who are sourcing such illegal content and selling them. In one instance, the seller explained the delay in sending CSAM because he was attending a Tuition Class due to which he could not send the content immediately. This raises several concerns about the age of these sellers who are engaging in such criminal activities with impunity.

c) Nominal rates: The ease and affordability of huge CSAM for a mere ₹50/-, which is less than a dollar, indicates the volume of such content that is available and easily accessible for all. A total of ₹530/- which is less than 6$ was paid to purchase 32 GB of CSAM from five sellers.

d) Profile of the children: Children between the ages of 3 to 12 years were featured in the CSAM with over 50 percent of them from India. Some videos also featured children as young as 1 year old. The children apparently belonged to all economic strata and significant numbers of videos were shot/recorded in what appears as a normal middle income group raising deep concerns about safety of children in all settings including the home and school.

e) Self-generated videos: 30 percent of the videos were self-generated by children themselves, raising several questions on the circumstances in which children as young as 6-7 years old have been groomed or coerced to create such exploitative content

f) Nameless victims, faceless perpetrators: The thousands of children sexually exploited on camera indicate the increased sexual violence on children which is unreported allowing the perpetrators to move with impunity.

Outcome of Investigation:

A complaint was lodged with the Director General of Police, Telangana State, presenting all the evidence to take legal action against all the accused i.e., Telegram for deliberately enabling/ facilitating the circulation and selling of CSAM on their platform, the persons who have supplied the CSAM, and the Payment gateways for enabling the accused to make the transaction to trade the prohibited content on the internet. The complaint was lodged as FIR. No. 3/2023 of CID Telangana.

Details of Accused:

1. Telegram for allowing the circulation and trading of CSAM on their platform
2. The 5 individuals who sold CSAM on Telegram
3. The Payment gateways Paytm and PhonePe

Charges pressed: U/S Section 13 of POCSO; Sections 66A, 66E, 67,67A 67B and 72 of the Information Technology Act as well as Rules 3 and 4 of the Information Technology (Intermediaries Guidelines) Rules, 2011.

Current status:

a) Notice has been given to Telegram U/s 91 CrPC seeking the required details of the users who traded the CSAM. Response still waited.

b) Notices have been served U/s 91 CrPC to payment gateways such as Paytm and PhonePe seeking the details of the information required for investigation. The payment gateways provided the details of the users of UPI accounts, their linked bank accounts, and other details as requested by the CID.

c) One of the accused with Telegram ID, 'Innocent boy', has been arrested, and the mobile phone used for trading CSAM with the investigator has been seized and sent for forensic analysis. The investigation is ongoing.

6.3.2 VALIDATION INVESTIGATION II: TRAFFICKING FOR COMMERCIAL SEXUAL EXPLOITATION VIA SDUKO.COM - A DATING SITE

Period of Investigation: 10 January 2024 - 17 January 2024

Intelligence Gathering: Instances shared by the global experts pointed to the increasing use by perpetrators of the use of ASWs to post profiles of forced/coerced victims advertising sexual services falsely portraying them as consenting. This camouflaging of victims among consenting

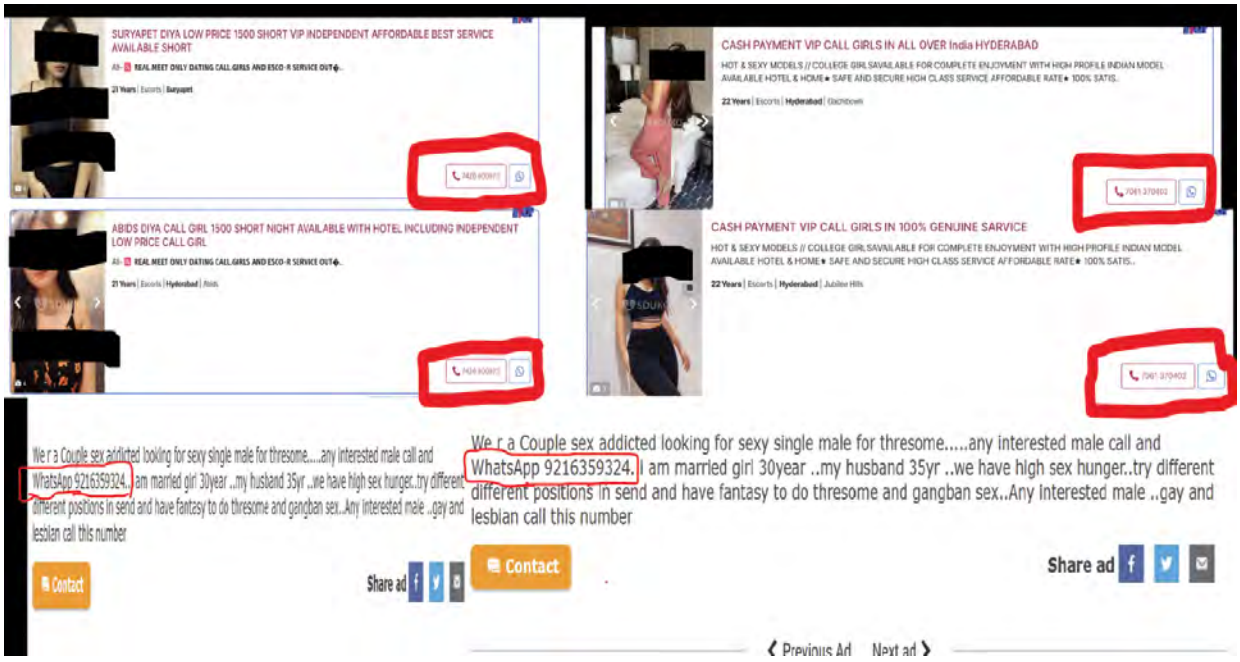
sex workers has allowed offenders to considerably expand their reach using online advertising as compared to street-based activities.

Prajwala's own experience of interacting with rescued victims whose services were advertised on 'Locanto' website reveals grooming and coercion in most cases. These victims now removed from sex slavery and recovering at the organization's safe homes have shared heartrending tales of cheating and betrayal that culminated into sextortion and sexual exploitation. Several such victims in their interactions cited 'Sduko Dating Network', a dating website, as the most accessible platform to seek underage girls.

With this credible information, the investigator sought to check out the veracity of this information.

The Investigation: As the first step, the investigator registered on the site with a nominal amount of ₹141/- that is less than two dollars with a dummy photograph. On browsing, it was found that users need not register, and only those who want to advertise need to register. The registration took less than 5 minutes.

To ascertain how the services were offered, the investigator through web surfing the pages found several individuals posting pictures of women/girls offering sexual services in different parts of India. Narrowing the search, the investigator started looking for what is available in Hyderabad and found that a person had posted an advertisement offering sexual services of girls and women of various ages. The mobile number of the advertiser was listed as +917878378875 and the URL of the advertisement was given as: https://in.sduko.com/escorts/hyderabad/gachibowli/hyd-2000-unlimited-short-all-type-certified-genuine-girls-available-now-in1mpqil5/



Screenshot 3: Advertisement of sexual services with the same phone number

In the web pages of the URL, the perpetrator had posted pictures of ladies and girls of different age groups, offering them for sexual pleasure at a cost. All the advertisements were linked to the same mobile number, and for further details the perpetrator asked that he be contacted on the above mobile number.

Screenshot 4: Advertisement of 16 year old underage girl for sexual services

On payment the investigator received a text message from the perpetrator that the girl was ready to be picked up. Person X then sent the location of 'Hotel Cent', near pillar No. 1201, Collectorate, 6-1-1063/c. Hyderabad to receive the girl.

Maintaining ethical and legal standards, the investigator at this stage contacted the AHTU, Hyderabad, seeking assistance to rescue the victim. The police team joined the investigator to take the operation forward.

The investigator then communicated with Person X and asked him to show the minor girl before the final payment could be made. Person X insisted on prior payment before the girl would be shown, and sent another mobile number +918854889964, which was linked to a Paytm UPI account.

On the repeated insistence of the investigator, Person X connected to a female voice, presumably the voice of the minor girl, who also insisted on prior payment of ₹6000/-. As the investigator stood firm on his request to see the girl before the payment was made, the person got abusive and started threatening the investigator that he would publicise the investigator's number as a middleman offering adult services and who was indulging in sex trafficking. He also threatened to not only harm his family, but also implicate him in a rape case or child trafficking case if the payment was not made. At this stage, it was concluded that this could be a case of financial fraud by extortion, the investigation was brought to a close.

Key Findings and Observations:

1. Dating sites acting as conduits for commercial sexual exploitation: Sduko dating network and other escort service websites are essentially for selling sexual services apparently by consenting adults. The same sites also provide access to individuals willing to provide underage minors which shows that there is a potential risk of sex trafficking using these sites.
2. Online brothel keeping and pimping: The advertisement of several 'women' with the same mobile number as the contact point is indicative of a single point of control, similar to what is seen in physical brothels and presence of mediators/pimps for soliciting sexual services which is illegal under Sec 3,4, 5 of ITPA, 1986.
3. Dating site as an enabler:
    a) Easy registration: The site provides easy registration options enabling fake profiles giving anonymity to conduct any activity related to selling sexual services.
    b) No Alerts when illegal services were sought: When the investigator was explicitly seeking for an underage girl no pop-ups or any other alerts were received indicating that it was an illegal search, which indicates the possibility of using the platform for commercial sexual exploitation on a regular basis especially for underage minors.
    c) Risk of Cyber frauds: As faced by the investigator and also described by several users on 'Quora',[69] these sites are a breeding ground for cyber frauds who use the easy registration means to advertise sexual services attracting paedophiles, and after gaining access to the phone number and other details of the user, indulge in extortion by means of blackmail. The usage of mule accounts for such fraudulent activities is also a potential means used, making it difficult for any investigation.
    d) Missing safeguarding mechanism: The site provides no means to report an alleged case of commercial sexual exploitation either of an adult or a child. Further, the site does not provide any alerts when illegal requests are made.
4. Commercial sexual exploitation: This case was that of a potential cyber fraud, but this does not rule out the possibility of advertising coerced adults and underage minors for sale of sexual services as seen and observed on Locanto website.

Outcome of Investigation: Crime No: FIR. No. 4/2024 of CID Telangana

Based on the contents of the complaint, CID Telangana registered a criminal case vide Crime Number 4/2024, and the case is under investigation.

Details of Accused: The online dating website SDUKO.COM, the person who uploaded the details of a minor girl for sexual services, and the account holder to whom the money has been transferred.

Charges pressed: Sec. 370(1), 366 (A), 372, 373 of IPC, R/w 511 IPC and sec. 506 IPC, Sec. 5 of Immoral Traffic (Prevention Act) and Sec. 67 and 67 (B) of the Information Technology Act and Sec. 14 and 15 of the POCSO Act 2012.

69 Online knowledge sharing platform where users can ask and answer questions on any topic

Current Status: Notices served U/S 91 CrPC to the website: www.sudko.com, the UPI service provider, the Mobile network service providers, and bankers seeking required information for investigation.

6.3.3 VALIDATION INVESTIGATION III: TRAFFICKING FOR ORGAN TRADE VIA TELEGRAM - AN INSTANT MESSAGING APP

Period of Investigation: From 5 December 2023 - 9 December 2023

About Organ Trade: Organ trafficking, a lucrative global illicit trade, is often a lesser discussed form of human trafficking. However, organ trafficking holds a critical place with transnational organized crime groups due to high demand and relatively low rate of law enforcement.

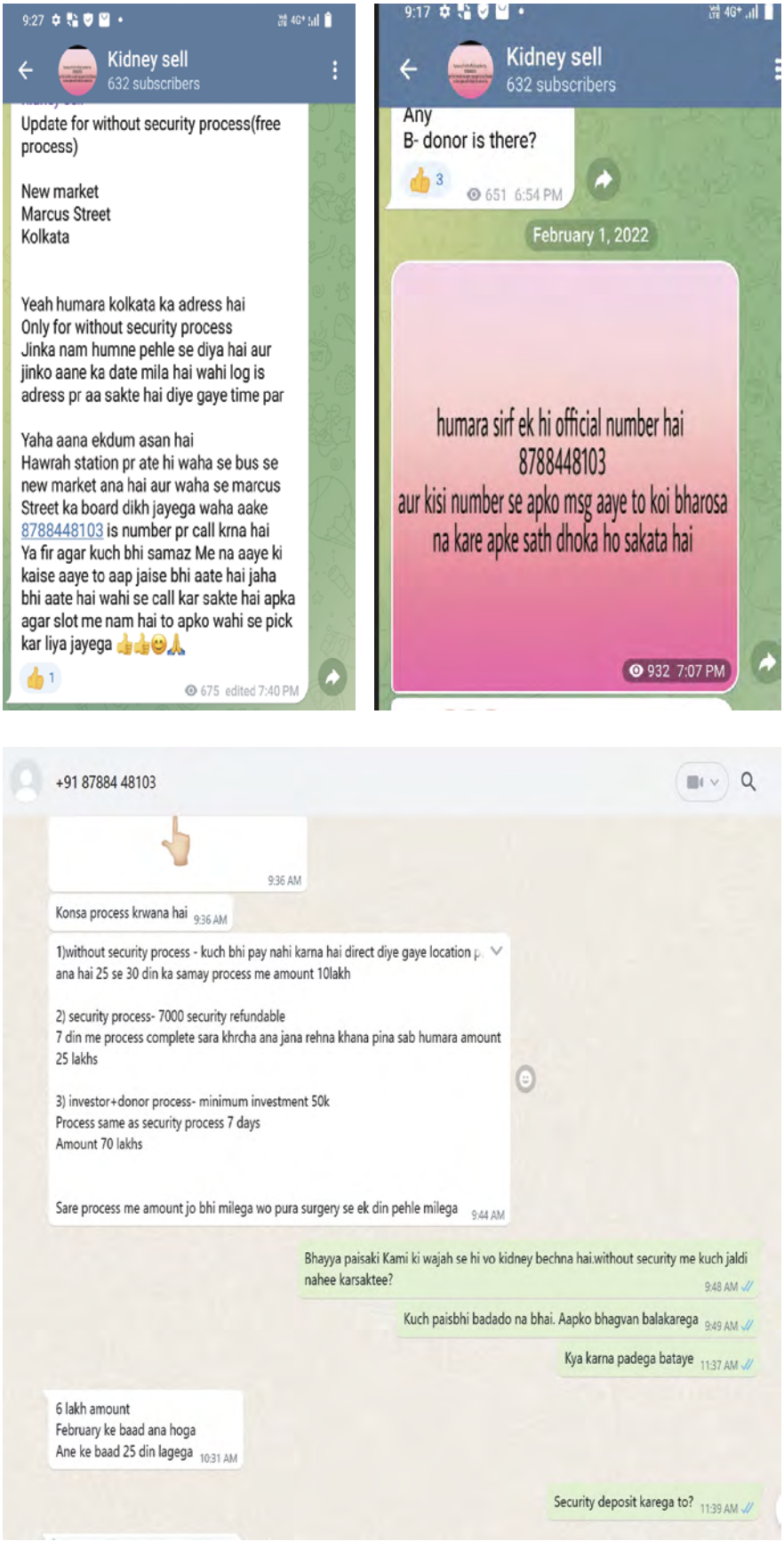
In 2023, the National Organ and Tissue Transplant Organisation (NOTTO), under the Union Ministry of Health and Family Welfare, ordered a probe into reports linking a renowned hospital in New Delhi, to a "cash for kidneys racket" involving Myanmar nationals. The allegations surfaced in a report by UK daily *The Telegraph* that stated "desperate young villagers" from Myanmar were paid to donate their kidneys to rich patients from Myanmar at a Delhi Hospital.

In India, the organ transplantation law permits donations from "near relatives" like siblings, parents, or spouses. Additionally, altruistic donations from friends and distant relatives are allowed, but strict measures are in place to verify that the motivation is driven by care rather than financial gain. These legal provisions aim to safeguard the poor and vulnerable from potential exploitation. Over the years, various news reports have pointed to poor people being allegedly lured by gangs operating social media groups to sell their organs for easy money. Recent media reports point to a probe ordered by the National Human Rights Commission into organ trafficking rackets operating in Haryana and Rajasthan[70]. The validation investigation was triggered by recent media reports of organ trade which indicated the involvement of cyber technology.

Intelligence Gathering: The investigator first searched social media for an entry into the organ sale groups. Facebook and Instagram pages, which had advertised organ sales, were contacted with no conclusive results. Repeated reference to the Telegram had been made on a few Facebook pages that had advertised organ transplant. Hence the Telegram app was identified to investigate organ trafficking.

The Investigation: The investigator signed up on Telegram with a pseudonym *Anindhit* by using a mobile number and posed as a potential seller of a kidney to make money. He searched on the Telegram and found a group with the name of 'Kidney Sell' that had 562 members. The investigator sent a request to admit him into the group, and was accepted by the admin. The investigator joined the group and was thus able to see the messages posted by the admin in the group. The investigator noted that only the admin could post messages on the group. The admin kept posting several advertisements offering payment in exchange for kidneys to interested donors and offered three schemes for kidney donors through his messages.

70 Human rights body NHRC sends notice to chief secretaries of Rajasthan, Haryana over organ transplant racket - India Today



Screenshot 5: Advertisement of kidney sale on Telegram

Scheme 1: Without any deposit

In this scheme, the donor did not have to make any deposit as all the expenditure would be borne by the receiver.

Waiting time for a donor: 25 to 30 days.

Payment offered: ₹10,00,000/-

Scheme 2: With a refundable deposit

To enrol in this scheme, the donor had to send a refundable deposit of ₹7,000/-. The entire expenditure including accommodation and travel expenses would be borne by the donors.

Duration of process: Completed within 7 days

Payment offered: ₹25,00,000/-

Scheme 3: Investor + donor process

The donor must invest a minimum of ₹50,000/-.

Payment offered: ₹70,00,000/-

A new flat will be provided as accommodation to the donors, with pictures and address of "New Market, Marcus Street Kolkata" accommodation attached.

Duration of process: 7 days.

The admin had posted his mobile number and asked to be contacted through WhatsApp for further communication The admin also posted some "thank you" messages purported to have been posted by the successful donors acknowledging the money received for donating their kidney, and these were screenshots from Facebook or Instagram accounts. When the investigator tried to contact these accounts, he could not make contact as they were private accounts.

Responding to his offer, the investigator introduced himself as a friend of a person in dire financial need who was willing to sell his kidney immediately and thus opted for Scheme 2. The admin asked the investigator to deposit ₹7000/- as per Scheme 2 and sent the QR code for initiating payment.

The investigator paid ₹100 to verify the account by scanning the QR Code.

After the initial payment was made, the admin asked the investigator to pay the remaining amount, and also provide a copy of donor's Aadhar Card and his passport-size photograph to start the process within 2 days. Since the investigator could not provide these details, he was blocked by the Admin. The investigation could not be taken forward due to ethical considerations of making a huge payment.

Key Findings and Observations:

1. Criminal trade of organs: Social media platforms such as Facebook and Instagram are being used for advertising organ trade which is illegal in India. Encrypted messaging apps, such as Telegram, are being blatantly used for advertising and making the first contact for these criminal transactions.
2. Attractive Advertising: The private channel option of Telegram provides extensive options to advertise criminal activities such as organ trade as an attractive scheme and follows the regular marketing gimmick of 'customer satisfaction' to further such criminal activity.
3. Cyber Technology as an enabler:
    a) Violation of the law of the land: Even though organ sales are illegal, social media platforms have not restricted pages that advertise organ sales. Platforms, such as Telegram, provide anonymous space through its private channels to advertise and initiate the first contact, and messaging apps such as WhatsApp are used to complete the transaction.
    b) One-sided communication: Telegram provides an option to the 'admin' to be the only communicating point barring any other member to post anything.
    c) Multiple usage of technology: Several online platforms are used in combination to facilitate an organized crime such as organ trafficking with traffickers using loopholes in all platforms to evade detection. Social media platforms such as Facebook are used to advertise and attract customers. Instant messaging apps like Telegram are used to roll out the schemes and WhatsApp is employed for actual communication.
4. Payment Gateways as Enablers: In this case, PhonePe has been instrumental in QR Code generation and providing access to criminals for receiving payments for illegal trade with ease.

Outcome of Investigation: Based on the contents of the complaint, CID Telangana has registered a criminal case vide Crime Number 3/2024, and the case is under investigation.

Details of Accused: Administrator/Owner of Group "Kidney Sell" of Telegram.

Charges pressed: U/S 18 and 19 of Transplantation of Human Organs Act-1994 and Sec. 370 (1) R/w 511 IPC and Section 66 – D of the Information Technology Act.

Current status:

1. As part of the investigation, CID Telangana has issued notices to Telegram, WhatsApp, PhonePe and Yes Bank Ltd to provide the required information for the investigation.
2. The accused has been identified. A team of CID officers led by the Investigating officer of the case apprehended the accused at his residence on 14 March 2024, and brought him to CID HQs, Hyderabad. His confessional statement has been recorded wherein he confessed that he was an Engineering dropout and working in a telecom. As he needed money for personal requirements,

two years back, he saw an advertisement in a group of Telegram, offering ₹10,00,000/- to kidney donors. Intending to sell his kidney to meet his financial needs he communicated with the moderator of the group and on his demand, he paid ₹16,000/- as registration charges. After receiving money, the moderator blocked him. While he did not lodge a police complaint, he got the idea to trap and cheat other donors in a similar manner. Thereafter he created the group on Telegram and started posting messages offering money to intended kidney sellers/ donors and cheated several people. The accused was produced before the concerned court on 15 March 2024, but the Court refused to take him on remand as the offenses are punishable with imprisonment of less than seven years. As such a notice U/s 41 (a) CrPC has been served on him to be present before the IO or the Court whenever required for investigation and trial.

6.4 Conclusion

The three validation investigations have given a clear insight on how cyber technology is playing an enabling role in facilitating many crimes including that of human trafficking. Easily accessible content related to child sexually abusive material available rampantly on surface web, advertisement for underage minors for sexual exploitation and blatant organ trade are some of the worst forms of crimes that are seamlessly committed using cyber technology. The involvement of multiple layers of perpetrators efficiently concealing the real players has made it cumbersome to crack the crime with investigating agencies reaching a dead end with some primary level of perpetrators being apprehended who could either be a former victim or just a cyber fraud. The accountability of the technological firms to prioritise user safety leans more towards providing free access to criminal intentions and less to safeguarding human lives.

Chapter

07

Commercial Sexual Exploitation

Chapter 7

Commercial Sexual Exploitation

7.1 Understanding Commercial Sexual Exploitation (CSE)

In an endeavour to get deeper understanding on the various facets of cyber enabled human trafficking the research adopted several methods and one of them was focus group discussion with police officers. Across the regions one particular purpose came out as a common trend and that was CSE. Several examples of CSE were given which were facilitated through cyber technology. This resonates with the insights gained from the global context. This chapter looks at this purpose more closely.

CSE traditionally refers to a range of exploitative activities involving the coercion or manipulation of individuals into engaging in sexual acts for financial gain.[71] Historically, CSE has been primarily associated with activities such as prostitution,[72] sex trafficking,[73] pornography production and distribution, sex tourism,[74] and online exploitation.[75] These forms of exploitation have been observed across various settings, including street corners, brothels, online platforms, and destinations known for sex tourism.

Within the traditional understanding of CSE, the causes have often been linked to factors such as poverty, gender inequality, migration, lack of education, substance abuse, and societal attitudes towards prostitution. Vulnerable populations, including women, children, migrants, and LGBTQ+ individuals, have been disproportionately affected by CSE.

The impact of CSE has been profound, resulting in physical, psychological, and social consequences for individuals and communities. Victims of CSE have experienced trauma, stigma, and a range of health risks, including HIV/AIDS and other sexually transmitted infections.[76]

---

71 Global Fund to End Modern Slavery.. About commercial sexual exploitation. Retrieved from https://gfems.org/modern-slavery/issues/about-commercial-sexual-exploitation/

72 Potterat, J. J., Rothenberg, R. B., Muth, S. Q., Darrow, W. W., & Phillips-Plummer, L. (2001). Pathways to prostitution: The chronology of sexual and drug abuse milestones. Journal of Sex, 35(4), 333–340.

73 Administration for Children and Families.. Human trafficking [Fact sheet]. Retrieved from https://www.acf.hhs.gov/otip/fact-sheet/resource/fshumantrafficking

74 Carolin, L. (2015). Sex trafficking in the tourism industry. Journal of Tourism &Amp; Hospitality, 04(04). https://doi.org/10.4172/2167-0269.1000166

75 Council of Europe. Online trafficking in human beings Retrieved from https://www.coe.int/en/web/cyberviolence/trafficking-facilitated-by-ict

76 United Nations Development Programme. (2012). Sex work and the law in Asia and the Pacific. Retrieved from https://www.undp.org/sites/g/files/zskgke326/files/publications/HIV-2012-SexWorkAndLaw.pdf

Additionally, CSE perpetuates gender-based violence, reinforces harmful stereotypes, and undermines human rights, contributing to broader societal harms.

Despite its prevalence, comprehensive research on this intersection of technology and exploitation is lacking. During the Focused Group Discussions (FGDs) conducted across fifteen states with Anti-Human Trafficking Officers and Cyber-Crime Officers this gap was explored by understanding the dynamics of CSE within the digital landscape. The discussions provided valuable insights into identifying trends and patterns of cyber usage for CSE.

7.2 Commercial Sexual Exploitation And CEHT

Our interactions with officers indicated a significant shift in what was the traditionally known CSE as a result of the integration of cyber elements. Some of the main patterns that emerged from their inputs:

- **Radical Shift in Exploitation Landscape**: Our findings revealed that integrating cyber elements into traditional CSE sparked a substantial transformation, resulting in a noticeable change in the way these crimes are carried out. Cyber-enabled CSE capitalizes on the anonymity, accessibility, and interconnectedness of the digital domain to facilitate crimes with unparalleled efficiency and global reach. Unlike traditional forms of exploitation, cyber-enabled CSE surpasses conventional barriers, empowering traffickers to effortlessly connect with hundreds of individuals worldwide with minimal digital exertion.
- **Increased Vulnerability**: In terms of vulnerability, a notable increase was observed in the number of potential victims in CSE due to cyber-enabled methods. Regardless of education, class, or caste, anyone using technology is vulnerable. CEHT does not discriminate, and can target emotionally vulnerable individuals from any background, highlighting the pervasive nature of this form of exploitation.
- **Exploitation through Digital Platforms**: A key finding reveals that traffickers, in addition to traditional methods, now exploit various digital platforms for different purposes, illustrating the versatility of cyber-enabled exploitation. Social media platforms such as Facebook and Instagram are commonly used for initial contact with potential victims, while instant messaging services such as WhatsApp and Telegram serve as preferred channels for further communication. Furthermore, pornography websites and applications accessed through VPNs play a significant role in cyber-enabled CSE, enabling traffickers to produce, distribute, and monetize explicit material involving victims of sexual exploitation.
- **Permanent Trauma/Inescapable Impact of Cyber-Sexual Exploitation Content**: One of the major findings was linked to the victims and the trauma they are subjected to when cyber technology is used for the purpose of trafficking. Unlike the traditional forms of human trafficking, the digital footprint created during instances of cyber-sexual exploitation remains permanent, haunting victims indefinitely. This enduring presence of harmful content renders emotional closure a daunting prospect, as the fear of its circulation and reemergence persists throughout the victim's life.

- **Invisibility of Primary Perpetrators**: Within the digital realm, our study revealed that perpetrators can manipulate innocent identities for financial transactions or communication, complicating investigations significantly. The time-intensive nature of these inquiries may inadvertently cause further victimization for innocent individuals whose SIM cards or bank accounts were utilized, prolonging their exposure to potential harm far beyond traditional investigative methods.

7.3 Forms of CSE within CEHT

An effort was made to understand the various forms of CSE facilitated by CEHT. Interactions with officers revealed that all forms of CSE previously committed physically have only accelerated with the usage of cyber technology.

7.3.1 Prostitution: Inputs from officers show that traffickers have expanded the scope of identifying potential victims through the use of cyber technology. Most officers cited social media platforms such as Facebook and Instagram as the most common places to identify victims. During the interactions with officers from Telangana, Locanto, a popular job site, was extensively mentioned as a space for soliciting and advertising for CSE. Several cases of CSE in Telangana have been identified through this site. During discussions with officers in Telangana, two cases involving victims of loan-app-coercion into prostitution were brought to light. In the first instance, two female victims were coerced into providing escort services at hotels after being unable to repay their loans, as the loan application gained unauthorized access to their personal contact details which was used to blackmail them into submission. In the second case, a male victim took out an instant loan from a fraudulent loan application and upon failing to repay it, his family, including his wife, received morphed videos of him via WhatsApp. Around the same time, his wife began receiving fraudulent job offers promising advance salaries via SMS. Faced with desperate circumstances, the wife accepted the advance that made her a victim trapped in prostitution. Subsequently, the victim was rescued from a hotel in Telangana.[77] This method of CSE differs significantly from traditional HT, in that it leverages digital platforms to reach a wider audience and conduct transactions discreetly, minimizing the risk of detection by law enforcement.

7.3.2 Pornography: Input from officers indicates that the production, distribution, and sale of pornographic material, often coercing victims into participating in explicit content creation or sharing, constitute a major aspect of CEHT. They stated that the traffickers are utilizing technology including popular pornography websites, streaming platforms like Hamster, and messaging apps such as Telegram to exploit victims for financial gain. Additionally, sextortion is frequently employed as a means of intimidating and coercing individuals to remain in exploitative situations, exacerbating the vulnerability of victims. In discussions with officers from Gujarat, it was revealed that traffickers from the region coerced a victim into performing sexual acts on camera via a live streaming pornographic platform.[78] This represents a departure from traditional HT, as traffickers can profit from the exploitation of victims remotely and anonymously, without the need for physical transportation or face-to-face interactions.

77 Telangana FGD on CEHT, Conducted on November 7, 2023, in Hyderabad.

78 Gujarat FGD on CEHT, Conducted on February 14, 2024, in Gandhinagar.

7.3.3 Sexual Exploitation: Many officers also shared that perpetrators utilize social media platforms such as Instagram and Facebook to groom, manipulate, and sexually exploit victims. They described victims being coerced into engaging in sexual activities through live streaming, sextortion, or other forms of online coercion. Officers from Punjab shared instances where perpetrators posed as romantic interests on Facebook, establishing relationships with victims before coercing them into engaging in sexual activities on camera. The recorded material was then circulated on platforms like Telegram. This form of exploitation diverges from traditional HT as it capitalizes on the accessibility of digital platforms to target and groom individuals into their exploitation, regardless of their physical location.

7.3.4 Distribution of CSAM: The officers further highlighted that traffickers are now utilizing online platforms and messaging apps like WhatsApp and Telegram to distribute CSAM, perpetuating the abuse of children by sharing explicit images and videos. They explained that the traffickers are utilizing encrypted messaging apps and VPNs to evade detection and law enforcement efforts. Officers from Telangana shared that traffickers in the region had created private groups on Telegram to share CSAM with other offenders for a nominal fee. This method contrasts with traditional HT, as traffickers can disseminate CSAM globally with minimal risk of detection, exploiting vulnerable children without the need for physical contact.

7.3.4.1 Child Victims as creators of CSAM: The officers highlighted that online predators often target children who may be addicted to online games that are freemium[79] and are compelled to purchase to seek advanced features. They exploit this vulnerability by offering in-game gifts or incentives to gain trust, to establish a connection with the minor victim. Once the connection is established, they use it to groom the victim into committing crimes such as generating CSAM material of minors known to them.

Officers shared an instance where a 16-year-old gamer victim while playing Fortnite, was promised a high-calibre gun by a predator in exchange for personal details like the victim's name, age, and city. When the victim received a less valuable 'shotgun', the predator asked him for his mobile number in exchange. The predator, under username "Bazookaboy", started speaking to the victim on Telegram. After establishing trust through frequent conversations, the predator messaged the victim again during gameplay, once again offering the high calibre ammunition. This time the predator asked for nude pictures of girls known to the victim in exchange for the promised gun as a pre-condition. The victim in this case realized the danger and blocked the predator.

In another instance shared, a 12-year-old child addicted to online games was heavily in debt as he had to purchase credits to progress and was being threatened by the predator of dire consequence. He was then coerced to self-generate CSAM content and also take videos of his friends.

79 Freemium is a combination of words "free" and ''premium" and refers to a business model that offers basic features of a product or service to users at no cost and charges a premium for advanced features.

7.3.5 Forced Marriages:

Officers also described the current misuse of matrimonial portals and social media platforms by the traffickers in facilitating forced marriages, coercing individuals into marriage against their will for exploitation. They highlighted that victims are being trafficked domestically or internationally for forced marriages, enduring physical, sexual, and emotional abuse. Officers from Madhya Pradesh disclosed instances where traffickers posed as potential spouses on matrimonial websites, deceiving victims into marriage before exploiting them for sexual purposes.[80]

7.4 Insights on Exploitative Technology Usage in Human Trafficking

The pervasive use of cyber technologies in human trafficking was discussed in great detail in all discussions. Officers provided detailed insights into how traffickers exploit digital platforms and applications to perpetrate their illicit activities. The officers identified two distinct kinds of cyber technology being utilized by traffickers. Below, we present a thorough presentation of their inputs:

7.4.1 Regulated Platforms: Facilitating Broad Communication

The Officers highlighted the extensive use of regulated social media platforms such as Facebook, Instagram, and Twitter, alongside matrimonial portals like Shaadi.com and Jeevansathi.com, by traffickers to identify and groom potential victims. Officers from Maharashtra disclosed the use of matrimonial websites such as Shaadi.com by traffickers to extract and profile existing images uploaded by victims, specifically targeting "young widows and divorcees" as potential victims.[81] Additionally, officers from Rajasthan described the usage of multiple fake profiles by traffickers on Facebook and Instagram, to recruit and groom female victims from various age groups.[82] According to the officers, traffickers use these platforms because they offer a wide reach, enabling communication with a vast audience. They explained that despite being regulated, these platforms remain open and accessible to everyone, providing traffickers with broad channels for profiling and establishing communication with victims for the purpose of exploitation.

7.4.2 Unregulated Platforms: Enabling Personalized Exploitation

Additionally, officers revealed information on the exploitation of closed, personalized platforms for unregulated interaction. As per their insights, gaming applications such as PUBG, FreeFire, and Ludo, alongside encrypted messaging apps like WhatsApp and Telegram, were identified as unconventional yet potent platforms for exploitation. Officers from Odisha revealed cases where traffickers utilized WhatsApp to communicate with clients nationwide, sharing profiles of victims for CSE.[83] Similarly, officers from Andhra Pradesh highlighted instances of the traffickers exploiting gaming apps like PUBG to establish contact with minors and groom them through in-app chat functionalities.[84] According to the officers, traffickers exploit these platforms to establish direct contact

80 Madhya Pradesh FGD on CEHT, Conducted on January 5, 2024, in Bhopal.

81 Maharashtra FGD on CEHT, Conducted on February 15, 2024, in Mumbai.

82 Rajasthan FGD on CEHT, Conducted on February 12, 2024, in Jaipur.

83 Odisha FGD on CEHT, Conducted on December 26, 2023, in Bhubaneswar.

84 Andhra Pradesh FGD on CEHT, Conducted on January 03, 2024, in Vijayawada.

with potential victims, frequently resorting to grooming tactics and offering rewards. They emphasized that the absence of regulation in these spaces allow traffickers to engage in one-to-one communication, enabling covert exploitation on a more personalized level. This is cited as one of the primary reasons for traffickers' preference for these platforms, as highlighted by the officers.

7.5 Profile of Victims

During the FGDs efforts were made to understand the diverse demographics of victims involved in cyber-enabled CSEC. Insights shared by officers highlighted that unlike traditional human trafficking scenarios the spectrum of victims in cyber-enabled CSE is broad and is inclusive of all social and economic strata. Below, we present a comprehensive summary of the findings gleaned from these discussions.

7.5.1 Diverse Demographic: Through their input officers highlighted that victims of cyber-enabled CSEC represent a diverse demographic encompassing individuals from various backgrounds. The insights shared underscored the broad spectrum of victims involved in cyber-enabled CSE, dispelling the notion that exploitation exclusively targets specific vulnerable populations.

7.5.2 Largely Female, Children, and Adults: According to the inputs provided by officers, victims of cyber-enabled CSE largely include female individuals who could be both children and adults. They stated that traffickers exploit gender-based vulnerabilities and societal norms to coerce and manipulate female victims into exploitative situations. Officers from Jharkhand narrated incidents of minor female victims who were profiled on Facebook by traffickers, were lured under promises of marriage, and sold in cities like New Delhi.[85] Additionally, officers from Meghalaya narrated incidents of adult female victims being targeted on common work-related WhatsApp groups, lured with lucrative job promises as beauticians, and ultimately sold for CSE in massage Parlors[86] in Delhi.

7.5.3 Rural and Urban: Officers further highlighted that victims of cyber-enabled CSE come from both rural and urban areas, indicating that traffickers target vulnerabilities across different geographic regions. They stated that economic disparities and limited access to resources contribute to vulnerabilities in rural areas, while in urban centers, traffickers' prey on not just individuals seeking employment or better prospects, but also those who are emotionally vulnerable. Officers from Rajasthan reported cases of rural girls being targeted by traffickers, abducted, and sold off as domestic workers in cities where they would be sexually abused.[87] They stated in such instances, the local spotter and city-based trafficker would communicate entirely over WhatsApp. Similarly, officers in Kerala shared that female victims from cities were being lured by job opportunities in Oman via WhatsApp groups and ultimately forced into CSE in Oman.[88]

---

85 Jharkhand FGD on CEHT, Conducted on January 8, 2024, in Ranchi.

86 Meghalaya FGD on CEHT, Conducted on February 7, 2024, in Shillong.

87 Rajasthan FGD on CEHT, Conducted on February 12, 2024, in Jaipur.

88 Kerala FGD on CEHT, Conducted on December 28, 2023, in Thiruvananthapuram.

7.5.4 Socioeconomic Diversity: Officers emphasized that victims of cyber-enabled CSE also hail from diverse socioeconomic backgrounds, ranging from the affluent to the marginalized. They explained that traffickers exploit financial vulnerabilities and aspirations for a luxurious life to coerce individuals into exploitative situations, irrespective of their socioeconomic status. Officers in Assam shared an incident where a minor victim from a remote village was contacted by the trafficker via WhatsApp directly, then lured under promises of a better life, and finally asked to meet at a particular location and was then sexually abused.[89] Officers from West Bengal reported a case where a woman from an affluent family was spotted by a trafficker on Facebook and was lured with acting assignments to later be sexually exploited.[90]

7.5.5 Diversity in Educational Backgrounds: Officers noted that victims of cyber-enabled CSE span the spectrum of educational attainment, from highly educated job seekers to those with no formal education. They stated that traffickers exploit educational vulnerabilities and aspirations for high-paying jobs to manipulate victims into exploitative situations. Officers from Kerala reported a case where international students were being targeted by fraudulent educational agencies only to be sent abroad and be forced into CSE.[91] Officers from Odisha stated cases where uneducated, rural women were being spotted by local spotters and sold off to placement agencies who would force the victims into sexually exploitative domestic work while advertising them on their websites.[92]

7.5.6 Emotional Vulnerability**:** The officers also highlighted emotional vulnerability as a common thread among victims. They explained that traffickers exploit feelings of loneliness, isolation, or emotional turmoil to manipulate and coerce victims into exploitative situations, using technology as a primary tool for grooming and establishing initial contact. Officers from West Bengal narrated an incident where a lonely married female victim was spotted and lured on the promise of companionship, only to be sold off in Pune.[93]

7.5.7 Marital Status: Marital status was identified as another factor contributing to victims' vulnerability to exploitation. Officers reported that unmarried, widowed, divorced, and even married women are vulnerable to manipulation and coercion by traffickers, who exploit vulnerabilities related to relationship dynamics, familial responsibilities, and societal expectations. Officers in Telangana stated incidents of traffickers using matrimonial portals like Shaadi.com to filter "divorced/unmarried" women, to meet them in person, and force them into CSE. They also reported that victims who had been abused would also be forced to create profiles on such portals to find customers for their services.[94]

7.5.8 Technology Usage: Officers pointed out that victims of cyber-enabled CSEC are individuals who actively engage with technology, including social media platforms, gaming apps, messaging apps, and online payment portals. They highlighted that traffickers exploit these

89 Assam FGD on CEHT, Conducted on January 18, 2024, in Guwahati.

90 West Bengal FGD on CEHT, Conducted on January 24, 2024, in Kolkata.

91 Kerala FGD on CEHT, Conducted on December 28, 2023, in Thiruvananthapuram.

92 Odisha FGD on CEHT, Conducted on December 26, 2023, in Bhubaneswar.

93 West Bengal FGD on CEHT, Conducted on January 24, 2024, in Kolkata.

94 Telangana FGD on CEHT, Conducted on November 7, 2023, in Hyderabad.

platforms to identify, groom, and exploit victims, irrespective of their technological literacy or proficiency. Officers in Punjab narrated an incident where a female victim from Haryana was targeted on Facebook by a trafficker, asked to travel to Punjab with intentions to force her into CSE.[95]

7.5.9 High Number of Victims: Officers emphasized that unlike traditional human trafficking scenarios, where victims often belong to specific vulnerable groups and are limited, the number of victims in cyber-enabled CSEC is significantly higher. They reasoned that the ability to spot and recruit victims simultaneously across cyber platforms contributes to this high number, with the profile of victims being inclusive of virtually anyone and everyone. Officers from Goa narrated a case where an organized network of traffickers, used high numbers of trafficked female victims to threaten male customers with fake rape charges, to extort money.[96]

7.6 Criminal Enterprise/Players of Crime

Based on inputs from officers, efforts were made to discern the various players and criminal enterprises involved in cyber-enabled CSE. Interactions with officers unveiled a complex network of actors, each fulfilling distinct roles within the criminal enterprise. Below is a detailed overview of the players involved in perpetrating cyber-enabled CSE:

7.6.1 Metropolitan Agents: Inputs from officers revealed that metropolitan agents function as intermediaries or facilitators within trafficking networks, especially in urban centers like Delhi and Mumbai. They stated that these agents hold a pivotal position in recruiting, transporting, and exploiting victims for financial profit, often masquerading as legitimate businesses or services. Officers from Jharkhand reported that local spotters from rural areas within the region would coordinate with agents in Delhi to send victims to the city, who would be sold into prostitution.[97] They further explained that the metropolitan agents are typically individuals who were originally from a local area but have since established residence in the city.

7.6.2 Young men and minor boys: Inputs from officers revealed that traffickers frequently recruit young men and minor boys to engage in multiple aspects of cyber-enabled CSE. They stated that these individuals are incentivized to participate in activities such as recruitment, grooming, and distributing explicit material on social media platforms. Furthermore, officers noted that traffickers target vulnerable individuals within the social circles or online communities of these young men and boys. Officers from Madhya Pradesh reported that a group of young men had been recruited by the main trafficker, to spot and lure girls on Facebook based on their "modern clothes" and transport them to Tamil Nadu.[98]

95 Punjab FGD on CEHT, Conducted on February 5, 2024, in Chandigarh.

96 Goa FGD on CEHT, Conducted on January 30, 2024, in Goa.

97 Jharkhand FGD on CEHT, Conducted on January 8, 2024, in Ranchi.

98 Madhya Pradesh FGD on CEHT, Conducted on January 5, 2024, in Bhopal.

7.6.3 Family Members: Inputs from officers revealed that family members play a complicit role in cases of familial exploitation or forced marriages, aiding in the facilitation of trafficking activities. They stated that these individuals exploit their relationships with victims to coerce, manipulate, or profit from their exploitation, thereby perpetuating the cycle of abuse within familial or domestic settings. Officers from Gujarat reported a case where a married female victim was forced by her husband and in-laws to live-stream sexual activities on a pornographic site, for financial gain.[99]

7.6.4 Organized Groups: Many officers shared that organized criminal groups play a significant role in the production, distribution, and sale of pornography, especially when it involves recording explicit material. They stated that these groups operate covert networks to exploit and profit from the sexual exploitation of victims, utilizing technology to create and disseminate pornographic content for commercial gain. Officers from Kerala narrated a case where a victim was spotted by a local agent who had connections in Saudi Arabia. The victim was forced to marry a Saudi national and later coerced through blackmail to recruit 17 girls who were taken to Oman to be sold to buyers who had selected their profiles. All communications in between the organized group and the buyers were done entirely through WhatsApp, and it was properly planned with divided responsibilities.[100]

7.6.5 Proxy Identities: Inputs from officers highlighted that proxy identities, often crafted using real SIM cards and mule accounts, are extensively used by organized criminal groups in various CSE activities, including contacting and communicating with the victim. These fake identities act as a cover, hiding the true perpetrators while allowing them to exploit and profit from the sexual exploitation of victims. According to the officers, the use of fake profiles based on genuine SIM cards and mule accounts make it harder to track and catch those involved in these acts of exploitation. Officers from Meghalaya narrated a case where a 20-year-old woman from a rural area of East Garo Hills was promised a lucrative job opportunity by individuals posing as a recruitment agency. The perpetrators had created a fake job website and had registered their numbers on SIM cards that were purchased from someone else, and their proxy numbers appeared as a legitimate company. She was asked to travel to Gurugram for the job and coordinated her travel with these proxy numbers. Upon reaching Gurugram, she was gang raped by the members of this organized criminal group. During the investigation, officers encountered difficulty in tracking down the real perpetrators because the SIM card numbers registered led back to the person from whom the numbers were originally purchased.[101]

7.7 Integration of Traditional and Technological Movement in Criminal Activities

An attempt was made to perceive the different modes of movement involved in cyber-enabled CSE. Insights shared by officers during the FGDs emphasized the dynamic nature of exploitation in the digital realm, wherein both perpetrators and victims navigate through various stages and

99 Gujarat FGD on CEHT, Conducted on February 14, 2024, in Gandhinagar.

100 Kerala FGD on CEHT, Conducted on December 28, 2023, in Thiruvananthapuram.

101 Meghalaya FGD on CEHT, Conducted on February 7, 2024, in Shillong.

modes of movement, each presenting unique challenges and complexities. Below, we present a comprehensive overview of the types of movement identified, as relayed by officers.

7.7.1 Digital Continuum

Officers stated that within the Digital Continuum mode, the entire exploitation process unfolds within the digital realm. They explained that perpetrators initiate and maintain contact with potential victims exclusively through online platforms such as social media, gaming apps, or matrimonial portals, allowing exploitation to occur without any physical interaction. Interactions with officers from Punjab revealed a gaming app called FreeFire that was used to establish contact with a vulnerable adolescent. The victim was groomed and coerced entirely through the in-game messaging and was never met in person.[102]

7.7.2 Virtual to Physical Transition

Officers provided insights into the Virtual to Physical Transition mode, explaining it as a transition from virtual interactions to real-world encounters. They elaborated that traffickers initially establish contact, then groom victims through online channels, and eventually arrange face-to-face meetings for exploitation in offline settings. Interactions with officers from Bihar revealed that after grooming a minor victim on Facebook, a trafficker in Bihar arranged for a physical meeting at a predetermined location in Muzaffarpur, where the victim was sold into prostitution.[103]

7.7.3 Cycle of Digital-Physical-Digital

Officers shared insights into the Cycle of Digital-Physical-Digital mode, stating that in this cyclical movement pattern, traffickers engage in a continuous loop of online and offline interactions throughout the exploitation process. They explained that the traffickers begin by initiating contact and grooming victims online, then progress to arranging offline meetings for exploitation, and finally revert to online platforms for sustained communication and coordination. Interactions with officers from West Bengal revealed that a trafficker-initiated contact with the victim through Facebook for a job, he then arranged an offline meeting for purposes of exploitation and its filming, and then continued to blackmail the victim through WhatsApp to demand subsequent exploitation activities.[104]

7.8 Legal Challenges

Based on our FGDs with investigating officers, valuable insights have been garnered regarding the significant legal challenges within this domain. This section offers an in-depth examination of the legal obstacles, as reported by officers, exposing the complexities encountered in addressing cyber-enabled CSE within the legal framework.

7.8.1 Difficulties in Tracing Perpetrators: Officers emphasized the daunting task of tracing perpetrators across digital platforms, where traffickers exploit encrypted communication

102 Punjab FGD on CEHT, Conducted on February 5, 2024, in Chandigarh.

103 Bihar FGD on CEHT, Conducted on February 1, 2024, in Patna.

104 West Bengal FGD on CEHT, Conducted on January 24, 2024, in Kolkata.

channels and anonymization techniques to evade detection. The global nature of the internet further complicates efforts to apprehend individuals involved in cyber-enabled CSE. This difficulty in tracing perpetrators severely hampers law enforcement's ability to identify and apprehend those responsible for these heinous crimes.

7.8.2 Interdepartmental Hurdles: The bureaucratic inefficiencies and jurisdictional disputes posed a serious obstacle that impeded seamless cooperation and information sharing among relevant stakeholders. These interdepartmental hurdles create silos within the legal system, leading to fragmented efforts and hinder the comprehensive response required to address this complex issue.

7.8.3 Jurisdictional Hurdles (Interstate/International): Jurisdictional challenges were identified as a significant obstacle in prosecuting cases of cyber-enabled CSE that span multiple jurisdictions. Differences in legal frameworks, jurisdictional boundaries, and international laws further complicate efforts to prosecute perpetrators operating across state or national borders. Moreover, the lack of international cooperation and extradition treaties exacerbates these jurisdictional hurdles, impeding law enforcement's ability to hold perpetrators accountable across geographical boundaries.

7.8.4 Victims' Cooperation: Officers highlighted barriers such as fear of retaliation from traffickers, trauma resulting from exploitation, and psychological manipulation as factors that impede victims' willingness to come forward and participate in legal proceedings. This reluctance to cooperate severely hampers investigation and prosecution efforts, prolonging the cycle of exploitation and injustice.

7.8.5 Compliance/Cooperation by Technology Companies: Officers emphasized the critical role of technology companies in combating cyber-enabled CSE but also communicated the challenges in ensuring their compliance and cooperation. Issues related to data privacy, encryption, and corporate responsibility pose significant hurdles for law enforcement's access to crucial digital evidence. Without the cooperation of technology companies, law enforcement's ability to disrupt trafficking networks operating through online platforms is severely limited.

7.8.6 Lack of Technical Capacities and Technical Knowledge: Officers highlighted the lack of technical capacities and expertise required to effectively investigate and prosecute cases of the rapidly evolving cyber-enabled CSE. They stated the lack of adequate training, resources, and technical expertise severely hampers law enforcement's ability to navigate digital evidence, trace perpetrators, and effectively combat cyber-enabled CSE.

7.8.7 Delay in Court Proceedings: Challenges such as prolonged court proceedings in cases of cyber-enabled CSE due to the complexity of digital evidence, jurisdictional issues, and bureaucratic delays within the legal system, was expressed. The admissibility and authenticity of digital evidence require meticulous verification and authentication, leading to delays in court proceedings. Additionally, jurisdictional disputes and interdepartmental hurdles further contribute to delays in legal proceedings, prolonging the wait for justice for victims and survivors.

7.8.8 Lack of Understanding of the Law: The complexities of cyber-crime legislation, data privacy laws, and international treaties governing online exploitation were cited as a serious knowledge gap. The lack of awareness, training, and understanding of these laws among key stakeholders severely impedes effective investigation, prosecution, and adjudication of cyber-enabled CSE cases.

7.9 Cases from Focus Group Discussions: Realities of Cyber-Enabled CSE

During the FGDs, several cases emerged that vividly depicted the complexities of cyber-enabled CSE. These cases offer a glimpse into the challenges and legal hurdles associated with addressing this form of exploitation. Here, we present a selection of representative cases identified by the officers themselves as instances of CEHT for CSE.

The cases cover various aspects of cyber-enabled CSE, including cross-border trafficking, the use of matrimonial portals to profile victims, exploitation through gaming apps for generating CSAM, baiting lonely married women via social media, and trapping victims through fake job advertisements to produce pornography. Each case serves to illustrate the diverse means and tactics employed by perpetrators to ensnare unsuspecting individuals into CSE.

CASE 1: TELANGANA[105]

Case Title: Cross Border Human Trafficking through WhatsApp and Botim

Case Lead: Bureau of Immigration (BOI), Hyderabad.

Investigated by: Anti-Human Trafficking Unit (AHTU), Cyberabad

Profile of Victim: Young, poor, Indian women from Coastal areas of Andhra Pradesh

Details of the alleged accused: Middle- aged Telugu woman and Malayali Muslim man

Details of the Case:

- BOI, Hyderabad gave the passport details and mobile number of a suspect woman who was frequently making regular international trips to Qatar, Bahrain, and Singapore, on tourist visas.
- AHTU, Cyberabad collected CDR of mobile numbers provided by BOI. The analysis of CDR found that the same mobile number was being used from different handsets. A total of 14 mule Sim cards and 5 mobile sets were traced to the accused female transporter.
- The AHTU further analyzed CDR data to establish the payment gateway and the transactions made through the mobile number.
- Upon analyzing the payment details, they found multiple bookings made in 5-star hotel bookings in Mumbai and Delhi.

105 Telangana FGD on CEHT, Conducted on November 7, 2023, in Hyderabad.

- On analyzing call logs, they were able to trace a frequently contacted Malayali[106] man. The accused Malayali man was in contact with the international traffickers through Botim; he was facilitating the accused female transporter to transport the victims to foreign countries via WhatsApp.
- **Modus Operandi (MO)**: AHTU found that the suspected woman would meet the victims at Hyderabad Airport, details of who were not known to her prior to the meeting. The accused female transporter would communicate with the victims only through WhatsApp on a group chat. She would accompany the victims through the entire journey till the specific foreign country. The travel and facilitation was done under the guidance of the accused Malayali man through WhatsApp.
- The AHTU found that the suspected woman would harbour the trafficked victims in a specific location which would be located close to the drop off hotels. On being instructed to drop off the victims, the accused female transporter would deliver the victim to traffickers for the specific country.

Outcome: Based on information from the BOI, the AHTU launched an operation aimed at targeting the primary suspect, "Anitha," in human trafficking. As a result of this operation, three individuals were arrested as per FIR no. 1126/2023, registered at Madhapur P.S, Cyberabad.

- During interrogation, they confessed that Anitha was the mastermind behind a local prostitution ring, enticing victims with job opportunities and coercing them into prostitution by arranging clients for them. Additionally, the arrested persons revealed that Anitha had a well-organized network for sending victims abroad for prostitution. Presently, Anitha, along with two other accused persons, are evading arrest, and the police are actively pursuing leads to arrest them.

Usage of Technology/Cyber:

- Botim – Was used by the accused Malayali man to communicate with international traffickers in Middle Eastern countries. The application is a messenger application.
- WhatsApp - Used for coordination and communication between the accused Malayali man and accused female transporter
- UPI - Was used by the accused Malayali man to pay the accused female transporter. And also used by the accused female transporter to pay for booking in 5-star hotels located in Delhi and Mumbai

CASE 2: TELANGANA[107]

Case Title: Trafficking victims through Shaadi.com for CSE

Investigated by: AHTU, Hyderabad

106 Malayalam is a language spoken in the state of Kerala, a coastal state in South India. People speaking Malayalam are called "Malayali"

107 Telangana FGD on CEHT, Conducted on November 7, 2023, in Hyderabad.

Status of case: Under Investigation

Details of Complainant: Suo moto by Hyderabad Commissionerate

Profile of Victim: Young widows and divorcees

In an ongoing operation by AHTU, Hyderabad, the following patterns have emerged:

- Accused used Matrimonial websites like Shaadi.com to profile existing images which have been uploaded by the victims. They identify 'young widows and divorcees' as potential targets.
- After profiling such victims, they establish communication through these websites and enquire about their financial status. Upon exchanging mobile numbers, the accused meets the victim in person, to lure them with money. The victim is then trafficked for CSE.
- It was also found that previously exploited victims had also made their profiles on the website to advertise their services.

Usage of Technology/Cyber:

Matrimonial Websites like Shaadi.com - Used for spotting victims and establishing communication

CASE 3: PUNJAB[108]

Case Title: Truth or Dare App Used to Coerce Minor Victim and publish CSAM on Instagram

Status of Case: Under investigation

Police Station: Cyber-Crime branch, Punjab Police Station

Details of Complainant: Family of victim

Profile of Victim: Minor girl from Punjab

Details of the alleged accused: Minor boy from Punjab

Details of the Case:

- A minor girl (victim) met a minor boy (accused) on Truth or Dare game app, they spoke during the game.
- Eventually, the accused dared the victim to take off her clothes on video call. The victim complied with the dare and stripped as part of the game.
- The accused screen recorded the victim without her consent. He then used the recorded video to coerce the victim into sharing more videos with him.
- When the victim refused to comply with his demands, he uploaded the video on Instagram using a fake account. The victim's family filed a complaint with Cyber cell.
- Police are working to establish evidence linking the accused to the upload, as there are discrepancies in the IP addresses associated with the account.

108 Punjab FGD on CEHT, Conducted on February 5, 2024, in Chandigarh.

Usage of Technology/Cyber:

- Truth or Dare gaming app- Used for spotting the victim and establishing first contact
- Instagram - Used to upload video of the victim through a fake account

CASE 4: WEST BENGAL[109]

Case Title: Married woman lured through Facebook for CSE

Status of Case: Under Investigation

Police Station: Murshidabad

Details of Complainant: Husband of woman

Profile of Victim: A married woman whose husband was overseas for work.

Details of the alleged accused: Organized group of men who befriend lonely women on social media and trap them for human trafficking.

Details of the Case:

- The victim was befriended by a person (accused) on Facebook and further spoke on Instagram. After developing a romantic relationship, she was persuaded to elope with the promise of marriage.
- The victim travelled to Sealdah Railways Station and was accompanied by another man (co-accused) who helped her onboard and travelled to meet the main accused.
- Upon the complaint of the victim's husband, the police used CDR and tracked the victim in Pune.
- The police rescued the victim from a brothel in Pune. However, the accused has not been caught yet.

Note: West Bengal Police has observed several cases of similar nature, where girls of varying profiles, including college students are spotted on social media, groomed to leave their homes on the promise of marriage, but they end up in brothels in various cities in Maharashtra, Delhi, Meerut, etc.

Usage of Technology / Cyber:

- Facebook - Used for spotting the victim
- Instagram - Used for establishing communication

109 West Bengal FGD on CEHT, Conducted on January 24, 2024, in Kolkata.

CASE 5: WEST BENGAL[110]

Case Title: Online fake job advertisement to lure women into CSE and shooting pornography

Status of Case: Under Trial

Crime no: 90/2020

Police Station: Bidhannagar Cyber-Crime

Details of Complainant: Victim's father

Profile of Victim: Under-graduate student around 18 years old

Details of the alleged accused: Organized group of men

Details of the Case:

- The Victim from a small village in Bangaon, came across an advertisement on Facebook calling for young girls for film acting roles. She contacted the job ad on the given contact number, via WhatsApp.
- She was called at an address for giving an audition. She was however sedated by a group of men and a video of the rape was shot and uploaded on xhamster.com. (porn website)
- Eventually, the villagers came to know of such a video and set fire to her house in rage. The victim's father complained to the police regarding the incident.
- Police traced the WhatsApp number used by the victim during initial contact. The WhatsApp account of the accused was found to be deleted; however, the police were able to trace the IMEI number of the alleged device.
- Police tracked the accused persons in New Town, where, at the time of the raid, they were in the process of shooting another porn video with another sedated victim.
- The Police, through the process of investigation, found that the accused, the organized group, were repeat offenders who used such videos that were filmed of the victim, to blackmail and further exploit them to make more porn films.

Usage of Technology / Cyber:

- Facebook - Used for posting fake job advertisements
- WhatsApp - Used for establishing communication
- Xhamster (porn website)- Used for uploading videos of the abused.

CASE 6: PUNJAB[111]

Case Title: Trapping minor girl on Ludo gaming app for potential CSE

Profile of Victim: A minor girl student of class 9th -10th (13-14 years), from Bahadurgarh

110 West Bengal FGD on CEHT, Conducted on January 24, 2024, in Kolkata.

111 Punjab FGD on CEHT, Conducted on February 5, 2024, in Chandigarh.

Details of the alleged accused: A boy/man likely based in Amritsar

Details of the Case:

- The victim from Bahadurgarh met the accused through a Ludo game, who initiated contact between them via its chat feature.
- Over the course of 5-6 months, communication between the victim and the accused extended to Instagram, eventually leading to a romantic attachment on the part of the victim.
- The accused groomed the victim to come and meet him, so the victim left her home and started her travel to Amritsar with the intention of meeting at the Golden Temple.
- During her bus journey, the conductor observed peculiarities in the victim's behaviour, noticing that she was wearing her school ID and carrying her school bag. Sensing something suspicious, the conductor engaged the victim in conversation, probing into her reasons for traveling and her destination.
- Concerned for her safety, the conductor further inquired about the victim's family contacts and ensured she was cared for during the journey. Upon learning of the situation, the conductor reached out to the accused, who denied any association with the victim.
- Taking swift action, the conductor contacted the victim's father by the number provided by the victim, who turned out to be an officer of Bahadurgarh Police. The victim's father had already initiated a search operation to locate his daughter across the city.
- With the assistance of the conductor, the victim's family located and rescued her from the situation.
- The local news agency conducted an interview with the conductor, highlighting his role in the rescue operation, and subsequently shared the recorded interview on Facebook for public awareness.

Usage of Technology/Cyber: A Gaming app (Ludo) to spot and establish contact

- Instagram for communication and grooming
- Facebook for spreading information regarding the crime

7.10 Analyzing Contrasts: CEHT vs. Traditional Human Trafficking (HT) for Commercial Sexual Exploitation (CSE)

Based on the inputs provided by the officers, a comprehensive comparison has been constructed to delineate the disparities between CEHT and traditional human trafficking for the purpose of Commercial Sexual Exploitation. The insights gleaned from the officers indicate a clear differentiation in the operations of CEHT and traditional HT, revealing their contrasting acts, means, and purposes.

Category	CEHT	Examples	Comparison with Traditional HT
Acts	Recruitment: Traffickers recruit victims through online platforms such as Facebook, Instagram, Snapchat, and dating apps.	Traffickers pose as potential romantic interests or offer false promises of employment on social media like Facebook largely remaining anonymous.	In traditional HT, recruitment typically entails physical methods like targeting vulnerable individuals in public spaces. The true identity of the traffickers is identifiable. Victims can physically recognize the chain of individuals involved, including the procurer/ recruiter, transporter, and others.
	Transportation/Transfer: Traffickers utilize messaging applications such as WhatsApp to coordinate meetings or facilitate virtual travel. In some instances, no physical transfer occurs; individuals are virtually connected to another location, for example, through live streaming.	A trafficker uses WhatsApp to arrange a virtual meeting between a potential victim and a client. Instead of physically moving the victim to the client's location, the trafficker sets up a live streaming session on Skype where the victim interacts with the client remotely.	Traditional HT often involves physical movement of victims across borders or within regions.
	Harbouring/Giving Shelter: Traffickers use online platforms like Telegram or encrypted messaging apps to harbor victims.	Traffickers maintain private online groups or forums where explicit material is shared.	Harbouring victims in traditional HT may involve physical locations such as brothels or private residences.
	Receipt: Traffickers receive payment for sexual services through online transactions or crypto currencies. These transactions in many cases cannot be traced. The usage of fake accounts is also common.	Payment for CSE is facilitated through payment apps like Paytm or PhonePe which may end in a mule account. This makes it a challenge to trace the trafficker.	Receipt of payment in traditional HT may involve cash transactions or other forms of payment exchanged in physical settings, which makes the transaction traceable.

Means	Threat or Use of Force or Violence: Traffickers employ online intimidation tactics such as cyber bullying, blackmail, or issuing threats to coerce victims. These threats may involve sharing irreversible sexual content with permanent implications.	Online threats or cyber bullying on social media is used to coerce victims into compliance.	In traditional HT, physical force, violence, or intimidation are used to control victims.
	Abuse of Power/Position: Traffickers leverage their authority or influence on platforms like LinkedIn or professional networks to exploit victims. They may utilize readily available personal details and credentials to perpetrate humiliation on a larger scale, such as hacking phones and disseminating content to all contacts.	Promises of job opportunities or career advancement used to manipulate victims.	In traditional HT, abuse of power or position may occur when traffickers masquerade as employers or recruiters. Furthermore, abuse of power can manifest through relatives, family members, or spouses who exploit their positions of trust and vulnerability.
	False Promise: Traffickers entice victims by weaving elaborate narratives of false opportunities, promising employment, education, marriage, or romantic relationships. They construct convincing marketing frameworks, fabricate employment contract letters, and manipulate feedback from others to create an illusion of authenticity, thus luring their victims into their trap.	False promises made on platforms like Facebook or matrimonial apps like Shaadi.com with the added benefit of fake IDs.	Similar false promises may be made in traditional HT, often involving recruiters who exploit vulnerabilities. Identity of the trafficker may be easier to identify.

	Kidnapping and Abduction: In cases of online grooming leading to physical abduction, perpetrators ensure the victim's active participation by grooming them, making it challenging to discern the abduction. The victim becomes an initiator through grooming, minimizing physical coercion. Instead, emotional manipulation compels the victim to willingly reach the destination, blurring the lines between coercion and consent.	Grooming on platforms like gaming apps or online chat rooms.	In traditional HT, kidnapping and abduction are prevalent, typically involving overt physical force or coercion. Unlike CEHT, traditional cases often exhibit clear instances of physical coercion that are visibly apparent.
	Cheating/Deception/Fraud: Traffickers employ online deception or fraud tactics on platforms such as loan apps or job portals. This may involve various cyber-crimes, including economic offenses, perpetrated against the victim before they are trapped in the trafficking situation.	False job advertisements in FB, are used to lure victims into exploitative situations in different locations over India.	Deceptive practices to cheat the victim are carried out in person and the identity may be known to the victim in traditional HT.
Purpose	Prostitution: Victims are exploited for commercial sexual services, which are advertised and arranged online. Typically, adult sexual services sites and job sites are utilized for advertising. However, the actual provision of services often takes place discreetly in hotels.	Services are solicited, advertised, and arranged through online advertising platforms like Locanto.	In traditional HT, victims may be coerced into working in various establishments such as brothels, massage parlours, or on the streets. Additionally, traffickers may exploit victims in settings like hotels, resorts, beauty parlours, and spas.

	Sexual Exploitation/Sexual Abuse: Victims are subjected to sexual exploitation facilitated by messaging apps such as WhatsApp and Telegram. This exploitation may include activities like live streaming via platforms like Skype. Importantly, the exploitation can take place entirely online, encompassing activities like sex chats, without the victim needing to physically move.	Sexual exploitation is done by trapping female victims to perform sexual acts on instant messaging apps like WhatsApp which provide video call services. Such videos are screen recorded without consent and later used to blackmail the victim into performing more sexual acts.	Victims may be forced into pornography production or sold for sexual services in physical settings in traditional HT.
	Pornography Distribution: Traffickers exploit encrypted instant messaging platforms like Telegram to create, distribute, and trade pornographic material. Many victims may not even be aware that their content has been recorded and manipulated for such purposes.	Distribution of pornographic material involving victims at minimal prices is done by anonymous sellers on platforms such as Telegram. The volume of pornography is extremely high at minimal costs.	In traditional HT, the distribution of pornography may involve victims being coerced into producing explicit material for sale. The victim is typically aware that their content is being prepared and used for exploitation.
	Distribution of CSAM: Traffickers exploit social media and messaging apps to distribute CSAM, perpetuating the abuse of children. Children may be groomed through various means, including online games, to self-generate CSAM content.	Fake accounts are made to share explicit images and videos involving minors using WhatsApp or Telegram groups.	In traditional human trafficking, the distribution of CSAM may involve victims being coerced into producing explicit material involving minors for sale or distribution. There is no involvement of self-generation of such content by the victims.
	Forced Marriages: Victims, primarily educated women and girls with cyber knowledge, are coerced into marriages for the purpose of exploitation. They endure physical and emotional abuse as part of this exploitation.	Victims are lured by false promises of love or work on social media/matrimonial apps, and they move to a different location without any coercion. Here, no middle person is required to bait the bride or transport her.	In traditional HT, victims, often from impoverished and illiterate families, may be sold or coerced into marriages by local agents. These victims are frequently transported by a handler to facilitate the arrangement.

7.11 Conclusion

Based on the valuable insights gathered from discussions with Anti-Human Trafficking Officers and Cyber-Crime Officers across fifteen states, it is clear that CEHT has significantly changed how CSE works. These discussions helped us understand how technology has made exploitation more widespread and harmful. CEHT, as a borderless space, has provided a larger landscape for predators, going beyond the vulnerable/high-risk area approach attached to traditional human trafficking. The means to reach a vulnerable person has multiplied with the advent of digital platforms such as social media, job sites, dating sites, and matrimonial sites, expanding the avenues for exploitation.

The use of digital platforms, including social media, gaming apps, and encrypted messaging services, has made it easier for traffickers to find, groom, and exploit victims. This happens regardless of where they live or their social status. Cyber-enabled CSE affects people of all genders, ages, backgrounds, education levels, and marital statuses. This shows how widespread and common it is in today's society.

Traditionally, CSE included activities like prostitution, producing pornography, sexual abuse, sharing CSAM, and forced marriages. But with cyber technology, these practices have evolved, making it easier for traffickers to reach and exploit victims. The irreversible damage inflicted on victims, both physical and psychological, further underscore the severity of cyber-enabled exploitation. Grooming in adult cases often appears as consent, and the emotional manipulation of the victim deters reporting, exacerbating the challenges faced by law enforcement agencies.

There are many types of people involved in cyber-enabled CSE, like metropolitan agents, young men, family members, and organized criminals. They each have different roles in exploiting victims and using technology to make money. The mix of old and new ways of doing things in cyber-enabled CSE makes it harder to stop and catch the people responsible, presenting new challenges for law enforcement. Additionally, law enforcement faces significant challenges in combating cyber-enabled CSE, including difficulties in tracing perpetrators, obstacles in cooperation between departments, and jurisdictional issues.

The cases presented highlight the changing landscape of cyber-enabled CSE, demonstrating how technology can be used for exploitation. These stories show how anyone can be targeted, emphasizing the urgent need to address this issue as people of all ages and gender use social media and digital platforms.

Despite the significant legal challenges involved in combating cyber-enabled CSE, including difficulties in tracing perpetrators, obstacles in cooperation between departments, and jurisdictional issues, efforts must be intensified. Collaboration across disciplines, building capabilities, and advocating for policy changes are essential to tackle the complex aspects of cyber-enabled CSE fully. These actions are crucial for protecting victims, prosecuting perpetrators, and preventing future exploitation in today's digital age.

Chapter

08

Cyber-Enabled Illegal Adoption

Chapter 8

Cyber-Enabled Illegal Adoption

8.1 Introduction

Sale of infant children under the guise of adoption was reported across all the regions by officers during the focus group discussions. In some states like Gujarat an explicit example was given where cyber technology was used. During the course of global consultations, child trafficking for adoption in China was mentioned by some experts. As this purpose of trafficking is less discussed in the digital realm, an effort was made to understand this further.

Adoption rackets in India pose a widespread problem, transcending national borders and perpetuating exploitation on a global scale. According to the NCRB, a staggering number of children suffer from exploitation each year. In 2022 alone, children reported missing were 83,350, while 2,878 identified children were victims of human trafficking.[112] This alarming statistic highlights the vulnerability of children in India and emphasizes their susceptibility to various forms of exploitation, including adoption rackets.

At the core of these adoption rackets lies the systematic kidnapping and trading of infants. Traffickers forcibly take innocent children from their families, resulting in a grave infringement of their rights and dignity.

The mentality required for trading children reflects a calculated willingness to exploit vulnerabilities, manipulate familial bonds, and profit from the suffering of others. The end goals of these activities are diverse, ranging from organ trafficking and forced labor to illegal adoption and sexual exploitation. People traffic children for various purposes, using them as commodities in illegal trades or fraudulently presenting them for adoption to unsuspecting families.

In India, the adoption process is solely under the purview of Central Adoption Resource Agency (CARA), which is a statutory body under the Ministry of Women and Child Development. All adoption applications, whether through an NGO or an orphanage, must be processed through CARA.[113] An adoption is illegal if not registered with CARA. Sections 80 and 81 of the JJ Act, 2015, prohibit offering or receiving children outside the processes laid down under the Act as well as their sale and purchase. Such acts are punishable with three to five years in jail or one lakh fine.[114]

112 https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf

113 https://mphc.gov.in/PDF/JuvenileJustice/j3-060314.pdf

114 https://cara.wcd.gov.in/PDF/JJ%20act%202015.pdf

Socioeconomic factors, legal loopholes, and the exploitation of vulnerable populations contribute to the flourishing of adoption rackets in India. Economic disparities, social stigma surrounding adoption, and inadequate enforcement of regulations create an environment ripe for criminal exploitation.

In 2013, an online news report highlighted a disturbing case where a newborn Indian baby was sold to a businessperson for ₹800,000/- (approximately USD 9576) via Facebook, shedding light on one of the earliest instances of adoption racket through social media.[115] This case involved the baby being sold multiple times, starting with the infant's grandfather, who falsely claimed the child was stillborn, leading to subsequent sale to a nurse and then a hospital attendant, before finally being sold on Facebook.

The emergence of technology has introduced new dimensions to these illicit activities. Online forums, social media platforms, and encrypted communication channels facilitate the advertisement and brokering of children, enabling traffickers to operate with increased anonymity and efficiency. This digital landscape not only expands the reach of adoption rackets but also complicates efforts to track and prosecute perpetrators.

The repercussions of technology entering this illicit racket are profound, amplifying the scale and sophistication of exploitation while simultaneously challenging law enforcement agencies and advocacy organizations to adapt their strategies to combat CEHT crimes effectively.

In the subsequent sections of this chapter, we will delve into the emergence of cyber-enabled adoption rackets, exploring how technological advancements have reshaped and expanded these illicit practices. By examining case studies and analyzing the role of digital platforms, we aim to provide a comprehensive understanding of this evolving phenomenon. Furthermore, we will investigate the vulnerabilities exploited by cyber-enabled adoption rackets, the modus operandi of perpetrators, and the challenges faced by law enforcement agencies in combating these crimes. Through this exploration, we seek to unfold the complex interplay between technology and exploitation, ultimately empowering stakeholders to address and mitigate the risks posed by such rackets in India.

8.2 Understanding Traditional Adoption Rackets in India

Adoption rackets in India are executed through a meticulously planned strategy, systematically exploiting vulnerabilities at every step of the process. This crime emerges from a complex interplay of gender bias and economic vulnerability. Gender discrimination and the secondary status of a girl child in certain communities exacerbate the issue. In some regions, the birth of a girl child is still viewed as a burden, leading to scenarios where infants are killed rather than being cared for. The roots of the problem extend to historical practices like infanticide, with areas like Usilampatti in Tamil Nadu where the Kallar community, and several communities across the country, gained notoriety for committing female infanticide until the late nineties. Media reports reveal even today the prevalence of selling girl children persists, highlighting the deep-seated societal issues at play.

In this grim trade, there are primary sellers, mid-sellers, and end sellers, each playing a distinct

115 https://sg.news.yahoo.com/baby-sold-on-facebook-for-rs-8-lakh--found-in-delhi-104029997.html

role in the exploitation of innocent lives. The primary sellers, often parents facing economic hardship, initiate the transaction out of desperation. The mid-sellers, who facilitate the illegal trade through networks and connections, then exploit them. The end sellers, by purchasing infants, perpetuate the cycle of exploitation, defining the sinister purposes with their actions.

The primary sellers in adoption rackets are individuals and couples from marginalized backgrounds, often facing dire socioeconomic circumstances or gender bias that leave them vulnerable to exploitation. Many reside in impoverished conditions, struggling with financial instability, and limited prospects for employment. The prospect of earning a substantial sum through the sale of their baby can be appealing amidst such adversity, prompting some to consider this option as a means of financial relief and also as a harmless way to get rid of their baby especially a girl child.

Moreover, these sellers are often victims themselves, falling prey to coercion or manipulation by traffickers who exploit their vulnerabilities. Traffickers employ various tactics, including deception, threats, or promises of financial assistance, to compel individuals into selling their babies. In some cases, sellers are led to believe that they are making a temporary arrangement or that their child will be provided with better opportunities elsewhere.

At the other end of the spectrum are buyers, either an individual or a couple actively seeking to adopt a child/children for various reasons. While some genuinely aim to provide a loving home, others have motives that are more dubious. For instance, some buyers exploit the lax regulations surrounding international adoption, where infants can be acquired more easily. These buyers often belong to affluent backgrounds and may have the resources to navigate the complexities of international adoption procedures.[116] Additionally, infants may be bought specifically for organ harvesting purposes, with buyers often being individuals or organizations involved in illegal organ trafficking networks. Moreover, some buyers see adoption rackets as a means to obtain children at a lower cost compared to legal adoption processes. These buyers may be motivated by financial constraints or a desire for expedited adoption, regardless of the ethical implications.

Facilitating these transactions are the intermediaries, individuals who play a pivotal role in coordinating adoption rackets. These intermediaries, including traffickers and brokers, capitalize on the vulnerabilities of sellers and manipulate buyers to ensure the smooth execution of the transaction. Intermediaries involved in adoption rackets come from diverse backgrounds, ranging from organized crime syndicates to individuals with connections in the adoption industry. Their modus operandi typically involves identifying vulnerable sellers, often through networks of informants or online platforms, and exploiting their desperate situations. Intermediaries may use deceptive tactics, such as false promises of financial security or better opportunities for the child, to persuade sellers to part with their infants.

Once sellers are identified, intermediaries orchestrate the transaction, coordinating between buyers and sellers to finalize the deal. They may forge documents or manipulate legal procedures to create the illusion of legitimacy, ensuring that the adoption racket remains undetected. Additionally, intermediaries often maintain a network of contacts within the adoption industry, including lawyers, doctors, and orphanage staff, who may facilitate the illegal adoption process. The

116 https://frontline.thehindu.com/cover-story/article30204931.ece

role of intermediaries in adoption rackets is paramount, as they provide the necessary expertise and connections to navigate the complexities of the adoption process.

Regardless of the motivations behind adoption rackets, the consequences for vulnerable children are severe, affecting their physical, emotional, and psychological well-being. Exploited by sellers, traffickers, intermediaries, and buyers alike, these children are subjected to a cycle of exploitation and suffering. Physically, they may suffer from neglect, malnutrition, and lack of medical care. Emotionally, they experience feelings of loss, confusion, and abandonment, with long-lasting effects on their self-esteem and mental health. They are treated as commodities rather than human beings, deprived of their fundamental rights and dignity.

The prevalence of adoption rackets exposes the shortcomings within India's legal framework governing adoption and the high demand for adoption. Typically a couple going through the procedure laid down by CARA have to wait for at least 3-4 years to be able to meet a child to adopt. At any given point in time, there are a large number of parents waiting to adopt. This demand-driven market incentivizes exploitation and poses risks to the well-being of vulnerable children.

8.3 The Intersection of Technology and Illegal Adoption: Cyber-Enabled Adoption Rackets

On June 2, 2022, a renowned news portal reported that Vijayawada city police had apprehended two individuals masquerading as medical professionals. They were arrested for their purported involvement in a scheme to sell a three-day-old female infant through a WhatsApp group, with a price tag of ₹3 lakh. The message disseminated across the WhatsApp group detailed the specifications of the infant for sale: "Female baby. 3 kgs. 3 lakhs. Birth certificate comes with our own surname." Alongside the message were accompanying visuals, including a video and photographs displaying the newborn girl.[117]

The landscape of adoption frauds in India has undergone significant evolution with the integration of technology, a transformation exemplified by the emergence of Covid-19 adoption rackets during the global pandemic. Amidst the Covid-19 crisis, perpetrators exploited the vulnerabilities of the situation to orchestrate adoption frauds involving Covid-19 orphans.[118] Through online platforms like Facebook, Twitter, WhatsApp, and Telegram, these perpetrators advertised orphaned children. This insidious exploitation not only increased the trafficking and exploitation of innocent victims but also highlighted the changing dynamics of adoption frauds in the digital age.

The integration of technology has profoundly affected the traditional practice of adoption frauds in India, leading to their penetration and expansion across various facets of crime. From publicizing on various platforms to networking with other perpetrators, communication through encrypted platforms, online booking of movement, and online payment, technology plays a pivotal role in every aspect of crime, fuelling its proliferation and sophistication.

---

117 https://timesofindia.indiatimes.com/city/vijayawada/andhra-pradesh-vijayawada-quacks-try-to-sell-infant-on-whatsapp-for-rs-3-lakh-arrested/articleshow/91951941.cms

118 https://theprint.in/india/beware-of-traffickers-social-media-posts-seeking-adoption-for-Covid-orphans-raise-concern/658695/

Technology has fundamentally changed the landscape of adoption frauds, particularly in how they are published and promoted. Perpetrators now leverage popular social media platforms like Facebook and Twitter, as well as classified websites such as Sulekha.com and Justdial.com, along with instant messaging apps such as WhatsApp and Telegram. These platforms offer perpetrators a cloak of anonymity and access to a vast audience, simplifying their ability to connect with vulnerable individuals in search of adoption services.

Furthermore, technology facilitates networking among perpetrators, enabling the establishment of complex syndicates and networks involved in adoption frauds. Social media and instant messaging platforms serve as virtual meeting places where perpetrators exchange information, share strategies, and collaborate on illicit activities. These networks amplify the reach and impact of the adoption frauds, making it increasingly challenging law enforcement agencies to combat them effectively.

Communication through encrypted platforms adds another layer of complexity to the adoption frauds, allowing perpetrators to conduct their operations discreetly and securely. Encrypted messaging services offer end-to-end encryption, ensuring that communications remain private and inaccessible to authorities. This enables perpetrators to coordinate logistics, negotiate terms, and exchange sensitive information without fear of interception or surveillance. Further, using technology, online booking for movement gets easier, enabling perpetrators to arrange transportation for trafficked children with ease and efficiency. The easy accessibility of online platforms to book flights, trains, and other modes of transportation, provides perpetrators with the means to facilitate the movement of victims across geographical locations, evading detection, and law enforcement scrutiny.

Online payment mechanisms further streamline adoption frauds, enabling perpetrators to conduct financial transactions securely and anonymously. Digital payment platforms with UPI facilities and online banking services facilitate the transfer of funds between perpetrators and buyers, circumventing traditional banking channels and financial regulations.

8.3.1 Unveiling the Adoption Racket: Case Studies in Exploitation and Technological Facilitation

A. CASE STUDY 1 - Illegal Adoption via Sulekha.com

During the focus group discussion held in Gandhinagar, Gujarat, on February 14, 2023, the officers discussed a notable example of the convergence of traditional adoption methods with modern technology. This case, originating from Baroda, Gujarat, was documented in Crime number Part A. 11196030220618/2022 registered with the Shahid Gunj Police Station. It involved the orchestration of an online adoption fraud through the widely used classifieds website *Sulekha.com*.[119] Ms. B.B. Patel, the Principal Investigator (PI) of the Missing Cell, AHTU in Baroda City, mentioned this case during the discussion, albeit with unclear details. The investigator in the research team thereafter went in person to gather all the information directly from the PI.

The accused individuals involved in the crime were identified as Saurav Vishwanath Beri and his wife Soma, along with accomplices Pooja, Deepak, Priyanka, and Devki. The couple, Saurav and

119 Gujarat FGD on CEHT, Conducted on February 14, 2024, in Gandhinagar.

Soma, originally from West Bengal were residing in Baroda for about eight years, and had been unsuccessful in conceiving a child despite undergoing fertility treatments. Faced with the lengthy and expensive legal process of adoption, they resorted to exploring online avenues for acquiring a child.

Their journey into the world of illegal adoption began when Saurav came across an advertisement on the classified website Sulekha.com, posted by the "Krishna Child Adoption Centre". Through this advertisement, prospective adoptive parents were enticed with the prospect of adopting a child for a significant sum of money. Negotiations ensued over WhatsApp, culminating in an agreement to adopt a newborn baby girl for ₹2.5 lakhs.

The transaction was meticulously planned, with arrangements made for the delivery of the baby at Baroda Central Railway Station on September 4, 2022. However, law enforcement authorities, acting on a tip-off given by the lawyer contacted by the buyers for creation of Aadhar Cards, intercepted the perpetrators as they attempted to carry out the exchange. Pooja and Deepak were apprehended red-handed, along with the infant baby girl, who was merely six days old at the time.

Upon further investigation, it was revealed that Pooja and Deepak had previously been involved in similar illicit activities, having delivered a male infant baby for ₹8 lakhs in Surat just two months prior. The involvement of multiple individuals in the syndicate, including Priyanka and Devki, revealed the complex network of adoption rackets operating across the country.

The modus operandi employed by the perpetrators involved using online classifieds such as Sulekha.com to advertise, instant messaging apps to negotiate adoption transactions, and UPI for payments, exploiting the vulnerabilities of childless couples and birth parents alike.

Additionally, when adoption transactions are conducted illegally, the fate of the child becomes uncertain. Without mechanisms for follow-up and safeguarding, the child lacks a safety net. Legitimate adoption processes involve agencies like CARA, CWC, and District Child Protection Officer (DCPU), which serve as safeguards for the child's welfare. In the absence of such safeguards, the child may be left vulnerable to exploitation and unknown dangers.

Extended Examination of Case Study 1

Background of Buyers:

Saurav Vishwanath Beri and his wife Soma were desperate to adopt a child having failed to have their own biological children.

Victim Profiles:

The sellers in this case are individuals from marginalized backgrounds, facing economic hardship and social stigma. Birth parents like Mitthan Singh and Simla Rani, agricultural laborers from Punjab, already struggled to provide for their five children. Faced with ongoing financial pressure, they considered relinquishing their child via the adoption process as a means to alleviate their burden and secure a better future for their newly born child.

Role of Traffickers:

The traffickers in this case operated as intermediaries, facilitating the illicit adoption transactions between the sellers (birth parents) and the buyers (adoptive parents). Their role involved orchestrating the entire process, from identifying vulnerable birth parents to connecting them with prospective adoptive parents. The traffickers often preyed on individuals facing economic hardship and desperation, exploiting their vulnerabilities for monetary gain.

One of the key individuals involved in trafficking was Priyanka, who along with her mother Devaki, played a central role in procuring infants from remote villages. They maintained a network of contacts across India and orchestrated the acquisition of infants, particularly targeting male babies due to their higher demand. Priyanka and Devki coordinated the logistics of the adoption transactions, arranging for the transportation of infants to their intended destinations.

Additionally, Priyanka collaborated with other accomplices, such as Pooja and Deepak, who were responsible for delivering the infants to prospective adoptive parents. Pooja, a mother of five children herself, had previously engaged in surrogacy and adoption-related activities. She leveraged her connections and experience to facilitate the transfer of infants, ensuring smooth execution of the adoption transactions.

Deepak, on the other hand, was involved in the transportation of infants and acted as a liaison between the traffickers and the adoptive parents. Together, Priyanka, Devki, Pooja, Deepak, and other accomplices formed a well-organized syndicate, exploiting the vulnerabilities of birth parents and manipulating the adoption process for their financial gain.

Technological Facilitation:

Technology served as a crucial enabler in orchestrating the adoption racket, providing perpetrators with anonymity and reach. Perpetrators utilized online platforms such as Sulekha.com as a virtual marketplace for illegal adoption transactions. They posted advertisements displaying infants available for adoption, and communicated with prospective adoptive parents through digital channels.

Specifically, perpetrators leveraged WhatsApp for negotiating adoption terms and sharing photographs of infants with potential adoptive parents. The encrypted nature of WhatsApp allowed them to communicate discreetly and maintain anonymity, shielding their illegal activities from scrutiny.

Additionally, the adoption racket involved the use of UPI for making payments related to adoption transactions. This digital payment method provided a convenient and secure way for perpetrators to transfer funds without leaving a paper trail, further facilitating their illicit activities.

In addition to leveraging online platforms and encrypted communication channels, the perpetrators employed sophisticated tactics to evade arrest. They utilized mule mobile SIM cards and bank accounts to avoid detection, further complicating efforts by law enforcement to apprehend them.

The case has made evident the pervasive nature of adoption rackets and the challenges faced by law enforcement agencies in combating these crimes. It serves as a stark reminder of the urgent need for regulatory measures and collaborative efforts to safeguard the rights and well-being of vulnerable children caught in the web of exploitation.

B. CASE STUDY 2 - Facebook and Illegal sale of infants

On April 7, 2024, Bachpan Bachao Andolan (BBA) took a significant step in combating infant trafficking by collaborating with the CBI to conduct a series of raids. These raids successfully dismantled a network of infant traffickers operating across India, leading to the rescue of several infants. This operation exposed the grim reality of the prevalent illegal adoption practices in the country, particularly those facilitated by cyber techniques. The case study highlighted the pivotal role played by the NGO in initiating a lengthy investigation that resulted in the arrest of criminals engaged in illegal adoption practices.[120]

Background and Initiation of Investigation:

The investigation was sparked by a concerning complaint received by BBA regarding a child adoption agency suspected of engaging in the illegal sale of babies.

Undercover Operation and Collaboration with Authorities:

BBA's staff, acting as decoy customers, utilized Facebook as a platform to initiate conversations with the alleged perpetrators. These interactions, conducted over Facebook Messenger, provided valuable insights into the alleged illegal activities of the adoption agency. The evidence gathered was promptly shared with the CBI for further examination and action. Recognizing the importance of collaboration, the CBI recommended that BBA continue communication with the perpetrators to gather more evidence.

Surveillance, Communication, and Evidence Gathering:

The alleged perpetrators received WhatsApp calls from BBA's staff, posing as potential buyers interested in acquiring a baby to gather more actionable intelligence. This strategic move allowed for the collection of additional evidence, while continuous surveillance of the suspect's communications provided valuable insights into their operations.

Rescue Operation and Arrests:

The culmination of the investigation led to a meticulously coordinated rescue operation, conducted in collaboration with the CBI. This operation resulted in the successful rescue of four

120 https://www.hindustantimes.com/india-news/cbi-busts-network-of-traffickers-in-delhi-involved-in-buying-and-selling-infants-101712425941553.html

children and the subsequent arrests of seven suspects directly involved in illegal adoption practices.

Modus Operandi and Cyber Facilitation

The traffickers created a fake Facebook page that looked like a real adoption agency. People who wanted to adopt had to sign up by giving their basic details. However, this sign-up was just a trick to get more information for their illegal activities. They asked questions that seemed like they were checking if the users were real, but it was just to get more data.

After signing up, the traffickers used different tricks to attract people who wanted to adopt. They showed pictures and information about kids available for adoption, often using images of foreign kids to make it seem more appealing. They would start chatting through Messenger, then move to WhatsApp. Then they would ask for a small payment to help with the adoption process.

They also kept up the act by posting updates about the kids' growth and development on the Facebook page. They would say these updates came from adoptive parents to make it seem legitimate. However, it turned out these claims were fake, just to trick people who wanted to adopt. These deceptive practices were meticulously analyzed and exposed by BBA's investigative efforts.

This case study highlights how technology fuels illegal adoption rackets and emphasizes the importance of proactive investigation in tackling such crimes. By using advanced surveillance methods and collaborating with law enforcement, NGOs such as BBA can aid in dismantling these networks. However, it also underlines the ongoing challenges posed by cyber enabled adoption rackets.

8.4 Examining the Legal Framework and Exploitative Loopholes in Adoption Practices in India

The legal framework governing adoption in India is carefully designed to ensure the protection, welfare, and best interests of children throughout the adoption process. Rooted in the JJ Act, 2015, and its accompanying Adoption Regulations, 2017, formulated by the CARA, these legislative instruments provide a comprehensive framework for ethical adoption practices while prioritizing the rights of children.

The JJ Act of 2015 serves as the foundation of India's adoption laws, emphasizing the importance of children's welfare and rights. This legislation outlines the fundamental principles and objectives for the care, protection, and rehabilitation of children in need, including those eligible for adoption. It underscores the significance of the best interests of the child in all decisions related to their welfare, establishing a strong ethical basis for the adoption process.

Accompanying the JJ Act are the Adoption Regulations of 2017, meticulously crafted by CARA to provide detailed guidelines and procedures for adoption practices. These regulations offer clear protocols and standards governing various aspects of the adoption process, from the eligibility criteria for prospective adoptive parents to the documentation requirements and adoption procedures. By outlining transparent guidelines, these regulations ensure accountability and adherence to ethical principles throughout the adoption journey.

CARA, as the apex body mandated to regulate and monitor adoption processes in India, plays a crucial role in implementing the provisions of the Juvenile Justice Act and Adoption Regulations. It oversees the accreditation and monitoring of adoption agencies, maintains a national database of adoptable children and prospective adoptive parents, and facilitates the adoption process through its online portal. Through its regulatory mechanisms, CARA ensures that adoption practices comply with legal requirements and ethical standards, thereby safeguarding the rights and welfare of children.

The legal framework governing adoption in India reflects a careful and comprehensive approach to child welfare, guided by principles of justice and respect for children's rights. By prioritizing the best interests of the child and establishing clear guidelines for ethical adoption practices, this framework aims to ensure that every child has the opportunity to grow up in a loving and nurturing family environment, where their rights and well-being are protected and respected.

8.4.1 Understanding the Adoption Process in India: The Roles of DCPO, CWC, and the Court

The adoption process for Indian prospective adoptive parents (PAPs) begins with registration on CARINGS page of CARA and then following instructions as provided there. This application initiates a thorough assessment process conducted by the SAA to evaluate the suitability of the prospective adoptive family. The assessment includes background checks, home studies, and counselling sessions to ensure that the prospective adoptive parents are capable of providing a nurturing and stable environment for the child.

Once the prospective adoptive parents are approved, they get added to the roster of other waiting parents and they are assigned a child as and when a child is available. Before finalizing the adoption, the child is placed in pre-adoption foster care with the prospective adoptive family, as outlined in Section 58 of the JJ Act. This interim period plays a pivotal role in facilitating the child's transition into the prospective adoptive family's home environment. During this phase of the adoption process, the District Child Protection Officer (DCPO) plays a role in overseeing the well-being of the child and ensuring that the placement within the adoptive family is conducive to the child's overall welfare. The DCPO's responsibilities encompass regular visits to the adoptive family's home, where they meticulously assess various aspects of the child's adjustment and integration into their new environment.

8.4.2 Identifying Gaps in Adoption Legislation

Despite the established legal framework governing adoption in India, several significant loopholes allow for the exploitation of vulnerable individuals and the perpetuation of adoption rackets. One notable loophole is the lack of stringent enforcement and monitoring of online adoption advertisements. Platforms like Sulekha.com provide a fertile ground for illicit adoption transactions, as individuals can easily post advertisements offering babies for adoption without adequate oversight. This loophole enables traffickers and unethical intermediaries to operate with impunity, exploiting the desperation of prospective adoptive parents and the vulnerabilities of birth parents.

Furthermore, ambiguities in the regulations surrounding the role of intermediaries pose another challenge to adoption regulation. While CARA guidelines prohibit the involvement of intermediaries in the adoption process, they often play a significant role in facilitating illegal adoption transactions. These intermediaries exploit loopholes in the system, such as ambiguous definitions of "facilitators," to circumvent regulations and profit from illegal adoption activities. This loophole allows unscrupulous individuals to exploit the lack of oversight and accountability, endangering the well-being of children and undermining the integrity of the adoption process.

Additionally, loopholes in the regulations governing documentation and verification processes further exacerbate the problem of adoption rackets. In the cited case from Baroda, perpetrators exploited weaknesses in the Aadhar card verification system to obtain false documents and falsify identities, enabling them to circumvent legal procedures and perpetrate illegal adoption transactions. This loophole highlights the need for stronger safeguards and verification mechanisms to prevent identity fraud and ensure the integrity of adoption procedures.

Furthermore, the absence of comprehensive oversight and regulation of cross-border adoptions presents another significant loophole in the legal framework. While international adoptions are subject to stringent regulations, gaps in coordination and enforcement between countries can be exploited by traffickers to facilitate illegal adoption transactions. This loophole allows traffickers to exploit differences in adoption laws and procedures between countries, making it difficult to track and prevent illicit adoption activities.

Addressing these loopholes requires a multi-faceted approach, including stricter enforcement of adoption regulations, enhanced oversight of online platforms, and greater collaboration between law enforcement agencies and adoption authorities. By closing these loopholes and strengthening the legal framework, India can better protect the rights and welfare of children and prevent the exploitation of vulnerable individuals in adoption rackets.

8.5 Lessons Learned and Future Actions in Combating Cyber-Enabled Adoption Rackets

Reflecting on the intricate dynamics of adoption rackets and the insights drawn from our investigation, several crucial lessons have surfaced, calling for both immediate and long-term actions to rectify systemic vulnerabilities and forestall future exploitation.

Below are the highlighted lessons gleaned from our examination of Cyber-Enabled Adoption Rackets:

- *Technological Facilitation*: The investigation into cyber-enabled adoption rackets highlights the critical role of technology in facilitating illicit activities. Perpetrators leverage online platforms and encrypted communication channels to orchestrate adoption transactions discreetly, exploiting the anonymity and reach provided by digital tools.
- *Deceptive Tactics*: Traffickers employ deceptive tactics, such as creating fake social media pages and posting false updates about children, to attract potential adoptive parents. These manipulative strategies underscore the need for vigilance and awareness among individuals seeking adoption opportunities online.
- *Vulnerability of Adoptive Parents*: The willingness of desperate adoptive parents to pursue

adoption through online platforms makes them susceptible to exploitation. Vulnerable individuals, driven by the desire for parenthood, may overlook red flags and fall victim to fraudulent schemes orchestrated by cyber-enabled adoption rackets.

- *Cyber security Challenges*: Cyber-enabled adoption rackets pose significant cyber security challenges, including data privacy concerns and the proliferation of online frauds. Regulatory measures and technological safeguards are essential to mitigate risks and protect individuals from falling prey to fraudulent activities online.
- *Collaborative Responses*: Addressing cyber-enabled adoption rackets requires collaborative responses involving multiple stakeholders, including law enforcement agencies, NGOs, and regulatory bodies. Enhanced coordination and information-sharing mechanisms are vital for detecting and dismantling criminal networks operating in the digital realm.
- *Education and Awareness*: Educating the public about the risks associated with online adoption processes is crucial for preventing exploitation and fraud. Adoptive parents should be equipped with the knowledge and resources to navigate adoption procedures safely and responsibly in the digital age.

The investigation into cyber-enabled adoption rackets highlights the need for proactive measures to address technological vulnerabilities, enhance cyber security protocols, and promote awareness among adoptive parents. As such, concrete solutions must be devised and implemented to effectively tackle the distinct challenges posed by adoption rackets and their exploitation through technology.

By adopting a multi-pronged approach that addresses both immediate challenges and systemic vulnerabilities, stakeholders can work towards building a more resilient and equitable adoption ecosystem. Collaboration between government agencies, law enforcement bodies, technology companies, and civil society organizations is essential to effectively combating adoption rackets and protecting the rights and well-being of vulnerable children. It is only through sustained and collaborative efforts that we can create a future where every child is afforded the opportunity to thrive in a safe and nurturing environment.

Chapter

09

Cyber Scamming/ Online Criminality

Chapter 9

Cyber Scamming/Online Criminality

9.1 Introduction

Inputs from global experts from Thailand and Philippines revealed an increasing number of young educated adults from South Asia being coerced to commit online criminality in the form of cyber scamming. Visible numbers of Indian youth among those trafficked for this purpose set the alarm to probe into this form and to understand the possible reasons for the computer skilled as a potentially vulnerable segment to be targeted in this new emerging form of human trafficking.

In a 2023 article by The Indian Express, it was revealed that unemployment rates were significantly higher among educated youth, reaching 18.4 percent in 2022, compared to just 3.4 percent for those without formal education.[121] This disparity underscores the challenges faced by educated youth in finding employment despite their investment in education. Exploiting this desperation and aspiration for a better life, human traffickers are using cyber technologies to trap and recruit unsuspecting individuals with technical skills for cyber scamming. These traffickers operate across various online platforms such as social media, messaging apps, and job sites, profiling their victims and luring them with false promises of high-paying jobs.

Unlike traditional trafficking victims, these individuals are targeted for their language proficiency and digital fluency, making them ideal candidates for online deception[122]. Recent graduates and those facing financial hardships are particularly vulnerable to promises of quick career advancement and lucrative opportunities in the technology sector. Fake online job advertisements serve as traps to ensnare these young people.

News reports have shed light on this emerging trend, exposing how educated unemployed individuals are targeted, groomed, and coerced into committing cyber-crimes. The Mekong Region, especially the golden triangle of Myanmar, Laos, and Thailand, has been identified as a hotspot for this exploitation, where thousands of youths from South Asia, including India, have been forced into slavery-like conditions to commit cyber-crimes.[123]

---

121 5000 Indians forced into cyber-slavery in Cambodia, MHA discusses rescue strategy. https://indianexpress.com/article/india/5000-indians-in-cambodia-forced-into-cyber-scams-mha-takes-note-9239156

122 Online scams in Southeast Asia create double victims: those targeted and those forced to carry them out. https://www.lowyinstitute.org/the-interpreter/online-scams-southeast-asia-create-double-victims-those-targeted-thos

123 Hundreds of thousands trafficked into online criminality across SE Asia. https://news.un.org/en/story/2023/08/1140187

To gain deeper insights into this trend, the research utilized three methodologies: an extensive review of news reports and published documents, interactions with law enforcement handling cyber scamming cases, and interviews with victims. The research team, led by a trained investigator, engaged with law enforcers and victims and conducted comprehensive desk reviews of relevant materials.

This chapter provides insights into this new and emerging form of organized crime that specifically targets educated and skilled individuals, coercing them into committing cyber- crimes, which has become a pervasive issue affecting many countries.

9.2 Understanding Cyber Scamming for Forced Criminality

Cyber scamming for forced criminality, a growing aspect of CEHT, involves the coercion of individuals into performing online scams and fraudulent activities. Cyber scamming leverages digital platforms and the internet to deceive individuals or organizations, often for financial gain.

Common techniques used in these scams include phishing, where fraudulent emails or messages trick individuals into revealing personal information; malware, which infiltrates and damages computer systems; social engineering, which manipulates people into divulging confidential information; identity theft, which involves impersonating someone to commit fraud; and online investment frauds, where fake investment opportunities steal money from unsuspecting investors.

Forced criminality refers to compelling individuals to engage in illegal activities against their will, using physical force, threats, psychological manipulation, or exploitation of vulnerabilities. In the context of cyber scamming, traffickers recruit victims through false pretenses such as fake job offers, isolating them and using threats, abuse, and psychological pressure to force compliance. This form of exploitation often involves blackmail, identity theft, and the exploitation of economic and social vulnerabilities, particularly targeting young adults, recent graduates, and individuals with IT skills.

9.2.1 Modus Operandi of Cyber Scamming

The modus operandi of cyber scamming involves a series of calculated steps designed to recruit, manipulate, and exploit victims. The process typically unfolds as follows:

- Recruitment: Traffickers use a variety of digital platforms, such as social media, job portals, and instant messaging apps, to identify and approach potential victims. They post fake job advertisements promising high salaries and rapid career advancement in the tech sector. These ads are designed to attract educated youth with IT skills who are desperate for employment.
- Grooming: After establishing contact, traffickers build trust with the victims by posing as legitimate employers or recruiters. They conduct fake interviews, provide counterfeit job offers, and create elaborate websites to support their claims. This grooming process aims to lower the victims' defenses and increase their willingness to cooperate.
- Coercion: Once trust is established and the victims are lured to isolated locations, often

in foreign countries, traffickers reveal their true intentions. Victims find themselves in controlled environments where they are subjected to threats, physical abuse, and psychological manipulation. Traffickers may confiscate identification documents, making it difficult for victims to escape.

- Execution of Scams: Victims are then forced to use their technical skills to carry out various forms of cyber-crime. This can include creating and sending phishing emails, developing malware, conducting financial frauds, and participating in online extortion schemes. The victims' expertise in digital technologies and languages makes them valuable assets in these illegal operations.

9.2.2 Profile of Victims and Traffickers of Cyber Scamming

Victims of cyber scamming for forced criminality under CEHT are typically young adults, aged between 20 to 30 years of age, with higher education degrees, especially in fields like information technology, computer science, and engineering. They often possess strong technical skills and are proficient in digital technologies, making them valuable targets for traffickers. These victims come from economically disadvantaged backgrounds, facing high levels of unemployment and limited job opportunities. They are driven by aspirations for better opportunities and are vulnerable to deceptive job offers promising lucrative salaries and career advancement.

Traffickers involved in cyber scamming are often part of organized crime syndicates or cybercriminal networks with sophisticated structures. They may include local recruiters, cybercriminals, and facilitators who provide logistical support. These traffickers exploit the economic desperation and aspirations of victims. They target vulnerable individuals through fake job advertisements, social media, and messaging apps, using deception and coercion to control their victims. Traffickers often operate internationally, making it challenging for law enforcement to track and dismantle their operations. A unique aspect of this form of trafficking is the double jeopardy the victim faces being victimized to perpetuate the crime which ends with most primary level recruiters/traffickers being former victims making it more impregnable to reach the actual operators.

The victims, mostly young men, are subjected to inhuman trauma and the psychological impacts are severe, including acute stress, anxiety, paranoia, depression, and post-traumatic stress disorder (PTSD). Socially, victims may become isolated and face stigma, while economically, they may suffer financial instability and legal repercussions. These factors highlight the profound personal and societal consequences of this form of human trafficking.

9.3 Cases of Human Trafficking for Forced Criminality through Online Scamming Centers in Southeast Asia

Recent news reports highlight a significant rise in cases of human trafficking for forced criminality at online scamming centers in Southeast Asia. According to The Indian Express, 5000 Indians were reportedly forced into cyber slavery in Cambodia alone.[124] The Indian government

124 5000 Indians forced into cyber-slavery in Cambodia, MHA discusses rescue strategy. https://indianexpress.com/article/

estimates that fraudsters have duped people of at least Rs 500 crore in India within a period of six months itself. Additionally, a BBC report identifies the bordering region of Myanmar, Cambodia, and Laos, known as the "Golden Triangle," as the main hub for these scamming operations, with countries like Thailand, Malaysia, Vietnam, and the Philippines acting as secondary hubs.[125]

A new trend in this form of human trafficking targets young, educated individuals with skills in computers and IT. Many victims are young, educated, multilingual professionals aged between 20 to 30 years of age. According to The Diplomat, English speakers are particularly valued.[126] This highlights the demand for educated youth with IT skills and proficiency in multiple languages, especially English, for cyber scamming activities.

Various agencies have conducted studies on this form of human trafficking, confirming its evolving nature and peculiar modus operandi. A 2023 report by the UNODC suggests that cyber slavery in Southeast Asia may constitute "one of the largest coordinated trafficking in-person operations in history."[127] Another report by IOM highlights a substantial rise in human trafficking related to online scams in the region, with estimates suggesting over 120,000 victims, particularly surging cases documented in 2023 alone.[128]

9.4 Unveiling Organized Cyber Scamming: Insights from Investigating Officers

To get a first-hand understanding of the nuances of this organized crime the investigator

india/5000-indians-in-cambodia-forced-into-cyber-scams-mha-takes-note-9239156

125 My hell in Myanmar cyber slavery camp. https://www.bbc.com/news/articles/cw076g5wnr3o

126 Cambodia's Cyber-Slavery Trafficking Denials Reflect Official Complicity, Experts Say. https://thediplomat.com/2024/04/cambodias-cyber-slavery-trafficking-denials-reflect-official-complicity-experts-say/

127 Casinos, cyber fraud and trafficking in persons for forced criminality in Southeast Asia. https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Summary_Policy_Brief.pdf

128 International Organization for Migration. Regional Situation Report on Trafficking in Persons into Forced Criminality in Online Scamming Centres in Southeast Asia. https://roasiapacific.iom.int/sites/g/files/tmzbdl671/files/documents/2024-03/iom-southeast-asia-trafficking-for-forced-criminality-update_december-2023-1.pdf

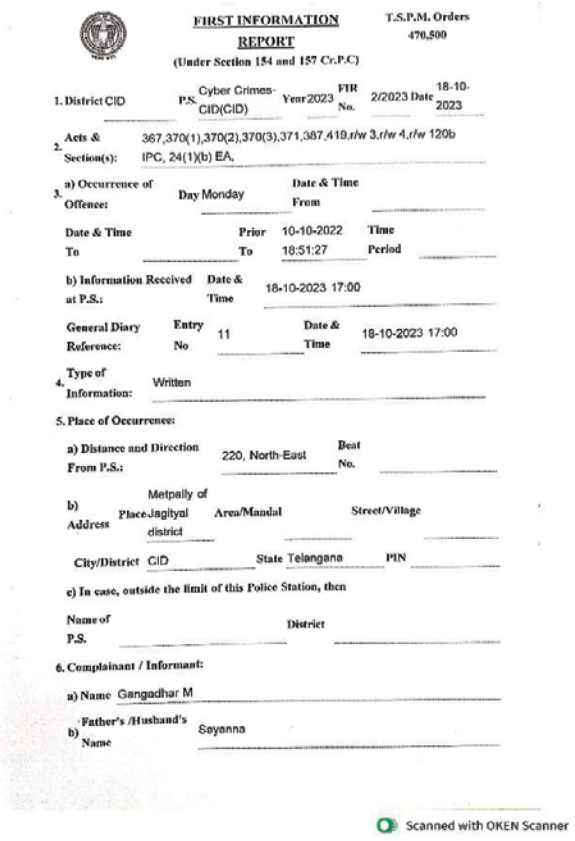
decided to probe two reported cases in the State of Telangana and met the investigating officers who were responsible for the case and the victims who fortunately escaped from the hell-holes. The two cases were reported in Hyderabad and Sircilla and were being investigated by the Crime Investigation Department and the district local police respectively.

A. Case – 1: Cr. No 2/2023 of Cyber-Crimes Police Station CID, Telangana

The case, registered as **Cr. No 2/2023,** was initiated Suo moto by the Crime Investigation Department, Telangana, based on a news report in the Times of India. The investigator met the officer responsible for the investigation and gathered the following information.

9.4.1 Brief Facts of the Case

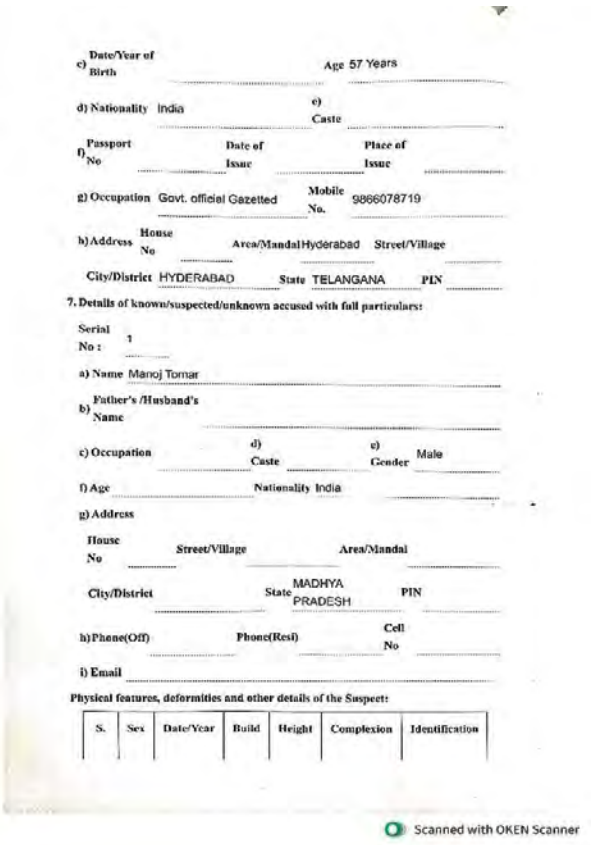
On January 18, 2023, Mr. M. Gangadhar, Deputy Superintendent of Police, Economic Offenses Wing-CID Telangana, submitted his inquiry report on a story reported in the Times of India to the Additional Director General of Police, CID, Telangana, Hyderabad. The report highlighted human trafficking and illegal detention of Indian citizens in the Myawaddy area of Myanmar in 2022 by a crime syndicate for forcible online scamming and extortion of money. Upon receiving the report, the ADGP CID instructed to register a case and hand it over to Mr. S. Harinath, Deputy Superintendent of Police, Cyber-Crime Unit, CID Telangana, for further investigation.



FIRST INFORMATION REPORT
(Under Section 154 and 157 Cr.P.C)
T.S.P.M. Orders 470,500

1. District CID P.S. Cyber Crimes-CID(CID) Year 2023 FIR No. 2/2023 Date 18-10-2023
2. Acts & Section(s): 367,370(1),370(2),370(3),371,387,419,r/w 3,r/w 4,r/w 120b IPC, 24(1)(b) EA,
3. a) Occurrence of Offence: Day Monday Date & Time From
Date & Time To Prior To 10-10-2022 18:51:27 Time Period
b) Information Received at P.S.: Date & Time 18-10-2023 17:00
General Diary Reference: Entry No 11 Date & Time 18-10-2023 17:00
4. Type of Information: Written
5. Place of Occurrence:
a) Distance and Direction From P.S.: 220, North-East Beat No.
b) Address Place Metpally of Jagityal district Area/Mandal Street/Village
City/District CID State Telangana PIN
c) In case, outside the limit of this Police Station, then
Name of P.S. District
6. Complainant / Informant:
a) Name Gangadhar M
b) Father's /Husband's Name Sayanna

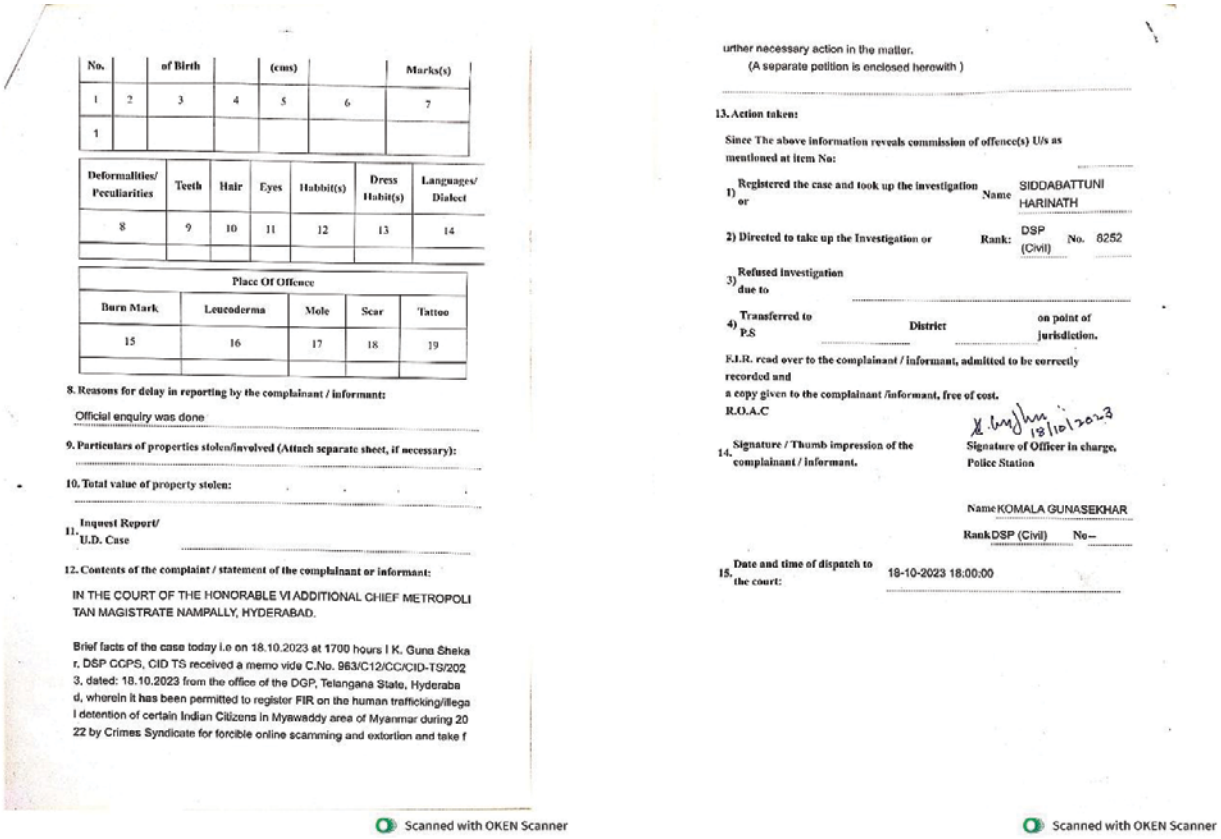
Scanned with OKEN Scanner



c) Date/Year of Birth Age 57 Years
d) Nationality India e) Caste
f) Passport No Date of Issue Place of Issue
g) Occupation Govt. official Gazetted Mobile No. 9866078719
h) Address House No Area/Mandal Hyderabad Street/Village
City/District HYDERABAD State TELANGANA PIN
7. Details of known/suspected/unknown accused with full particulars:
Serial No : 1
a) Name Manoj Tomar
b) Father's /Husband's Name
c) Occupation d) Caste e) Gender Male
f) Age Nationality India
g) Address
House No Street/Village Area/Mandal
City/District State MADHYA PRADESH PIN
h) Phone(Off) Phone(Resi) Cell No
i) Email
Physical features, deformities and other details of the Suspect:

S.	Sex	Date/Year	Build	Height	Complexion	Identification

Scanned with OKEN Scanner



No.		of Birth		(cms)		Marks(s)
1	2	3	4	5	6	7
1						

Deformalities/ Peculiarities	Teeth	Hair	Eyes	Habbit(s)	Dress Habit(s)	Languages/ Dialect
8	9	10	11	12	13	14

Place Of Offence				
Burn Mark	Leucoderma	Mole	Scar	Tattoo
15	16	17	18	19

8. Reasons for delay in reporting by the complainant / informant:

Official enquiry was done

9. Particulars of properties stolen/involved (Attach separate sheet, if necessary):

10. Total value of property stolen:

11. Inquest Report/ U.D. Case

12. Contents of the complaint / statement of the complainant or informant:

IN THE COURT OF THE HONORABLE VI ADDITIONAL CHIEF METROPOLI TAN MAGISTRATE NAMPALLY, HYDERABAD.

Brief facts of the case today i.e on 18.10.2023 at 1700 hours I K. Guna Sheka r, DSP CGPS, CID TS received a memo vide C.No. 963/C12/CC/CID-TS/202 3, dated: 18.10.2023 from the office of the DGP, Telangana State, Hyderaba d, wherein it has been permitted to register FIR on the human trafficking/illega l detention of certain Indian Citizens in Myawaddy area of Myanmar during 20 22 by Crimes Syndicate for forcible online scamming and extortion and take f

Scanned with OKEN Scanner

urther necessary action in the matter.
(A separate petition is enclosed herewith)

13. Action taken:

Since The above information reveals commission of offence(s) U/s as mentioned at item No:

1) Registered the case and took up the investigation or — Name SIDDABATTUNI HARINATH

2) Directed to take up the Investigation or — Rank: DSP (Civil) No. 8252

3) Refused investigation due to

4) Transferred to P.S — District — on point of jurisdiction.

F.I.R. read over to the complainant / informant, admitted to be correctly recorded and
a copy given to the complainant /informant, free of cost.
R.O.A.C

14. Signature / Thumb impression of the complainant / informant.

18/10/2023

Signature of Officer in charge, Police Station

Name KOMALA GUNASEKHAR

Rank DSP (Civil) No–

15. Date and time of dispatch to the court: 18-10-2023 18:00:00

Scanned with OKEN Scanner

FIR of the CID Case

9.4.2 Details of Accused

Manoj Tomar S/o Yashwant Singh Tomar age 26 years R/o U-Block, DLF Phase-3 Gurgaon Haryana, N/o ward No. 02, Galli No. 09, MLD Colony, Ambah Morena, Madhya Pradesh is the accused identified by the victims.

9.4.2.1 Victim's profile

V. Sri Krishna, a 29-year-old resident of Hanuman Nagar, Metpally town in Jagityal, Telangana, completed his M.Sc. in Mathematics and Computer Science from Jagityal. After graduation, he traveled to Iraq on a work visa, where he worked as an accountant in Erbil City for two years. Later, he transitioned to a cashier role with the Italian Contingent in Erbil, holding this position for three years. As his work visa approached expiration, he began searching for new job opportunities using various social media platforms.

One day, he received a WhatsApp message from someone identifying themselves as Arya Muthu from Thailand, offering a data entry operator position in Thailand with a monthly salary package of ₹1.5 lakh. He discussed this offer with his friend Raghu, who had also graduated from the same college in Jagityal and hailed from the neighboring village of Mannegudem in Korutla. Raghu, who was also Sri Krishna's roommate in Erbil, expressed interest in joining him for the job in Thailand. Arya Muthu communicated with both Sri Krishna and Raghu via Facebook Messenger and conducted interviews through video calls, with Manoj Tomar as the main recruiter. Both of them

were informed about their selection for the job and were asked to make necessary preparations for their departure.

9.4.2.2 The Trafficking Journey

Arya Muthu arranged their visit visas and flight tickets remotely. In late August 2022, they arrived in Bangkok from Qatar, Arya Muthu monitoring their journey via WhatsApp calls. At Bangkok airport, individuals in police uniforms received them and handed them over to an armed person in a jeep, followed by another armed escort. Initially taken to the city outskirts, they returned to the airport and met two individuals from Kerala. They all traveled together in the same jeep.

After a 5–6-hour drive, they stayed in a hotel where their passports were taken for work permits. Feeling uneasy, Sri Krishna took photos of the hotel and uploaded them. The next morning, they reached a checkpoint where guards were bribed, then ferried across the Moei River into Myanmar, which Sri Krishna recorded.

In a dense forest resembling a small township, their phones were formatted, and movements restricted. Despite promises of ₹1,50,000/- monthly, they were paid only ₹70,000/-. They realized Arya Muthu and Manoj Tomar was one and the same person. They were informed it was an online scamming center and they were given false identities, brief training, and made to sit on computers with scamming applications. Held hostage, they had no choice but to comply while Danny, their handler, monitored them.

9.4.2.3 The World of Online Criminality

Each member had specific tasks. Danny, the handler, assigned daily tasks such as creating fake accounts and chatting on messaging apps to recruit people aspiring to work in Bangkok. He also arranged air tickets and visas. One member targeted unemployed youth by offering fake jobs, trained in creating fake social media accounts, and identifying potential targets based on posting patterns.

Tasks included trapping individuals for cyber scams, scamming for money, managing fake social media accounts to acquire personal details, and luring Americans for fake cryptocurrency investments. They gained trust through chats, ensuring money was transferred discreetly. They used various social media and messaging apps and were monitored both virtually and physically. Specialized surveillance apps were installed to prevent victims from contacting others.

The two victims endured harsh working conditions, working 16 hours daily, facing punishment for non-performance, including beatings, electric shocks, and deprivation of food and water.

9.4.2.4 The Way to liberation

Amid their ordeal, Sri Krishna and Raghu managed to contact Arya Muthu (alias Manoj Tomar) and requested help to return to India. Sri Krishna somehow managed to inform his parents about their plight and arranged some money.

Arya Muthu demanded two months' salary as ransom for their release and facilitated a transfer of ₹50,000/- through the Binance cryptocurrency exchange. Sri Krishna also managed to contact Sri Sushil Rao, editor of Times of India Hyderabad, exposing their plight.

The story garnered national attention, leading to a Suo moto case registered by CID Telangana. The Ministry of External Affairs intervened, urging the Myanmar government to free the stranded Indians. Sri Krishna and Raghu identified Manoj Tomar in the compound as the one who trapped them. Reportedly, 10 victims paid ransom in cryptocurrency for their release, while the rest were rescued with the Indian Embassy's intervention.

9.4.2.5 Status of the investigation

The CID team when they started investigating the first target Manoj Tomar @Arya Muthu. He was arrested on 18-10-2023, and after the inquiry he turned out to be a victim of the same fraud, hence his statement u/s 164 Cr. P.C. got recorded by the concerned court.

9.4.2.6 Manoj Tomar's Ordeal: From Victim to Accused

Manoj Tomar, also known as Arya Muthu in the trafficking scheme involving V. Sri Krishna, turned out to be a victim himself, coerced into trapping others for scamming jobs. Manoj, a Bachelor of Arts graduate from Jiwaji University Gwalior, Madhya Pradesh, completed his degree in 2018. In July 2022, he received a job offer via WhatsApp from an unknown number named Danny, promising a data entry job in Thailand with a salary of ₹1.5 lakh along with free accommodation and food.

Following Danny's instructions, Manoj recorded a video in English and sent it. Subsequently, he was informed of his selection and was asked to choose a flight date to Bangkok. On July 4, 2022, he boarded a flight from New Delhi to Bangkok. Upon arrival, armed men received him, and he was taken to the outskirts of Mae Sot town, about 450 km from Bangkok. Crossing a river into Burmese territory, they reached a small township with Chinese-style wooden buildings. Here, Danny collected Manoj's passport, provided him with a new SIM card, and instructed him to use the name "Yash" for communication.

Feeling trapped in the highly guarded facility, Manoj acted under duress and started recruiting other victims as per instructions. To escape, he arranged ransom money with the help of his brother, transferring ₹1,00,000/- to his account, which was converted to cryptocurrency and paid to Danny. Later, he learned that he and 10 other victims, including Krishna and Raghu, were to be released. After reporting the loss of his passport at the police station in Mae Sot, Thailand, he was detained for 16 days before being deported to India on December 2, 2022.

Despite being initially trapped like other victims, Manoj found himself forced to follow the instructions of the handlers upon reaching the compound.

B. Case 2 - Cr. No 33/2024 Town Police Station, Sircilla

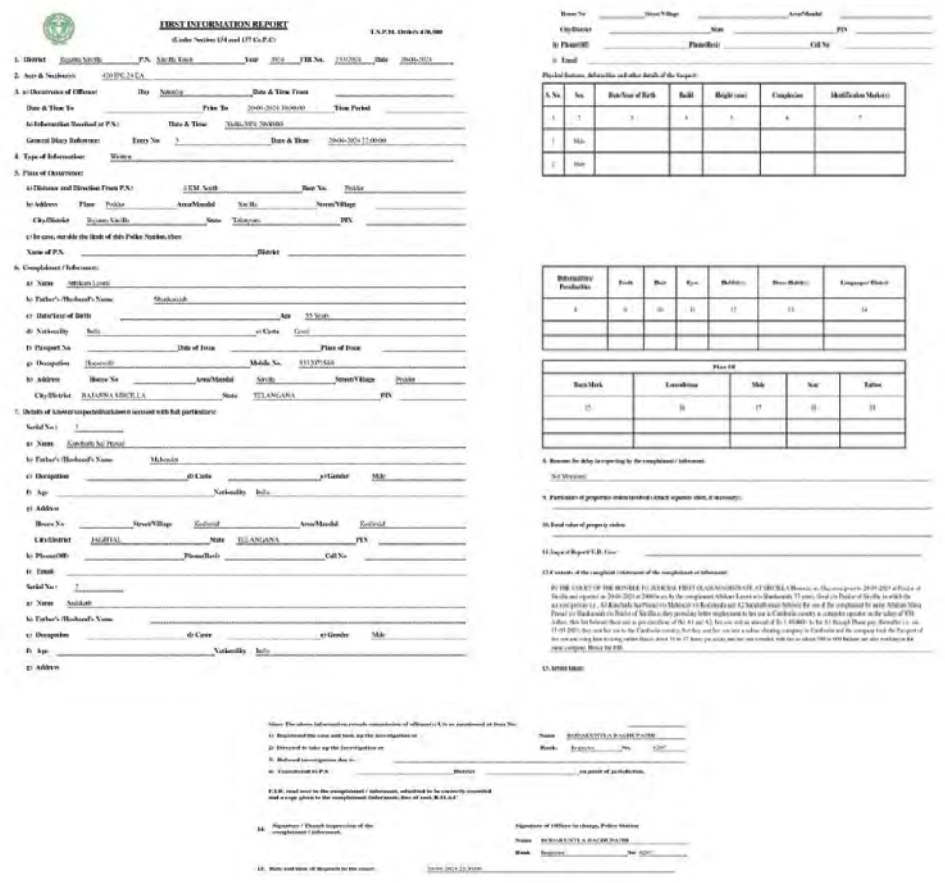
The second case booked U/S 420 IPC and 24 of Immigration Act was investigated by the team was registered in Sircilla after Smt. Athikam Laxmi, the mother of the victim, approached

the Superintendent of Police (SP) of Sircilla. She lodged a complaint to save her son, Athikam Shivaprasad, who was held captive in Cambodia. The investigator, guided by Mr. Akhil Mahajan, IPS, SP of Sircilla, met with the investigating officer from the Town Police Station. The complaint alleged that Athikam Shivaprasad was taken to Cambodia under false promises of a job as a computer operator with a salary of USD 950 per month and was subsequently kept in captivity.

The investigation identified several local mediators involved in facilitating this illegal human trade. Among them, four accused persons were identified locally, out of which one has been arrested:

- C. Sai Prasad of Kodimyal Jagityal (arrested)
- Prabhakar is presently in Maldives (not arrested)
- Abid Hussain Ansari from Pune, Maharashtra (Notice U/s 41 (a) served)
- Shadab from Bihar, presently in Dubai (Not arrested)

The FIR copy in this case is attached below. Since the case is still under investigation, the officer was not willing to share all details. Therefore, the investigator met with the victim and his family to gather firsthand information and the victim's perspective. It's important to note that the police recognized this case as an international cheating case and not as a human trafficking case hence Sec 370 of IPC pertaining to human trafficking was never applied.



FIR of the Sircilla Case

9.5 Understanding The Crime – From The Victim's Perspective

To gain insight into the crime from the victims' perspective, six survivors were contacted, though some were initially hesitant to speak due to the trauma they endured. Through persistent efforts and trust-building, they shared their experiences, shedding light on the impact of the crime on their lives.

A. Hyderabad to Myanmar

One of the victims, Ayaz Ali, a 25-year-old B. Com graduate from Shastri Puram, Yaqutpura, in the Old City of Hyderabad, shared his story. In 2017, he worked as an Office Helper in Dubai for a salary of ₹40,000/- per month. Upon returning to India in 2018, he worked in a banquet hall as a caretaker for a salary of ₹15,000/- per month, supporting his large family of seven members, including his aged and bedridden father.

9.5.1 Trafficking Bait

After returning to India, Ayaz continued to seek job opportunities abroad. In July 2022, he came across an advertisement on a Facebook Page posted by a user with the id "Ayan Khan," offering data entry jobs in Bangkok, Thailand. With his computer skills, Ayaz felt it was a good fit for him. He responded to the advertisement, and subsequent communications were made through Facebook Messenger and WhatsApp.

Ayan Khan was offered the job opportunity in Bangkok as a data entry operator with a salary of ₹1,00,000/- per month, along with decent accommodation and food. Ayaz was informed that the job visa would cost ₹2,00,000/-. He paid ₹1,00,000/- in advance through UPI provided by the recruiter and received an offer letter. Later, he met the agent Ayan Khan in person and paid ₹1,00,000/- in cash.

9.5.2 The Trafficking Journey

The agent instructed Ayaz to purchase a Thai Airways flight ticket from Bangalore to Bangkok for August 7, 2022, promising reimbursement later. They were asked to obtain tourist visas, with the assurance of converting them to work visas upon arrival. Ayaz bought the ticket and joined a WhatsApp group of 8 people at Bangalore Airport, including three from Hyderabad, who were all heading to the same destination.

Upon landing in Bangkok, they were directed to get tourist visas by paying the fee. After immigration clearance, they were met by two individuals in military-like uniforms armed with firearms, who escorted them to a pickup truck. They traveled about 8 hours through the jungle until they reached a lakeside, where they boarded a boat to the other side.

On the other side of the lake, they were handed over to new guards by their escort. Communication was difficult as the guards didn't understand English, and any attempts to communicate were met with glares. The truck then traveled for 2 more hours through forests and

small villages with Burmese signboards until they arrived at a high-security compound with a large black iron gate. The truck entered the compound upon arrival.

9.5.3 Cyber scamming compounds - A Hell Hole

Upon arrival, they discovered concrete blocks and traditional Burmese hut-type structures made of bamboo. A person of Indian origin, introducing himself as Nicholas alias John, welcomed them, indicating he was the team leader, possibly from Kerala based on his accent. He explained they were in a compound controlled by the Chinese in Myanmar and instructed them to rest in a hall, warning against unnecessary roaming. Realizing the gravity of their situation all of them obeyed. They were served fruits and chapati with dal before sleeping.

The next morning, 'John' revealed that they would work in departments like cryptocurrency websites, gaming sites, loan apps, and fake customer care centers to scam Indian nationals. Some victims protested, stating they were misled about their work. In response, armed guards arrived, beating those who resisted. Two victims tried to fight back and were severely beaten, then forced to stand in a river for hours until they fainted. Ayaz mentioned around 200 men, mostly Indians, were working there, threatened with dire consequences if they resisted, including rumors of murders and burials in the jungle for dissenters.

Scars of torture in the compound

9.5.4 Tasks and Operations in the Compound

All the group members underwent training for their assigned tasks. One category involved engaging people over the phone, convincing them to download loan apps on their mobile devices, compromising their privacy and security. Once the caller agreed, the line would be transferred to the team supervisor.

Another task was persuading individuals to invest in fake cryptocurrency on bogus websites. Additionally, they targeted youth, encouraging them to download and invest in betting apps and play various games.

Another category involved providing leads to individuals based on Google queries, posing as a legitimate customer care center. When the target agreed, the call would be escalated to the team supervisor.

Several other departments in the compound, most likely supervised by Chinese nationals, targeted different countries. All calls were recorded and closely monitored, and strict instructions were given not to disclose anything about the facility.

9.5.5 Victim's Journey to Liberation

Ayaz Ali Khan earned the trust of his team leader John by actively engaging in work and assuring him of his cooperation if the company fulfilled its promises. Eventually, he requested a mobile phone from John to contact his family and assure them of his safety. With a strict warning from John not to disclose anything about the facility, Ayaz briefly communicated with his family. Later, he managed to convey to his uncle in Telugu about the danger he was in and urged him to rescue him.

Ayaz's uncle, Imtiaz, traveled to Bangkok with the help of his contacts and negotiated with the syndicate for Ayaz's release, paying a ransom of ₹2,50,000/- (equivalent to USD 29,947). Similarly, other victims also paid ransoms and returned to India. Upon returning, Ayaz contacted a local leader and shared his story, which was then tweeted, alerting the nation.

The Government of India took serious action upon receiving this information and sent a special team to Bangkok. With the assistance of the Thai Government, approximately 370 victims of such fraudulent job syndicates were rescued and brought back to India.

Unfortunately, none of the victims were willing to lodge a complaint indicating deep rooted fear and threat perception to their lives by the criminal syndicates.

9.5.6 Starting afresh

Out of 8 victims contacted by the researchers, 6 victims are presently working in Gulf countries and two of them are working in India.

B. Sircilla to Cambodia

Atikham Shivaprasad, a resident of Sircilla Town in Telangana, hails from a modest family background. He is the only son of A. Shankaraiah, a retired bus conductor from RTC, who is paralyzed and bedridden, requiring constant medication. Shivaprasad completed his B.Sc. Degree with Chemistry in 2016 and aimed to secure a government job, but faced repeated disappointments. In 2022, he found employment as a sales representative in an overseas pharmaceutical company, earning ₹30,000 per month. Alongside, he honed his computer and IT skills, hoping to explore international job opportunities, particularly in countries like the United States or UK.

Unable to find suitable opportunities abroad, Shivaprasad sought help from his neighbor, Ajay Kumar, who had worked in the Maldives. Ajay mentioned Kancharla Sai Prasad from Kodimyal town, Jagityal District, who could assist in securing overseas jobs. Sai Prasad discussed job prospects with Shivaprasad over the phone, offering a computer operator job in Cambodia with a salary of around USD 1200 per month, a significant increase from his current income.

Shivaprasad was introduced to Deepu, a Nepali citizen working as a senior agent in a Chinese

company in Cambodia. He was informed that the process fee would be ₹2,00,000/-, but Shiva Prasad could only arrange ₹1,40,000/-. He transferred ₹1 lakh to Sai Prasad and ₹40,000/- to Sai Prasad's wife's account via UPI.

Another person named Sadakhat, from Pune, claimed to work as an agent for Deepu. He collected Shivaprasad's passport details and arranged an "Electronic Visa" for tourism in Cambodia, valid for up to 30 days. Sadakhat also arranged a flight ticket via Singapore Airlines from Hyderabad to Phnom Penh via Singapore. The visa and flight details were shared with Sai Prasad through WhatsApp and then forwarded to Shivaprasad.


KINGDOM OF CAMBODIA
Nation - Religion - King
Visa no. 2024010119857
Surname
ATHIKAM
Given Name
SHIVAPRASAD
Passport No
Country of Nationality
India
Date of Birth
18 Feb 1996
Gender
Male
Length of Stay
One month (single entry)
Visa Issued
05 Jan 2024
Expire Date
05 Apr 2024
Visa Type
T
Immigration Use Only
e-visa
TIHO SAMNANG

9.5.7 The Journey into Trafficking

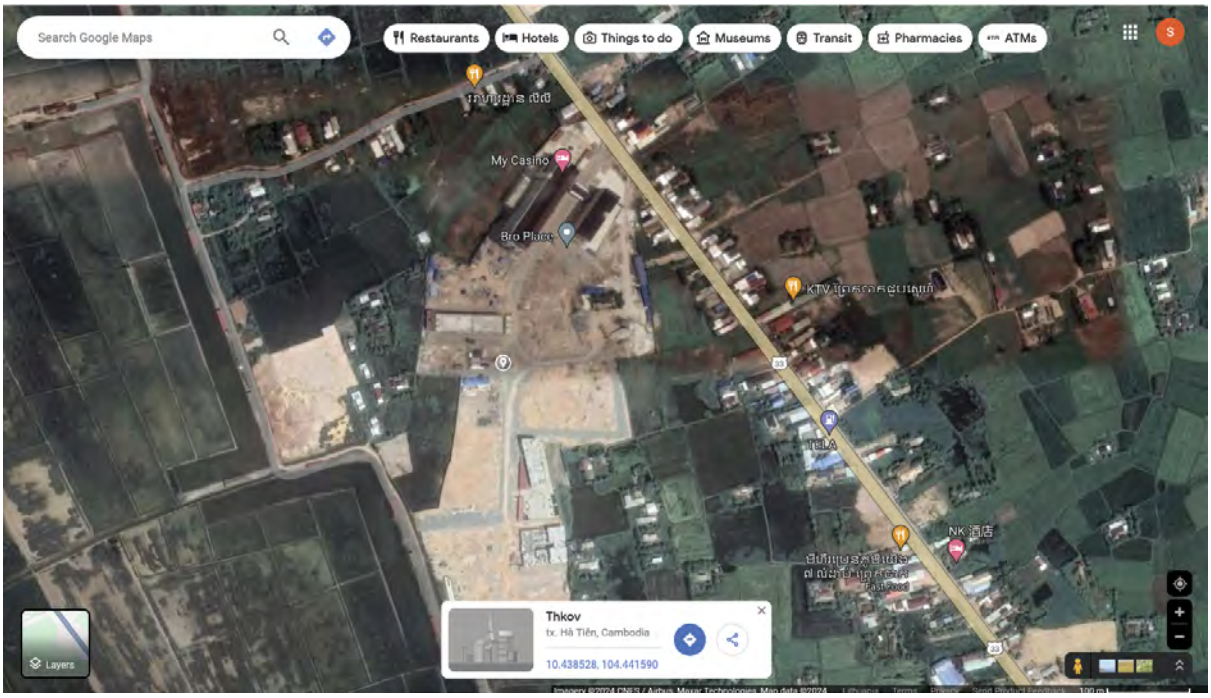
On January 11, 2024, Shivaprasad boarded a Singapore Airlines flight from Hyderabad and arrived in Phnom Penh on January 12, 2024. Upon arrival, a Cambodian national recognized Shivaprasad from the photo shared on WhatsApp and received him. Due to the language barrier, communication was challenging. He was then escorted to a small car, marking the beginning of a 250 kilometers road journey that lasted about five hours.

9.5.8 Entering the World of Exploitation

The vehicle eventually stopped in front of a high-security compound. Security personnel checked his baggage, frisked him, and confiscated his passport. Shivaprasad was then assigned to a room along with 12 others. The compound comprised 4 buildings, each with 7 floors. Approximately 1500 people worked in the compound, predominantly Indians, Nepalis, Sri Lankans, Bangladeshis, and Pakistanis, with a few Chinese nationals as well. Among them, around 600 were Indians.

Upon arrival, Shivaprasad's first interaction was with a Chinese individual known as the "Master," who spoke fluent English. The Master informed him that he wasn't recruited for a computer operator job but for cyber scamming, emphasizing that resistance was not an option. Shivaprasad underwent 7 days of training on how to scam Indians by posting positive reviews on websites.

Shivaprasad, like others, had to endure 12-hour shifts with no breaks. During lunchtime, they had to bring food to their workplace to minimize time away from the computer. Each team, comprising 16 members including the leader, worked on desktop computers with Telegram



Location of the Cyber Scamming Centre

registered with Indian sim cards. They were provided with Indian bank account details linked to mobile numbers for receiving money from victims.

Each person in the compound had a daily target of trapping at least 12 people. Failure to meet targets resulted in additional working hours. Poor performance led to punishments such as physical exercises, beatings, deprivation of food and water, and confinement. Good performance was rewarded with incentives of USD 12 for each new victim trapped.

Refusal to perform tasks led to severe punishments. Those who protested were beaten in front of others and video recorded. Rebellion was met with cuts on muscles as a warning.

The food supplied, including beef, insects, lizards, and poorly cooked boiled food, was unfit for Indian consumption. Shivaprasad, along with others, preferred vegetarian options but rarely received them. This affected their health significantly.

Realizing the scam and deteriorating health, Shivaprasad expressed his desire to return home. The Master demanded ₹4,00,000/- for his release, which Shivaprasad couldn't afford as he had already paid ₹1,40,000 to his agent.

9.5.9 Modus Operandi of the crime

The caller reaches out to people using mobile numbers provided by the team leader on Telegram, offering a chance to earn money by posting positive reviews for popular travel websites like yatra.com, makemytrip.com, cleartrip.com, and travelguru.com. Interested individuals are directed to a portal resembling legitimate travel sites, where they register with their email ID, mobile number, and bank account details.

Users are given sets of 30 links, each leading to templates for positive feedback. They earn ₹1500/- for every set completed, which takes around 30 to 45 minutes. Earnings are verified through bank balance confirmation, encouraging users to complete more tasks for more money.

The scheme escalates when users are asked to invest ₹10,000/- for access to 90 links, promising a return of ₹19,000/- upon completion. Further investments are encouraged for additional link packages, but users receive only a fraction of the promised amount, with the rest shown as credited on the website.

Attempts to withdraw earnings lead to requests for depositing half the withdrawal amount before processing. Users are enticed with promises of upgraded accounts for higher earnings, but persistent withdrawal requests result in account blockages.

Female victims asking for money return face escalated threats. They are coerced into generating nude videos, which are then used to blackmail them into depositing money, under the threat of sharing the videos with their contacts. Shivaprasad shared a case where an individual lost ₹25 crores over six months due to this scheme.

9.5.10 Money Laundering Process

Once the caller convinces the customer to join various schemes, mule bank account details are provided. After depositing the agreed amount, the depositor must share a screenshot of the payment on Telegram with the caller. Agents manage several hundred bank accounts, rotating them after multiple transactions to avoid suspicion. New accounts are shared periodically.

Indian agents convert the deposited amount into cryptocurrency and transfer it to the handler's crypto account. This process helps disguise the origin of the funds and makes it harder to trace the illegal transactions.

9.5.11 Victim's liberation

From the outset, Shivaprasad realized he was ensnared in a trafficking racket facilitating cyber fraud. Choosing to break free, he remained silent for a while, observing the harsh treatment of those who resisted. When he got access to his mobile phone, he reached out to a relative in the Police Department in Sircilla District. Together with his mother, they sought help from the Superintendent of Police in Sircilla District, leading to the arrest of local agents and the registration of a case.

- Seeking Government Assistance

  On April 4th, 2024, Shivaprasad emailed the Ministry of External Affairs seeking assistance. Responding to his plea and the efforts of the Sircilla Police, the Ministry contacted the Indian embassy in Cambodia for his rescue. On April 25th, 2024, embassy staff from Phnom Penh, accompanied by Cambodian armed police, arrived at the compound for inquiries.

- Rescue and Return

  Identifying himself, Shivaprasad expressed his desire to return home when the embassy staff arrived. His passport was handed over to them. Ten victims, including Shivaprasad, came

forward to return home. Among them, six were Indians, and four were Chinese nationals. They were rescued and placed under police protection. Shivaprasad's statement was recorded, and he was provided with USD 450 and a flight ticket to Hyderabad.

- Safe Return Home

  On April 27th, 2024, Shivaprasad boarded the flight to Hyderabad, where he was received by his relatives. He provided the coordinates of the compound's location in Cambodia, where the cyber scamming operation was underway.

- Current Status

  Athikam Shivaprasad returned to India with assistance from the Indian Embassy and local police, where he was received by his relatives. He is currently living with his family. He is still recovering from the trauma that he faced in the past few months.

9.6 Insights from the Analyses of the selected cases of Cyber Scamming

Human trafficking for online criminality or cyber scamming is the most recent purpose of exploitation and is largely cyber-enabled targeting the educated skilled youth and represents a disturbing trend. While the situation is acknowledged by the authorities' interventions to counter the same is still in its nascent stage. Key insights gained after the study of the reported cases serves as a starting point to explore the possibility of designing comprehensive programs to address the same:

- Targeted Victims: Hundreds of thousands of young, educated individuals from South Asia, particularly between 18 to 30 years of age, are specifically targeted. They are promised lucrative jobs in the IT sector, making them vulnerable to exploitation. The victims mainly come from countries like India, Pakistan, Sri Lanka, Bangladesh, China, and Indonesia.
- Victimization Techniques: Victims are often enticed through various cyber platforms, both online and offline. They are approached with promises of high-paying jobs abroad, exploiting their desperation for employment. Many victims are skilled in cyber technologies, making them prime targets to commit cyber-enabled crimes.
- Coerced to become Perpetrators: This organized crime by design targets victims to continue the cycle of crime. The victims apart from being coerced or manipulated into committing cyber fraud, such as posting fake reviews, participating in financial scams, or other illegal activities are also compelled to recruit new victims.
- Lack of Support Services: Upon their return, victims find themselves without any support system. There are no victim services to assist them, leaving them unemployed, heavily indebted, and psychologically traumatized. The absence of trauma-informed support exacerbates their suffering.
- Fear and Reluctance to Report: Victims are often too afraid to report the crime due to the lack of comprehensive victim protection and the fact that most have escaped these dungeons of horror by paying a ransom. They live in constant fear of reprisals from their traffickers with the additional moral burden of committing further crimes.

- Corruption and Facilitation: Corruption among border security officials in destination countries facilitates the trafficking process. This corruption enables traffickers to operate with impunity, making it challenging to intercept and rescue the victims.
- Need for International Cooperation: Currently, there are no formal agreements between countries to rescue and rehabilitate the victims. Ad hoc methods are used based on the victim alerts. There is a pressing need for international cooperation to address this transnational crime effectively.
- Urgency for Action: While this form of organized crime is still emerging, the sheer number of victims demands urgent action. Efforts are required to prevent further victimization and establish a robust response mechanism. This includes comprehensive victim support, dismantling criminal syndicates, and international collaboration to combat this modern-day slavery.

While this form of organized crime may seem relatively new and still gaining recognition, the alarming number of young people already ensnared in this situation demands urgent action from both governmental and non-governmental entities. It is imperative to not only prevent further victimization but also to develop a robust response mechanism.

Efforts must be intensified to prevent this crime by all means. There is a pressing need to bring about inter-country consensus at the regional level on a comprehensive response strategy. This strategy should focus not only on rescuing victims and providing them with holistic support but also on dismantling the criminal syndicates behind these activities through mutual cooperation. The scale of this problem necessitates a coordinated action at local, national, and international levels to effectively combat human trafficking by this online cyber scamming.

Chapter

10

Exploitation in War/Combat Zone

Chapter 10

Exploitation in War/Combat Zone

10.1 Introduction

The news report of a young Hyderabadi man killed in a drone attack in the Ukraine-Russia war was the precursor for a series of field investigations to understand the true facts behind the case. Interactions with the family revealed a criminal conspiracy which was largely cyber-enabled to lure young gullible youth with offers of job abroad in the service industry, and then coerced to work in the highly risky and lethal combat zone. This chapter provides an insight into this new form of human trafficking which has emerged due to the current unrest arising in the geopolitical situations.

The recent turmoil in several regions has provided fertile ground for the proliferation of such heinous offenses. The conflict between Israel and Hamas-led Palestinian militant groups, which erupted into a full-scale armed confrontation chiefly in and around the Gaza Strip in October 2023, has served as a stark reminder of the devastating consequences of warfare. Similarly, the invasion of Ukraine by Russia in February 2022 escalated the Russo-Ukrainian War to unprecedented levels of violence, resulting in catastrophic loss of life and a massive refugee crisis. Additionally, tensions between Azerbaijan and Armenia reached a boiling point in September 2023, leading to protests in Armenia following Azerbaijan's military offensive in Nagorno-Karabakh.

In the midst of these conflicts, the demand for human resources to fuel the war machine has never been more pronounced. Traffickers, recognizing the opportunity presented by the chaos and desperation engendered by armed conflict, have brazenly exploited vulnerable individuals for recruitment into these bloody confrontations. The loss of life has created a void that traffickers are all too eager to fill, preying on the vulnerable and marginalized with promises of opportunity and prosperity.

To understand this disturbing phenomenon, the investigator interacted with the victims and their families, seeking to unravel the modus operandi of traffickers through the harrowing experiences of those directly affected. Through an in-depth exploration of three case studies involving individuals recruited for war fronts in Ukraine the complexities of CEHT for war recruitment was better understood. Examining the nuances of these cases and delving into the lived experiences of the victims aims to foster a deeper understanding of this egregious form of exploitation and advocate for meaningful action to combat it.

10.2 Case Studies of Young Men Trafficked to War Zone

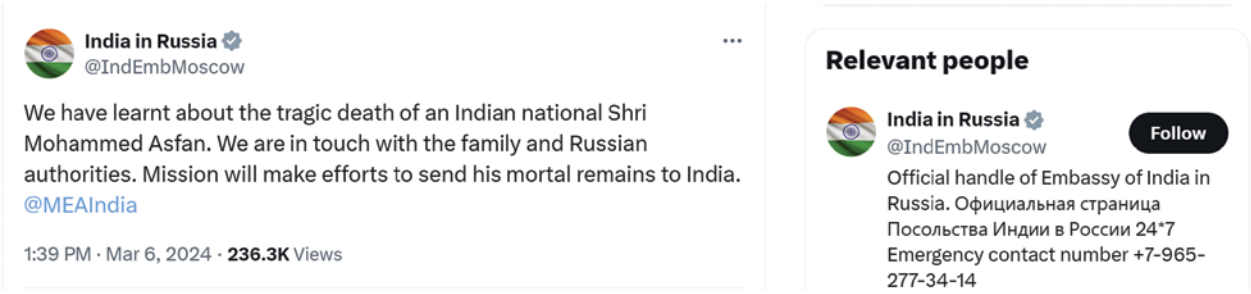
The cases of CEHT involving Indian youths lured into military service in Russia highlights the alarming convergence of technology and exploitation. This nefarious scheme, orchestrated through social media and deceptive promises, trapped unsuspecting individuals, leading to tragic consequences.

The investigation yielded specific details, as outlined below in the form of three case studies. **Case Study 1** focuses on victim Mohammed Asfan, **Case Study 2** delves into the experiences of Syed Iliyas Hussaini, Mohammad Sameer Ahmad, Abdul Nayeem, and Mohammed Sufiyan, while **Case Study 3** reveals the ordeal faced by Mohammed Tahir Rafeeq Bhai Shaik. During the course of the research, the team accessed a survivor who managed to escape the war zone.

10.2.1 Case Study 1: Mohammed Asfan

10.2.1.1 How it started:

On the 6th of March 2024, the Indian Embassy in Moscow tweeted about the tragic death of an Indian National Mohammed Asfan, from Hyderabad sparking widespread attention.



10.2.1.2 Research and Investigation:[129]

The research team interacted with Mohammed Asfan's family in Hyderabad to understand how he was recruited. As the research was being done in tragic circumstances the team also assisted the family to exert pressure on the Government of India to expedite the repatriation of the mortal remains of Mohammed Asfan from Russia.

In our interactions with the elder brother of Asfan it was revealed that a viral YouTube video by Faisal Khan @ Baba Blog was the bait used to entice him with offers of great jobs in Russia including an option to migrate to Europe. The video showcased employment opportunities in Russia with many promises. These promises included:

- *Non-Combat Roles*: Assurances of roles such as cleaning work, security of buildings, and working in the kitchen. The video also led many to believe that they would receive substantial financial compensation for their services, with promises of salary increments after completion of training.

129 Prajwala aggressively advocated for providing support to these victims/survivors after coming to know of their plight. Prajwala continues to follow up on the case. Those details are not mentioned in the report to retain focus. Details of the case and Prajwala's intervention is detailed at www.prajwalaindia.com

Modus Operandi / Luring Tactic: Viral YouTube Video

- *Russian Work Visas*: Assurances of legitimate work permit to facilitate employment in Russia for the specified roles.
- *Training Period*: During the training period a monthly salary of ₹40,000/-, with the expectation of a significant raise to ₹1,00,000/- per month upon completion of training.
- *Non-Deployment at Border*: Individuals obtaining the visa would not be deployed at the border or involved in combat activities. Instead, they would be working in non-combat zones within the Russian Army infrastructure.
- *Permanent residency in Russia*: Promises of permanent residency in Russia after working there for six months to a year.
- *Lure of residency in Europe*: The video also subtly indicates being taken to Finland and other European nations.

The video effectively preyed on the aspirations of individuals seeking better opportunities abroad, masking the true intent of exploitation behind the facade of legitimate employment prospects.

10.2.1.3 Victim's Profile and Luring Tactics:

Mohammed Asfan, a 30-year-old resident of Bazarghat, Hyderabad, came across Baba Blog's online offer of military helper jobs in Russia. Enticed by promises of non-combat roles like kitchen and miscellaneous work, he responded to the offer. After engaging in several discussions with Baba Blog, Asfan paid over ₹2 lakhs in India to obtain a Russian tourist visa on his passport, believing it to be a legitimate employment opportunity.

10.2.1.4 Journey to Exploitation:

Upon reaching Moscow on November 9, 2023, Asfan met with consultancy agents as planned and paid them approximately ₹80,000/- in US Dollars. He then underwent two weeks of military training alongside others from Indian and Nepali backgrounds at undisclosed locations arranged by the Military.

10.2.1.5 Events Leading to Tragedy:

Once inside the military camp, Afsan realised it was a trap as every day he was being led closer to the conflict zone. Realizing the deception, Asfan reached out to his family for help. By now instead of the promised non-combat roles, he found himself at the Ukraine border, where intense combat was ongoing between Russia and Ukraine. Unable to leave due to his confiscated passport, Asfan repeatedly contacted his recruiter for assistance, but received no aid. Tragically, his life ended in a drone attack. On the 6th of March 2024 Indian Embassy in Russia tweeted about the death of Mohammed Afsan in Russia.

10.2.2 Case Study 2: Syed Iliyas Hussaini, Mohammad Sameer Ahmad, Abdul Nayeem, and Mohammed Sufiyan

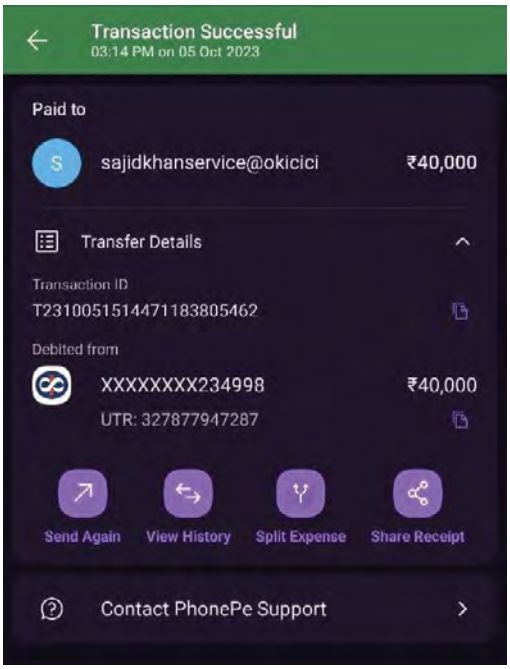
With media attention regarding Mohammad Afsan gaining momentum with political leaders also voicing their concerns; concerned families from other parts of the country also started raising their voice. The news of four young men from Karnataka alerting their families to rescue them from Russia led the investigator to meet the families of all four men living in Kalburagi one of the largest cities in Northern Karnataka.

10.2.2.1 Victims' Profile and Luring Tactics:

Hailing from Kalburagi, Karnataka, these four individuals, employed in a Dubai packaging factory, were targeted through the same viral YouTube video by Faisal Khan @ Baba Blog.

10.2.2.2 Journey to Exploitation:

Intrigued by the promises outlined in the YouTube video they visited the consultancy office of said Baba Blog in Dubai. They hoped to secure employment opportunities in Russia, as described in the video. However, upon their engagement with the consultancy office, they were asked to pay ₹3,00,000/- per head, divided into various stages for the helper job.

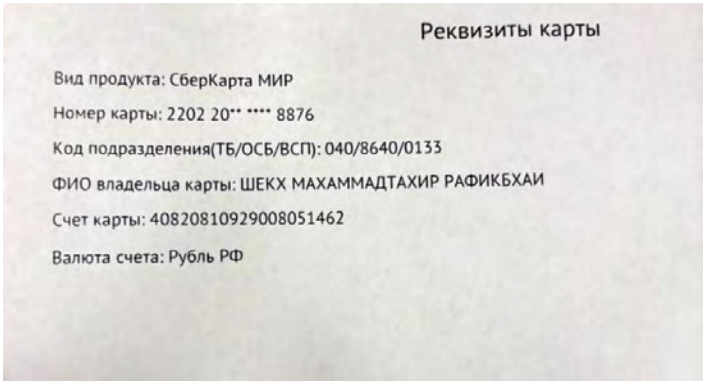


The victims initially paid half of the required amount at the Dubai consultancy office. At this stage, their passports were collected, and Russian tourist visas were obtained on their behalf. Subsequently, they returned to India and completed the remaining payment, executing transactions through net banking or by issuing checks from their personal accounts to the specified account details provided by the recruiters.

On the 18th of March 2023, the victims boarded a flight in Chennai bound for Moscow, with a layover in Sharjah. Upon their arrival in Moscow, the agents Nazil and Pushkrit received them. Each victim handed over ₹80,000/- worth of money in US dollars to these agents. Subsequently, the agents transported the victims to an undisclosed location, from where they were handed over to Russian Army agents.

At this undisclosed location, their travel documents were confiscated purportedly due to security reasons, and they were subjected to a 15-day training program. This training regimen included instruction in the use of various firearms, grenade launchers, and grenade throwing techniques. Additionally, they were provided with military attire, and subsequently taken to the border area of Ukraine.

Once at the border, the victims were assigned tasks such as digging bunkers and trenches to facilitate combatants in hiding and firing. Notably, while Iliyas, Sameer, and Sufiyan were deployed in a single location, Nayeem and Yousuf from Jammu and Kashmir were deployed in different locations along the border of Ukraine.


Реквизиты карты

Вид продукта: СберКарта МИР

Номер карты: 2202 20** **** 8876

Код подразделения(ТБ/ОСБ/ВСП): 040/8640/0133

ФИО владельца карты: ШЕКХ МАХАММАДТАХИР РАФИКБХАИ

Счет карты: 40820810929008051462

Валюта счета: Рубль РФ

Snapshot of the contract letter

10.2.2.3 Events Leading to Tragedy:

Despite being assured of non-combat roles; the victims were deployed in active combat zones along the Ukraine border. On February 21, 2023, a Ukraine drone attack targeted their position, resulting in casualties among the Russian personnel. The attack occurred approximately 100 meters away from the bunker/trench where the victims were stationed. In the aftermath, the victims discovered scattered dead bodies, including their friend Hamil Ashwin. Following the attack, the survivors were left stranded and desperate to return home. However, their efforts to seek assistance were hindered by the confiscation of their travel documents by the Russian Army agents for security reasons. This left them unable to seek help or leave the country. Despite their challenges, the survivors persisted in contacting their parents whenever they could access the internet through WhatsApp calls.

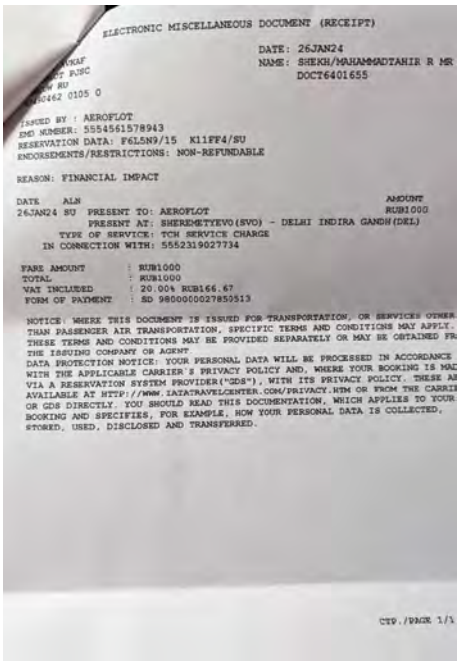
The family alerted the media and the CBI has taken up the case and has apprehended recruiters located in India.

10.2.3 Case Study 3: Mohammed Tahir Rafeeq Bhai Shaik

Investigator's interactions on WhatsApp with the four men stranded in Russia revealed that one Indian belonging to Gujarat had somehow escaped and was back to India. The investigator was able to secure the details of the returnee and went to meet him in Gujarat.

10.2.3.1 Victims' Profile and Luring Tactics:

Mohammed Tahir Rafeeq Bhai Shaik, a 24-year-old individual from Ahmedabad, with an Indian passport had completed his 12th grade. Tahir had watched the YouTube videos by Baba vlogger offering jobs primarily in Russia, particularly as helpers to the Russian Army. Similar to the first two case studies, these videos, purportedly posted from St. Petersburg, Russia, detailed job offers with training periods and salaries, requiring a payment of ₹3,00,000/- in installments.



10.2.3.2 Journey to Exploitation and on ground experiences:

Tahir contacted Faizal Khan via WhatsApp at Mobile No. 7066665290 and made payments totalling ₹1,10,000/- through UPI transactions to a QR code provided to him.

Subsequently, Tahir received confirmation of his flight to Russia, initially scheduled for December 15th, 2023, from Chennai. However, due to a purported delay, Tahir, along with other aspirants, stayed in a private accommodation in Pallavaram, Chennai, coordinated by agents named Sufiyan and Pooja. Tahir made further payments totalling ₹1,10,000/- in cash to an individual named Moin in Chennai. On December 25th, 2023, Tahir, along with another aspirant named Hamil, arrived in Moscow, Russia, where they were received by a person named Jobi Benasm Nijil, a person belonging to South India.


भारत गणराज्य REPUBLIC OF INDIA

P IND

JOBI BENSAM

NIJIL

भारतीय/INDIAN M 29/11/1984

THOTTATHUVILAI, TAMIL NADU

MADURAI

09/09/2016 08/09/2026

P<INDJOBI<BENSAM<<NIJIL<<<<<<<<<<<<<<<<<<<<

P3807660<1IND8411291M2609083<<<<<<<<<<<<<<4

Upon arrival, Tahir and Hamil were accommodated in a two-bedroom flat in Moscow, later transported to a military hospital for health checkups and then to Rayzan City for training. The training, conducted in Russian, involved various military exercises including firearm handling. Tahir managed to obtain a picture of the contract in Russian, where the salary was mentioned as RUB.1,95,000/-, approximating to ₹2,00,000/-. When concerns were raised about the safety conditions Tahir was told by the commander that the chances of a safe return from the frontline were only 10 percent.


GULF AIR

GULF AIR

BOARDING GATE WILL BE CLOSED 20 MINUTES BEFORE DEPARTURE TIME.

PASSENGER NAME SHEKH/MAHAMMADTAHIR RAFIKB

DEPARTURE DATE 23DEC2023 DEPARTURE TIME 04:10

FROM CHENNAI TO BAHRAIN

FLIGHT GF 69

BOARDING GATE CLASS SEAT SEATING

03:30 GATE Y 15A ZONE 2

23 DEC 2023

SHEKH/MAHAMMADT

MAA-BAH 23DEC2023 GF 69

GF 3902724-25

GATE Y 15A ZONE 2

23 DEC 2023

072 6662283425 1

SEQ. 126

10.2.3.3 Negotiations with the commander and escape from training camp

Following this revelation, Tahir negotiated with Commander Alexander to avoid frontline deployment by offering him half of his monthly salary amounting to approximately RUB.1,00,000/. Additionally, upon learning about their potential deployment to Ukrainian territory, Tahir, along with friends Suresh and Praveen, offered the commander an immediate payment of RUB.100,000/- to avoid deployment. Exploiting the drunken state of the commander, Tahir managed to retrieve his passport and escape from the camp, eventually seeking assistance from a YouTuber named Raja Pathan to facilitate his return to India.

10.2.3.4 Tragic Events and Victims: Connecting Case Studies 1 and 2

During his stay, Tahir witnessed tragic events including the death of Hamil in a drone attack and Asfan due to lack of medical treatment for bullet injuries sustained during combat. Sameer, Iliyas, and Sufyan were also involved in a fatal incident while performing woodcutting and trench digging duties. These incidents underscored the perilous and exploitative nature of the job offers and conditions faced by Tahir and other aspirants.

10.3 CBI Case and Advocacy Efforts

In response to these grave violations, a case was registered with the CBI to probe the trafficking of these individuals. On the 6th of March 2024, the CBI Special Crime-1 New Delhi registered vide RC. 048 2024 S 0005 U/S 120 B, 420, and 379 IPC, listed 19 persons as accused. The accused include Faisal Abdul Mutalib @ Baba (A-10), Mohammad Sufiyan Dawood Ahmad Darugar (A1), Baba Vlogs Overseas Recruitment Solutions Pvt. Ltd Thane (A12), Pooja W/o Md. Sufiyan (A13), Ramesh Kumar Palanisamy from Tamil Nadu (A-14), and Mohammed Moinuddin Chhipa from Rajasthan (A15).

Prajwala has supported the families by writing to the Ministry of External Affairs and voiced their concerns. Efforts by CBI and the diplomatic efforts of the Government have ensured that all the trapped Indians were removed from combat zones and kept in service zones.

10.4 Analysis of CEHT for War Recruitment: Insights, Challenges, and Solutions

Having examined the intricacies of CEHT through the detailed exploration of three case studies, we now transition into the analysis phase. In this section, we delve deeper into the insights from the case studies, identify the challenges and loopholes revealed, and propose practical solutions to address them. By critically analyzing the patterns and dynamics observed in the case studies, we aim to formulate comprehensive strategies to combat CEHT effectively.

10.4.1 Insights from the Case Studies

10.4.1.1 Recruitment Deception:

The case studies illustrate how individuals were misled by deceptive recruitment tactics. The victims were attracted by promises of lucrative jobs abroad, only to find themselves in hazardous situations with little recourse for help. Viral YouTube videos played a significant role in luring victims with false assurances of non-combat roles, high salaries, and legitimate work visas.

10.4.1.2 Role of Technology:

The viral YouTube video crafted by traffickers served as a powerful tool to entice individuals into the trafficking scheme. Through persuasive narration and enticing visuals, the video showcased false promises of lucrative employment opportunities in Russia. Specific details such as non-combat roles within the Russian Army, attractive salaries, and assurances of career advancement were highlighted to captivate the audience. Moreover, the video's viral nature ensured widespread exposure, reaching a vast audience of individuals seeking employment opportunities abroad. Its accessibility on platforms like YouTube made it easily shareable, amplifying its impact and increasing its reach. The communication thereafter was pursued on instant messaging applications such as WhatsApp.

10.4.1.3 Exploitation of Vulnerabilities:

The case studies reveal how traffickers exploit the vulnerabilities of individuals seeking better opportunities abroad. In Case Study no. 2, four individuals from Karnataka, who had previously worked in a factory's packaging section in Dubai, were enticed by promises of better-paying jobs in Russia. Despite their prior employment in Dubai, they fell for the allure of higher salaries in Russia, only to find themselves trapped in exploitative situations along the Ukraine border. Similarly, Mohammed Asfan and Mohammad Tahir were deceived by promises of non-combat roles and high salaries, leading them to accept a job offer in Russia and unknowingly become involved in the conflict.

10.4.1.4 Deceptive Practices:

Traffickers employed deceptive tactics, including false promises of non-combat roles and legitimate work visas, to lure victims into the scheme. In both case studies, victims were assured of positions in Russia involving non-combat duties, such as cleaning work and security, to make the opportunity appear safe and lucrative. However, upon arrival, they were placed in dangerous situations along the Ukraine border, directly involved in military activities.

Additionally, traffickers provided falsified documents, including work visas, to deceive victims into believing they were entering lawful employment agreements. These documents were later revealed to be fraudulent, offering victims no legal protection.

10.4.1.5 Systemic Vulnerabilities:

These cases expose gaps in the recruitment process on a national and international level, resulting in individuals like Mohammed Asfan, Syed Iliyas Hussaini, Mohammad Sameer Ahmad, Abdul Nayeem, Mohammed Sufiyan, and Mohammed Tahir Rafeeq Bhai Shaik, falling prey to exploitative schemes. Vulnerabilities include inadequate monitoring, limited awareness among migrants, and few avenues for legal recourse.

10.4.1.6 Impact of Trafficking on Victims:

The case studies revealed the significant challenges faced by victims of trafficking and the complexities encountered in providing assistance. The victims in all cases experienced profound physical and psychological harm due to their exploitation. They endured coercion, violence, and forced labor, resulting in considerable trauma and distress. This loss of autonomy left them feeling vulnerable and powerless. Tragically, the trafficking resulted in the death of two victims.

10.4.1.7 Obstacles in assisting victims:

Access to crucial services and assistance was frequently hampered by legal and administrative obstacles. Their precarious legal status and fear of reprisals made it difficult to seek assistance. Language barriers and mistrust further hindered efforts to provide effective support. Moreover,

the transnational nature of trafficking complicated assistance efforts. Victims found themselves stranded in foreign countries without access to consular assistance. Navigating complex legal frameworks and bureaucratic procedures required coordination among multiple official stakeholders.

10.4.2 Loopholes Identified from Case Studies

10.4.2.1 Regulatory Oversight:

The lack of effective regulatory oversight to monitor and regulate online content related to employment opportunities abroad is a significant loophole. Traffickers exploited this gap by disseminating false information through online platforms without facing consequences. The absence of stringent regulations allows traffickers to operate with impunity, preying on vulnerable individuals seeking better opportunities abroad.

10.4.2.2 Verification Procedures:

Existing verification procedures for work visas and employment contracts were insufficient to detect fraudulent activities. Traffickers capitalized on these loopholes by providing falsified documents and misleading information to victims. In the case studies, victims were deceived by promises of legitimate employment opportunities in Russia, only to find themselves trapped in exploitative situations along the Ukraine border.

10.4.2.3 Limited Awareness:

Many individuals, particularly those from marginalized communities, lack awareness about the risks associated with overseas employment opportunities advertised online. The absence of comprehensive awareness campaigns and outreach programs leave such individuals susceptible to trafficking schemes. As seen in the case studies, victims were enticed by promises of lucrative salaries and non-combat roles in Russia, unaware of the deceptive nature of the offers.

10.4.3 Recommendations to fill in the loopholes

10.4.3.1 Strengthen International Cooperation:

There is an urgent need for international cooperation to deal with human trafficking cases related to transnational borders for the urgent redressal of human beings trapped in exploitative conditions in another country. Robust mechanism for early rescue and safe repatriation is at the core of victim friendly services that needs to be prioritised.

10.4.3.2 Enhanced Regulation:

Authorities must implement stricter regulations to monitor and regulate online advertisements and content related to overseas employment. This includes vetting and verifying the authenticity

of recruiters and job offers to prevent traffickers from exploiting loopholes. Regular audits and inspections of recruitment agencies and online platforms should be conducted to ensure compliance with regulatory standards.

10.4.3.3 Public Awareness Campaigns:

Government agencies and NGOs should launch comprehensive public awareness campaigns to educate individuals about the risks associated with accepting employment opportunities advertised online. These campaigns should emphasize the importance of verifying job offers, conducting due diligence, and recognizing the warning signs of trafficking. Targeted outreach efforts should be directed towards vulnerable communities, including marginalized groups and individuals with limited access to information.

10.4.3.4 Collaborative Efforts:

Governments, law enforcement agencies, NGOs, and technology companies must collaborate to combat CEHT effectively. This collaborative approach should involve sharing information, resources, and best practices to identify and disrupt trafficking networks operating online. Multi-stakeholder partnerships should be established to facilitate information exchange and coordination, with a focus on leveraging technology to prevent and combat trafficking. Additionally, platforms and tools should be developed to facilitate reporting mechanisms for individuals at risk or victims of trafficking to seek assistance and support.

Chapter

11

Cyber-Crimes and CEHT

Chapter 11

Cyber-Crimes and CEHT

11.1 Introduction

Interactions during the entire course of data collection with police officers from Cyber-Crime Police Station and AHTUs clearly showed a clear correlation between cyber-crimes and CEHT cases. Several examples shared by Cyber Inspectors indicated the probability of the cases being a human trafficking case. This chapter explores the potential of a cyber-crime to become a human trafficking case.

Initiating our examination of cyber-crime prevalence in India and its relation to CEHT, it is crucial to highlight the significant impact of these digital transgressions. In 2022, India experienced a notable upsurge in cyber-crimes compared to the previous year. According to the most recent data released by the NCRB in 2023, there was a 24 percent increase in cyber-crimes registered in 2022 compared to 2021, with a total of 65,893 cases reported under cyber-crime. Remarkably, the predominant motive behind the majority of cyber-crime cases registered in 2022 was fraud, followed closely by extortion, and instances of sexual exploitation. This surge mirrors a broader trend, as other categories of crime also experienced upticks, including economic offenses (11 percent), crimes against senior citizens (9 percent), and crimes against women (4 percent).[130]

These statistics emphasize the widespread occurrence of cyber-crimes and necessitate concerted efforts to address them comprehensively. The rise in cyber-crime instances, particularly those driven by fraudulent motives, highlights the urgent need for robust preventive measures and enforcement mechanisms to safeguard individuals and businesses from digital exploitation.

Insights gathered from interactions with law enforcement officers and relevant stakeholders across the 15 states of India reveal the multifaceted nature of cyber-crimes and their potential links to the escalation into human trafficking cases. From the use of online grooming methods to exerting coercive influence through digital channels, the avenues for exploitation are diverse and often subtle.

A thorough understanding of the cyber-crime landscape reveals that financial fraud and exploitation, particularly targeting vulnerable demographics such as women and girls, are significant aspects of this digital realm. From the misuse of personal data for illicit financial gain to the use of coercive tactics in sextortion schemes, cyber criminals adeptly exploit technology to take advantage of inherent vulnerabilities which is very similar to what happens during the process of

130 https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf

human trafficking. Furthermore, the anonymity provided by cyber space emboldens perpetrators, ranging from individual hackers to organized criminal groups, to operate with relative impunity.[131] This anonymity, combined with the global reach of digital platforms, presents significant challenges in detecting and prosecuting offenders. Within this context, our research effort seeks to explore the potential for these cyber-crimes to evolve into cases of human trafficking, elucidating the complex relationship between digital exploitation and the vulnerabilities it exploits. It's important to note that even in traditional cases of human trafficking it is the vulnerability of individuals that predators exploit.

11.2 Cyber-crime Trajectories and the Nexus with CEHT

During the FGDs the officers shared in detail some cyber-crimes which they felt had the risk of becoming a human trafficking case. These crimes which were mostly cyber financial frauds such as pig butchering, sextortion, honey trapping, loan app scams, and package fraud had the potential to render a victim completely helpless and corner the person to desperate circumstances.

These specific modus operandi in cyber-crimes were chosen based on their common occurrence, relevance, and their potential intersection with human trafficking from the perspective of CEHT. The examination criteria included analyzing the traffickers' characteristics, motivations, and modus operandi to anticipate their potential connections to human trafficking in the digital age.

Aspects like persistent exploitation, the existence of criminal networks, and the predator's vulnerability are vital to this analysis. These factors provide insights into how a cyber-crime, initially confined to the digital realm, possesses the potential to evolve into a more severe form of organized crime, encompassing elements of human trafficking.

11.2.1 Pig Butchering

a) Pig Butchering as a cyber-crime:

During the FGDs, the officers provided detailed insights into the workings of the pig butchering scam, revealing its deceptive tactics and harmful consequences. At its core, the pig butchering scam operates as a sophisticated modus operandi orchestrated by faceless, organized groups targeting vulnerable individuals, primarily through popular messaging platforms like WhatsApp and Telegram.[132] The scheme begins innocuously, with perpetrators enticing victims with promises of easy money in exchange for simple online tasks, such as liking, reviewing, or sharing links to Google Play Store or YouTube videos.

As victims comply with these tasks, they are rewarded with nominal payments, typically ranging from ₹250/- to 300/- (USD 3 to 4), credited to their bank accounts. Encouraged by the initial success, victims continue to engage in similar activities, earning slightly higher amounts with each task completed. However, the scheme escalates as perpetrators pressure victims

131 https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html

132 Andhra Pradesh FGD on CEHT, Conducted on January 03, 2024, in Vijayawada.

into investing large sums of money for supposedly higher returns, under the guise of lucrative investment opportunities.

During the briefing by officers in Andhra Pradesh, an incident was described involving the exploitation of young village boys through WhatsApp and Telegram.[133] The Officers shared details of how a group of scammers specifically targeted these vulnerable individuals, offering them the opportunity to earn money by simply liking and sharing a YouTube video.

In this particular case, the communication was primarily text-based, with the perpetrators gradually gaining the victims' trust by making small payments ranging from ₹200/- to 500/- (USD 2 to 6 approximately) multiple times. As victims grew more trusting of the scheme, the scammers escalated their offers, enticing them with investment schemes promising higher returns. The victims were often pressured to deposit substantial sums of money, typically ranging from ₹20,000/- to 30,000/- (USD 239 to 359) with the promise of even greater profits. However, once the victims complied, and deposited the money, the scammers disappeared without a trace, leaving the young village boys deceived and financially drained.

Another illustrative case shared during the discussions with officers from Andhra Pradesh pertained to a lower middle-class family based in Vijayawada. The family, consisting of an illiterate father and a literate daughter, operated an eatery generating up to ₹40,000/- (USD 479) per day. Notably, it was primarily the daughter who maintained the income. However, financial difficulties arose, prompting the family to request the daughter to withdraw funds from their account. To their surprise, the account was found empty.

Further investigation revealed that the daughter (victim) had initially withdrawn ₹40,000/- to invest. Initially, she made small investments, but gradually increased her stakes over time. Unfortunately, her investments resulted in significant losses, leading her to utilize the daily earnings from the eatery to continue investing.

As her debts reached ₹12 lakh (USD 14,398), the victim felt overwhelmed by guilt and shame. Desperate to find a way out, she was willing to do anything to settle her debts. Exploiting her situation, the perpetrators insisted she travel to different cities for contract prostitution to repay the interest which she resisted. Eventually, they forced her to agree to go to Hyderabad on a two days contract as an escort. It was then that she finally opened up to her family about what was happening.[134]

b) Profile of Perpetrators and Victims of Pig Butchering:

The officers outlined the profiles of both perpetrators and victims involved in pig butchering scams, underlining the stark power dynamics at play. Perpetrators, often operating as organized groups with sophisticated digital capabilities, exploit the vulnerabilities of their victims for financial gain. Victims, predominantly young individuals from economically disadvantaged backgrounds, are enticed by the allure of easy money and the promise of financial stability.[135]

---

133 Andhra Pradesh FGD on CEHT, Conducted on January 03, 2024, in Vijayawada.

134 Telangana FGD on CEHT, Conducted on November 7, 2023, in Hyderabad.

135 Madhya Pradesh FGD on CEHT, Conducted on January 5, 2024, in Bhopal.

Perpetrators employ manipulative tactics, leveraging victims' financial desperation and lure of easy gains to ensnare them in the scheme. Victims, lacking the resources or knowledge to discern the legitimacy of the scheme, become unwitting participants in their own exploitation.

c) Pig Butchering and CEHT:

The pig butchering scam, a method used in cyber-crime, with its focus on exploiting vulnerable individuals for financial gain, presents a clear pathway for its potential to become a CEHT case due to several key factors. Firstly, the perpetrators specifically target vulnerable individuals, exploiting their economic circumstances, lack of education, or limited opportunities. Secondly, by enticing victims with the promise of quick and easy money, they capitalize on their ignorance of the risks associated with online engagement. This initial vulnerability makes victims susceptible to further exploitation and coercion, mirroring the tactics employed by traffickers in recruiting individuals into trafficking situations.

Initially, baited with promises of quick and easy money, the victims gradually find themselves drawn deeper into the scam as they suffer financial losses and accrue mounting debts. Finally, the perpetrators exploit this desperation, offering false assurance of debt relief or financial stability in exchange for compliance with their demands. This financial coercion creates a sense of dependency on the perpetrators, eroding the victims' confidence and leaving them susceptible to further exploitation.

Furthermore, in cases like the one in Andhra Pradesh, where the young girl engaged in pig butchering investments to support her family secretly, the deeper she became involved, the harder it became for her to confide in others due to fear of repercussions. This highlights how victims, initially drawn in by promises of support or financial gain, can become increasingly isolated and dependent on perpetrators. Perpetrators groom victims by gradually building trust and rapport, further enhancing the victims' reliance on them for guidance and support. As perpetrators gain control over victims' perceptions and behaviours, they create conditions conducive to continued exploitation.

As victims become increasingly isolated from their families and support networks, maintaining secrecy about their activities out of fear and shame, they become more dependent on the perpetrators for validation and direction. This isolation and dependency creates a conducive environment for the perpetrators to exert greater control over the victims, potentially leading to their involvement in more serious forms of exploitation, including human trafficking. In the case of the young woman from Andhra Pradesh, she was being coerced into sex trafficking as means of clearing her debts.

In many cases, the victims of cyber-enabled crimes can also be driven to become perpetrators themselves out of desperation. As their financial situation worsens, and they find themselves trapped in a cycle of exploitation, victims may be compelled to engage in illicit activities themselves. This could involve luring others into similar schemes or participating in other criminal activities to alleviate their own financial burdens. The perpetrators may exploit this vulnerability, coercing victims into perpetuating crimes under the guise of debt repayment or financial restitution.

Officers in Odisha narrated cases where Telegram groups were used to lure victims into liking and commenting on travel-related google content. Within these Telegram groups, fabricated payment screenshots were posted by other criminals to deceive victims.[136] These tactics aimed to build trust, and convince victims to invest more in the modus operandi, promising to double their earnings. In the end, victims found themselves in large debts and were compelled to join the scammer groups.

In essence, the progression from cyber-crime victims to potential victims of CEHT is driven by financial coercion, emotional manipulation, and isolation from support networks. Perpetrators exploit vulnerabilities and desperation to gain control over victims, leading them down a path of increasing dependency and susceptibility. The victim's confidence diminishes as they become trapped in the cyber-crime scheme, leaving them vulnerable to additional exploitation, including CEHT.

11.2.2 Honey Trapping

a) Honey Trapping Scams as a cyber-crime:

Across the country in several states the officers provided insights into the practice of honey trapping in cyber-crime. It involves using seduction to ensnare young and middle-aged men for ulterior motives. Perpetrators, often working in organized groups, use seduction and deception to target affluent, educated males aged between 30 to 50 years.[137] Instances related to national security have been reported, where men in the defense force were honey trapped into revealing national secrets. In cyber space, the manifestations and purposes of honey trapping have diversified.

In this form of cyber-crime, perpetrators, often using a female persona, initiate video calls on messaging apps like WhatsApp or Telegram. During these calls, they employ various tactics, including pre-recorded or live-streamed videos of a female undressing or engaging in explicit activities.[138] The objective is to entice and manipulate male victims into compromising situations, ultimately recording the encounters to extort money or sensitive information such as state secrets.[139]

The officers in Madhya Pradesh, India, shared a case involving a male victim in a honey trapping situation.[140] The victim, a 35-year-old educated, wealthy man was randomly contacted by a woman on WhatsApp. Posing as an attractive woman, a video call was initiated with the man. The woman stripped naked during the call and recorded the interaction without the man's consent. Later, the woman used the compromising footage to blackmail the man, demanding a significant sum of money to prevent its public release. Fearful of the potential reputational damage and personal embarrassment, the man complied with the woman's demands, resulting in substantial financial loss and emotional distress.

---

136 Odisha FGD on CEHT, Conducted on December 26, 2023, in Bhubaneswar.

137 Punjab FGD on CEHT, Conducted on February 5, 2024, in Chandigarh.

138 Maharashtra FGD on CEHT, Conducted on February 15, 2024, in Mumbai.

139 Gujarat FGD on CEHT, Conducted on February 14, 2024, in Gandhinagar.

140 Madhya Pradesh FGD on CEHT, Conducted on January 5, 2024, in Bhopal

b) Profile of Perpetrators and Victims of Honey Trapping:

The officers highlighted that victims targeted in honey trapping cyber-crimes are often affluent, educated males aged between 30 to 50 years of age.[141] These individuals may hold positions of authority, possess valuable assets, or have access to sensitive information, making them lucrative targets for exploitation. Perpetrators specifically target these individuals due to their perceived financial stability and potential access to valuable resources.

On the other hand, Officers stated that the front-end perpetrators of honey trapping cyber-crimes are often women who are part of organized groups or individuals with sophisticated digital capabilities.[142] They possess a deep understanding of human psychology and leverage this knowledge to manipulate victims for personal gain, in several cases morphing technology is also used to manipulate visual content.

c) Honey Trapping and CEHT:

The potential intersection between honey trapping cyber-crimes and CEHT is a deeply concerning aspect that merits thorough exploration. During the briefing by the officers in Gujarat, India, it was revealed that instances of honey trapping had targeted members of the armed forces, aiming to extract details of national secrets and financial gains.[143]

Unlike other cyber-crimes, honey trapping predominantly exploits sexual vulnerabilities and often targets affluent, educated men aged between 30 to 50 years of age. Perpetrators, often utilizing false identities and seductive tactics, lure male victims into compromising situations, such as engaging in explicit video calls or sharing intimate photographs. This is similar to the case in Madhya Pradesh, India, where the perpetrator trapped the victim by posing nude on a video call and recorded the video to blackmail the 35-year-old man.[144] The psychological manipulation inflicted upon these victims can be profound, leaving them emotionally vulnerable and susceptible to further exploitation.

Given that honey trapping primarily targets affluent, educated men, perpetrators exploit their financial stability and access to resources to extract financial gain or other favors. However, the manipulation and coercion inherent in honey trapping create conditions ripe for further exploitation, including trafficking. Perpetrators collect incriminating material evidence, such as recorded videos and images, during the honey trapping process, which can be used to coerce the victims into extortion or committing other forms of crimes, such as cyber scamming or recruiting for sexual exploitation. Victims may undertake various actions in a bid to safeguard their reputation, pay off extorted amounts, or end up blackmailing others.

Moreover, the sexual nature of honey trapping cyber-crimes creates opportunities for perpetrators to engage in activities directly linked to human trafficking by way of coercing the victims into engaging in activities that facilitate or contribute to trafficking operations, such as

141 Madhya Pradesh FGD on CEHT, Conducted on January 5, 2024, in Bhopal.

142 Goa FGD on CEHT, Conducted on January 30, 2024, in Goa.

143 Gujarat FGD on CEHT, Conducted on February 14, 2024, in Gandhinagar.

144 Madhya Pradesh FGD on CEHT, Conducted on January 5, 2024, in Bhopal

recruitment, grooming, or exploitation. The victims, manipulated and coerced by the perpetrators, may become unwitting accomplices in trafficking crimes, perpetuating a cycle of exploitation and victimization.

11.2.3 Sextortion

a) Sextortion in Cyber-crimes:

Sextortion has been used maliciously in several cyber-crimes and involves the coercion or blackmail of individuals using intimate or sexually explicit material, such as photos or videos. Perpetrators typically obtain these materials through deceptive means, such as posing as a romantic partner or manipulating victims into sharing sensitive content. Once in possession of the material, perpetrators use it to extort money or other favors from the victims under the threat of exposure.[145] This form has been reported practically across all the 15 states.

Sextortion exploits the intimate trust shared between individuals in romantic or sexual relationships, leveraging this vulnerability for financial gain or other malicious purposes. The officers across the country shared that victims of sextortion often experience profound feelings of shame, guilt, and fear, as their privacy and dignity are violated by perpetrators seeking to exploit their vulnerabilities for personal gain.[146]

The officers from Gujarat, India, recounted a case of sextortion involving an elderly victim. The victim, a lonely 75-year-old senior citizen from a middle-class family was lured through a Facebook account. Initially contacted by someone posing as a lady, the victim engaged in nude video calls, unaware of the crime unfolding. As the calls progressed, the scammer coerced the victim into undressing and participating in explicit activities, which were recorded without his knowledge. Subsequently, the man was threatened, and a demand for ransom in exchange for not releasing the compromising videos was made. Despite paying a substantial amount—approximately ₹1.5 crore which is equivalent to USD 1,79,989 the victim continued to face extortion demands. Overwhelmed by the relentless demands, the victim sought help from the police. The police promptly registered the case that led to the arrest of one of the accused, and the recovery of some of the extorted amount.[147]

Similarly, Officers from Kerala recounted an incident involving a victim from Thrissur who lodged a complaint. The victim had been involved in a relationship with a boy, who subsequently recorded videos of their sexual encounters. The accused then shared these videos on Telegram and sold them for ₹50/- each. A case was filed against the accused under Section 69 of the IT Act.[148]

b) Profiles of Victims and Perpetrators of Sextortion:

Interaction with the officers revealed that victims of sextortion typically fall within the

145 Rajasthan FGD on CEHT, Conducted on February 12, 2024, in Jaipur.

146 Telangana FGD on CEHT, Conducted on November 7, 2023, in Hyderabad.

147 Gujarat FGD on CEHT, Conducted on February 14, 2024, in Gandhinagar.

148 Kerala FGD on CEHT, Conducted on December 28, 2023, in Thiruvananthapuram.

demographic of young women aged between 18 to 30 years, although individuals of any gender or age may also be targeted. Additionally, it was noted that individuals on the brink of marriage are often the primary targets for blackmail.[149]

Perpetrators, as described by the officers, are frequently former romantic partners or acquaintances who possess intimate material obtained through consensual or non-consensual means.[150]

In most instances, perpetrators leverage the threat of exposing intimate material to coerce victims into compliance with their demands for money or other favours.[151] Sextortion tactics commonly involve revenge pornography, and at times the use of morphed images. This manipulative behaviour establishes a power dynamic in which perpetrators exert control over their victims, exploiting their vulnerabilities and inflicting fear and desperation.

c) Sextortion and CEHT:

The link between sextortion used in cyber-crimes and CEHT exposes a troubling path where the victims can be forced into commercial sexual exploitation or sex trafficking. Sextortion, using manipulation and coercion based on sexual vulnerabilities, threatens individuals, especially young women between the ages of 18 to 30 years. Perpetrators often exploit intimate material obtained through consensual or non-consensual means, leveraging the threat of exposure to coerce victims into compliance with their demands for money or other favors. In the case described by the officers in Kerala, the video recorded during consensual sexual encounters was circulated without consent and monetized by the accused.[152]

The emotional and psychological trauma inflicted upon victims of sextortion can render them more susceptible to manipulation and coercion by traffickers. This vulnerability creates conditions conducive for exploitation, leading victims to further victimization and potential involvement in trafficking activities. The officers from West Bengal shared details of a case involving a female employee of ICICI Bank and her colleague. The two coworkers had been in a romantic relationship for four years. It was later revealed that the colleague was married before their relationship began. When the woman discovered this, she tried to end the relationship. However, the colleague resorted to blackmail. He threatened to release intimate photos and videos they had taken together unless she complied with his financial demands.[153]

Sextortion in females can have particularly dire consequences, as victims may be pushed into prostitution, online adult sexual services such as phone sex or video sex chat, or even coerced into registering fake rape cases for extortion purposes. Additionally, victims may become perpetrators themselves, perpetuating prostitution and luring or recruiting other victims. Many victims now sheltered in the Prajwala Safe Home were coerced into prostitution by the means of sextortion. The situation becomes even more disturbing when the content is disseminated through various social

149 Jharkhand FGD on CEHT, Conducted on January 8, 2024, in Ranchi.

150 Bihar FGD on CEHT, Conducted on February 1, 2024, in Patna.

151 West Bengal FGD on CEHT, Conducted on January 24, 2024, in Kolkata.

152 Kerala FGD on CEHT, Conducted on December 28, 2023, in Thiruvananthapuram.

153 West Bengal FGD on CEHT, Conducted on January 24, 2024, in Kolkata.

media platforms, messaging apps or posted on adult sexual services sites creating a permanent content and inflicting irreversible trauma for the victims.

Perpetrators of sextortion often use the threat of exposing intimate material to coerce victims into complying with their demands, whether for money, sexual favors, or other forms of exploitation. This manipulation empowers perpetrators to wield control over their victims' lives. Furthermore, the emotional and psychological trauma inflicted upon victims of sextortion can render them more susceptible to manipulation and coercion by traffickers. Victims, grappling with feelings of shame, guilt, and fear, may be coerced into engaging in activities that facilitate or contribute to trafficking operations, such as recruitment, grooming, or exploitation.

11.2.4 Package Frauds

a) Package Frauds a new form of Cyber-crime:

A new form of cyber-crime shared by the officers from the 15 states is what they call 'package frauds', which represents a deceptive tactic wherein, perpetrators exploit the trust and goodwill of individuals, particularly on platforms such as matrimonial sites like Shaadi.com or social media platforms like Facebook.[154] The officers stated that perpetrators, often operating under false identities or using fake accounts, befriend victims and establish a sense of trust and emotional connection.[155] Once trust is established, perpetrators feign sending gifts to their victims, claiming that the packages are held up in customs and require payment for clearance. However, these purported gifts are non-existent, and perpetrators use this ruse as a pretext to extort money from their victims. Victims, unsuspecting and eager to assist their supposed loved ones, fall prey to this deception and willingly pay the requested customs fees.

The officers further elaborated that the methods employed by perpetrators in package frauds often involve the use of fake URLs, fraudulent credit card numbers, fake IVRS or other deceptive means to extract money from victims.[156] These fraudulent activities can result in significant financial losses, with victims sometimes losing lakhs of rupees to these elaborate scams.

The officers from Assam shared a case involving a young girl who had fallen victim to an online scam. According to their report, the victim, an active Facebook user, met a person posing as a soldier in the American Army. Very quickly this man was able to groom the victim in a romantic relationship. This individual, over time, expressed a desire to leave the army and settle in India, discussing plans to bring his pension income. Eventually, he claimed to have sent a gift to the girl, leading her to receive a call from a woman posing as a custom official, asking for money to clear the supposed gift. The girl's parents discovered a payment of ₹1 lakh from their account had been made, prompting them to report the incident to the police. Investigation revealed that the accused only communicated with the victim through text and voice messages on Facebook, with no live voice calls. Further inquiry uncovered that the accused's bank account was associated with an individual from Manipur.[157]

---

154 Kerala FGD on CEHT, Conducted on December 28, 2023, in Thiruvananthapuram.

155 Meghalaya FGD on CEHT, Conducted on February 7, 2024, in Shillong.

156 Punjab FGD on CEHT, Conducted on February 5, 2024, in Chandigarh.

157 Assam FGD on CEHT, Conducted on January 18, 2024, in Guwahati.

The officers from Maharashtra recounted a case involving a 27-year-old female software engineer from Nashik who was deceived through a fake profile on Jeevansathi.com, a matrimonial website. The accused, pretending to reside outside India, proposed marriage to the victim and communicated via WhatsApp.[158] Claiming to have sent a gift stuck at customs, the accused orchestrated a scam involving a fake customs officer who used voice-changing technology to dupe the victim. Consequently, the victim lost 15 lakhs to the accused and his accomplice.

b) Profile of Victims and Perpetrators of Package Frauds:

Officers described the victims of package frauds as typically individuals in the age range of 21-40 years, both male and female, who are financially stable. These victims may be seeking companionship or relationships on matrimonial or social media platforms, making them vulnerable to exploitation by perpetrators posing as potential romantic partners or friends.[159]

Perpetrators of package frauds were described by the officers as varying in their demographics, ranging from individuals operating independently to highly organized gangs orchestrating elaborate schemes. They often exploit the anonymity and reach of online platforms to create fake identities and establish trust with their victims. Officers further explained that perpetrators possess sophisticated digital skills and knowledge of online deception techniques using sophisticated technologies including IVR and voice morphing, allowing them to carry out these fraudulent activities with impunity.[160]

c) Package Frauds and CEHT:

Package frauds extend beyond financial deception, posing risks that intersect with CEHT. Victims, emotionally ensnared and financially drained, become vulnerable to exploitation and manipulation, potentially leading to trafficking situations.

Perpetrators of package frauds employ sophisticated deception tactics to exploit the trust and emotional vulnerability of their victims. By posing as potential romantic partners, perpetrators establish intimate connections with victims, fostering a sense of emotional dependence and reliance. Victims, eager to reciprocate affection and trust, willingly comply with perpetrators' requests for financial assistance, unaware of the elaborate deception at play.

The financial losses incurred by victims of package frauds can be staggering, with perpetrators extracting significant sums of money under false pretences. These losses not only undermine victims' financial stability but also exacerbate their vulnerability to further exploitation. Perpetrators, recognizing the financial hardship and desperation of their victims, may exploit their precarious situation to coerce them into engaging in activities that facilitate or contribute to trafficking operations.

Moreover, package frauds often carry a heavy emotional toll on victims, with feelings of shame,

158 Maharashtra FGD on CEHT, Conducted on February 15, 2024, in Mumbai.

159 Maharashtra FGD on CEHT, Conducted on February 15, 2024, in Mumbai.

160 Maharashtra FGD on CEHT, Conducted on February 15, 2024, in Mumbai.

guilt, and betrayal accompanying the realization that they have been deceived. Perpetrators leverage this emotional manipulation to maintain control over their victims, using shame and fear as tools of coercion. Victims, grappling with the stigma and embarrassment associated with falling victim to fraud, may feel isolated and helpless, making them susceptible to further exploitation by traffickers seeking to exploit their vulnerabilities for profit or other nefarious purposes.

The intersection between package frauds and CEHT is particularly concerning due to the targeting of victims' respectability and reputation. Victims of package frauds, given their standing in the community, are individuals whose public image is of paramount importance to them. Perpetrators may threaten to tarnish victims' reputation or blackmail them into funding illicit activities, such as commercial sexual exploitation. In some cases, the victims may even be coerced into becoming perpetrators themselves, further perpetuating the cycle of exploitation and victimization.

Furthermore, the digital dimension of package frauds opens up new avenues for exploitation in the cyber realm. Perpetrators may use online platforms and social media to recruit and groom victims for trafficking, exploit compromised personal information for identity theft or online extortion, and coerce victims into participating in online financial schemes or cyber scams. Victims of package frauds, already vulnerable and traumatized by their experiences, may find themselves further ensnared in a web of cyber-enabled exploitation, perpetuating the cycle of victimization in the digital age.

11.2.5 Loan App Scams

a) Loan App Scams as a cyber-crime:

Loan app scams have emerged as a serious cyber-crime issue, preying on vulnerable individuals facing financial instability and economic hardship. These scams are orchestrated by organized malicious groups who exploit the digital realm to trap unsuspecting victims in a web of deceit and financial ruin. It's important to note that all loan apps involved in these schemes are fraudulent. They exploit people's debts, similar to traditional human traffickers, but with higher interest rates and added risks like public shame and sextortion, often targeting middle-income earners. The alarming trend of suicides among victims highlights the desperation and vulnerability induced by debt. Scammers from these apps use threats and intimidation, making people more susceptible to exploitation. Therefore, it's crucial to investigate them closely in the context of human trafficking.

The MO of these scams involves the creation and dissemination of very authentic looking loan apps, strategically designed to appeal to individuals in desperate need of immediate cash assistance. These apps often promise quick and hassle-free loans, targeting individuals at one end from marginalized communities who lack access to traditional banking services or formal financial institutions,[161] and at the other end from middle income families who are facing sudden financial hardships like those observed during the Covid-19 pandemic. The apps are designed in such a manner that allures the potential victim to accept all conditions without checking the content, inadvertently giving access to both contacts and gallery of the device.

161 Andhra Pradesh FGD on CEHT, Conducted on January 03, 2024, in Vijayawada.

Once the victim downloads these deceptive loan apps, they are subjected to predatory terms and conditions, including exorbitant interest rates and unrealistic repayment terms. Victims, already burdened by financial strain, find themselves trapped in a cycle of debt from which escape seems impossible. The call centers associated with these scams employ aggressive debt collection tactics, including harassment, threats, and intimidation, to coerce victims into repaying the loans.[162]

What distinguishes these scams, as detailed by the officers, is the ruthless exploitation of vulnerability and desperation. Perpetrators capitalize on the dire financial circumstances faced by their victims, manipulating their desperation for financial relief to extract money through deceitful means.[163] Victims, deceived by the promise of quick cash, unwittingly fall into the clutches of these scam operators, only to find themselves trapped in a downward spiral of debt and despair.

The devastating consequences of loan app scams are highlighted by the tragic stories recounted by the officers, wherein individuals driven to the brink of despair have resorted to extreme measures, including suicide, as a means of escaping the overwhelming debt burden imposed upon them.[164]

The Loan Application Scamming Case, as narrated by the officers of Maharashtra, uncovered a sophisticated operation conducted by an organized gang.[165] Victims from diverse backgrounds, including individuals facing financial struggles or in urgent need of money were targeted through instant loan apps available on the Google Play Store. As per the officers' accounts, the gang enticed victims with promises of easy loans, transferring small amounts of money along with hefty interest and charges.

Exploiting victims further, the criminals accessed their contacts and photo galleries, using manipulated images and videos to extort them. Victims endured relentless mental and verbal abuse, not only directed at them but also at their associates and relatives. This coercion often led victims to seek more loans, exacerbating their already dire financial situation. The severity of the case came to light when one victim tragically took his own life due to the distress caused by the harassment.

During the investigation, the officers discovered a complex network with ties to criminal elements in China. While operatives on the ground were based in India, the masterminds operated from abroad. Working in tandem, law enforcement authorities conducted raids across multiple locations, including Bengaluru, Gurgaon, Andhra Pradesh, and Uttarakhand, resulting in the arrest of 14 individuals involved in the scam.

Utilizing forensic techniques such as tracing the money trail and analyzing Call Detail Records (CDR) and metadata, the officers gathered crucial evidence to build their case. Furthermore, a substantial amount of illicit funds was successfully blocked by the police, preventing further financial losses.

Similarly, officers from Vijayawada shared a trend where students were relying on loan apps to

162 Kerala FGD on CEHT, Conducted on December 28, 2023, in Thiruvananthapuram.

163 Odisha FGD on CEHT, Conducted on December 26, 2023, in Bhubaneswar.

164 Maharashtra FGD on CEHT, Conducted on February 15, 2024, in Mumbai.

165 Maharashtra FGD on CEHT, Conducted on February 15, 2024, in Mumbai.

finance their expenses.[166] These apps would gain access to the victim's contact details and full call records. Subsequently, the perpetrators, who were either the owners of these apps or individuals employed by the main developers, would exploit this information to send morphed photos and false criminal allegations about the victims to all their contacts. Even if the students turned off their phones or removed their SIM cards, the perpetrators continued to victimize them in this manner by connecting to all their contacts.

b) Profile of Victims and Perpetrators of Loan App Scams:

The officers highlighted that victims targeted by loan app scams could be from marginalized communities, both male and female, who lack stable economic conditions and face dire financial circumstances or from middle income families who are facing sudden financial loss. These vulnerable individuals, struggling to find financial solutions to survive are enticed by the promise of quick cash provided by these fraudulent loan apps.[167]

The officers further elaborated that the perpetrator of loan app scams, often organized malicious groups operating behind the façade of legitimate businesses, exploit the desperation and vulnerability of their victims for financial gain. They design deceptive loan apps with predatory terms and aggressive debt collection practices, trapping victims in a cycle of debt from which escape seems impossible.[168]

c) Loan App Scams and CEHT:

The intersection of loan app scams with CEHT creates a complex landscape fraught with risks and vulnerabilities with financial exploitation using tactics like sextortion, extortion, and public shaming are frequently used to coerce compliance. This coercive environment not only compounds the financial burden on victims but also increases their susceptibility to trafficking activities.

Victims initially seek quick solutions to financial problems but end up trapped in a cycle of debt and manipulation. Perpetrators exploit their situation, using harassment, threats, and blackmail to extort more money. Loan app scams often combine coercion with aggressive debt collection and psychological manipulation. The victims start with small loans but soon face escalating demands, making them vulnerable to be coerced into exploitative situations.

As victims sink deeper into financial despair, their emotional well-being also deteriorates. Feelings of shame, guilt, and hopelessness permeate their thoughts, rendering them even more susceptible to exploitation. In most cases the perpetrators connect with all the contacts on the victim's device with abusive messages triggering shame and humiliation among friends and relatives.

Interacting with the victims at the Prajwala Safe Home revealed the case of a woman who worked in an unaided school and who had lost her job during the Covid-19 pandemic. Her husband, a software engineer in a private firm had also lost his job and had taken a loan from an instant loan

166 Andhra Pradesh FGD on CEHT, Conducted on January 03, 2024, in Vijayawada.

167 Bihar FGD on CEHT, Conducted on February 1, 2024, in Patna.

168 Telangana FGD on CEHT, Conducted on November 7, 2023, in Hyderabad.

app to manage the financial crisis. With prolonged lockdown, and no financial resources in hand, the man was unable to pay back the interest and was harassed by the recovery agents. Soon his morphed images were circulated to all the contacts on his device with derogatory messages.

While the husband struggled with this public humiliation and became suicidal, the woman started receiving messages on her phone about the availability of jobs that would not require any educational qualifications and the option to receive an advance on humanitarian considerations. Desperate for any financial opening, the woman with the consent of her husband walked straight into the trap laid by the traffickers who coerced her into prostitution. Accepting the small advance and the lack of financial alternatives pushed the woman into a helpless position to comply with the demands made by the traffickers who supplied her to private houses for prostitution. Eventually the woman was rescued but was unable to share the true facts as her family was being intimidated by the perpetrators. The arrest of the perpetrators in another crime that was publicly reported led to the victim to share her agony.

In another instance recounted by a police officer in Telangana, female victims of loan apps were coerced to work in a call center to harass and intimidate other debtors failing which they were threatened with public retribution. This is very similar to the modus operandi used in trafficking for online criminality/cyber scamming all such instances indicate the various methods adopted in cyber-crimes such as fake loan apps to coerce vulnerable men and women to other crime situations including human trafficking.

11.3 Insights from Analysis of the selected cyber-crimes

Cyber-crimes in general have the potential to branch out to several other crimes including organized crimes like human trafficking. The following are the insights gained from closely studying some cyber-crimes and their relation to CEHT.

a) The organized nature of most cyber-crimes is similar to the organized set up of human traffickers who prey on human vulnerabilities.

b) While the primary objective for all cyber-crimes is financial, when it uses certain methods such as sextortion and public humiliation, the potential to coerce a human being to other forms of exploitation that will continue to raise revenue such as CSE is very high.

c) The nature of the cyber-crime is to minimize detection. Using regressive tactics to take control of a human being and then coerce them to commit other crimes has been the main tactic used that has also been extended to compel persons to act in support of human trafficking, thus ensuring the main criminal is never apprehended, and the criminalized victims are fixed for the crime.

d) CEHT can be facilitated online and consequently moves on to the physical realm. The need to have layers of online operations which will distract an investigating agency makes the synergy between these two crimes more real sometimes with the same persons involved.

e) Cyber-crimes targeting women and girls very often corner the victims into desperate situations that makes them vulnerable and easily manipulated for either further

victimization or to work in support of a crime such as luring another victim with false promises of a job or marriage.

f) Human trafficking syndicates are spread over the entire cyber space in constant move to spot a vulnerable person and so are the cyber criminals; the possibility and potential for converged operations are high.

g) Trafficked individuals are not only victims, but also coerced into committing cyber -crimes. Our research, based on information from officers, revealed that traffickers exploit victims' vulnerabilities to involve them in online criminality. Cyber scams like job scams, online betting, lottery scams, and fake loan apps are examples of crimes trafficked persons are coerced to commit. These individuals, already trapped in trafficking networks, are forced into online fraudulent activities under threat of violence and further exploitation.

In essence, the progression from cyber-crime victims to potential victims or perpetrators of human trafficking is driven by financial coercion, emotional manipulation, and isolation from support networks. Perpetrators exploit vulnerabilities and desperation to gain control over victims, leading them down a path of increasing dependency and susceptibility. As victims become trapped in cyber-crime, their confidence diminishes, rendering them vulnerable to further exploitation such as CEHT.

As we confront the complexities of cyber-enabled exploitation, it is imperative that we adopt a multi-faceted approach that addresses the root causes of vulnerability and provides robust support systems for victims. By understanding the nexus between cyber-crimes and human trafficking, we can develop targeted interventions to disrupt trafficking networks, support victims, and prevent further exploitation in this digital age.

Chapter

12

Legal and Institutional Framework

Chapter 12

Legal and Institutional Framework

Having delved deep into the various facets of CEHT in our preceding chapters, our next step is to probe into the legal and institutional preparedness in the country to address this problem. Mapping the institutional strengths and gaps will pave way for a clearer strategy to leverage existing mechanisms and design a more nuanced framework for future requirements. This is also a critical component in developing a National Plan of Action (NPoA) to combat CEHT as it will throw light on existing possibilities within the system to immediately address the problem.

In this chapter, we will examine the legal and institutional framework, and present an overview of the manner in which these structures work while looking at the gaps.

12.1 Institutional Framework

One of the strongest features of governance in India is the unique federal structure originating from the Constitution of India. In addition to the federal structure there is the clear division of responsibilities of the Legislature, Executive, and the Judiciary.

The Constitution of India[169] sets out a schedule clearly earmarking the responsibilities of the State governments and the Central government with the State List and the Central List. Some functions that are identified with overlapping jurisdictions feature in the Concurrent List. The Lists are a part of the Constitution for a clear distribution of responsibility for legislating, making policies, allocating resources, etc. The primary responsibility for tackling issues such as human trafficking lies with the State Governments. "Criminal laws" and "Criminal procedures" are items which are enumerated in the Concurrent List that means the competence to legislate lies both with the Center as well as the State Governments. However given the extent, magnitude, intensity, and the evolving nature of human trafficking, the Central Government has taken a proactive role whereby it provides for the institutional scaffold and framework under which human trafficking can be tackled. This ranges from enacting legislations, creating infrastructure, issuing advisories, allocating resources, engaging with global agencies, enhancing capacity of local resources, and setting up safe spaces for the trafficked. There are many schemes and policies of the Central government which are executed in partnership with the State governments.

169 7th Schedule the subject of "public order" and "police" are enumerated in List II i.e. the state list

12.1.1 Relevant Ministries of the Central Government:

A. Ministry Of Home Affairs

The Home Ministry is primarily responsible for the management of borders, internal security, administration of Union Territories, management of Central Armed Police Forces, etc. The Women Safety Division, which is one of the many divisions in the Ministry, includes the Anti-Trafficking Cell. This Cell is the main command and operation center which handles and looks after all matters pertaining to Trafficking in Persons and Smuggling of Migrants as well as the two United Nations Protocols, the Trafficking in Persons Protocol, and the Smuggling of Migrants Protocol. This Cell is the nerve center of cooperation with other key ministries, officers of the various other states who are a part of their respective AHTUs, and calibrate the Central Government's response and coordination with the State governments. In addition to the efforts made at the national level, the Central Government aids the efforts of the States as well. It supports the States by giving the States financial assistance for setting up, operating, and maintaining AHTUs at District levels.

Some additional efforts undertaken by the Home Ministry to strengthen the institutional anti-trafficking framework are:

1. Ratification of multilateral treaties and signing of bilateral agreements to coordinate with international partner countries. The Government of India has also signed various memorandums with foreign governments. The goal of these memorandums is to prevent human trafficking in addition to ratification of the United Nations Convention on Transnational Organized Crime (UNCTOC) protocol on Prevention, Suppression and Punishment of Trafficking in Persons, particularly Women and Children.

2. MHA since 2006 has had an Anti-Trafficking Cell which acts as an interface with all Central Government agencies, departments and ministries. In addition to this the MHA issues regular advisories to States and Union Territories for tackling human trafficking and regularly holding judicial colloquiums and state level conferences to sensitize officers at the State level.[170]

3. The Intelligence Bureau's Multi Agency Centre (MAC) has been created to facilitate swift information exchange among law enforcement entities. A parallel vision led to the creation of the Crime Multi Agency Centre (Cri-MAC) within the National Crime Records Bureau (NCRB). Cri-MAC operates 24x7 to ensure continuous online sharing of crime-related information and fostering seamless communication among LEAs. Its web-based application on the secured CCTNS network improves digital communication, expediting coordination for early detection and prevention of crime nationwide. Access to the Cri-MAC application is restricted to authenticated ICJS users, preventing public access through open networks. However its biggest advantage is swift cooperation among all law enforcement agencies.

4. Other bodies under the Home Ministry which work towards elimination of human trafficking:

170 https://www.mha.gov.in/sites/default/files/202212/humantrafficking_29092022%5B1%5D.pdf

a. National Investigation Agency

The National Investigating Agency (NIA) was set up vide the National Investigation Agency Act of 2008. The initial purpose for the creation of this body was counter terrorism investigation and issues pertaining to national security. Post the 2019 Amendment to the NIA Act, the agency has been empowered to investigate cases of human trafficking under Section 370 and 370A of the Indian Penal Code (Sections 143 and 144 of BNS).

b. Anti-Human Trafficking Units

In the year 2006, in partnership with the United Nations Office on Drugs and Crime, the Home Ministry had initiated the process of creation of AHTUs.These AHTUs were initially run as pilot projects in a few states. Over the period of time Home Ministry has established 696 AHTUs in 28 states and 8 union territories. The Units feature a multi-disciplinary support system and collaboration with relevant ministries to combat trafficking. Each state has a designated nodal officer, often a senior police official, with some states appointing multiple officers and establishing AHTUs. The Unit emphasizes ongoing capacity building through training, workshops, and judicial colloquiums. The Ministry facilitates regular meetings of nodal officers to enhance inter-state police cooperation, crucial for trafficking investigations, demonstrating sustained commitment through human and financial resources.

c. Bureau of Immigration

The Bureau of Immigration, an autonomous body under the Ministry of Home Affairs, oversees entry and exit regulations in India. The Foreigners Regional Registration Office (FRRO), a component of the Bureau, manages the registration, movement, stay, and departure of foreigners. The FRRO is responsible for recommending residence permit extensions and collaborates with the Ministry of External Affairs on visa issuance. Notably, FRRO issues exit permit documents to trafficking victims from other countries.

d. Bureau of Police Research and Development (BPR&D)

Established in 1970 under the Ministry of Home Affairs, the Bureau of Police Research and Development (BPR&D) aims to enhance the police force through technical support, systematic study of police challenges, and the application of science and technology. Evolving over time, BPR&D has taken on additional roles, such as addressing prison reform, providing police officer training, and conducting research on criminal justice issues in India, including trafficking.

e. National Crime Records Bureau

The National Crime Records Bureau (NCRB), operating under the Ministry of Home Affairs, serves as the central agency for collecting and analyzing crime data in India. It compiles information on criminal complaints, victims, case progress, prosecution status, and trial outcomes, generating an annual report titled “Crime in India.” NCRB’s latest 2022 report includes data on human trafficking.

NCRB is also the nodal agency to receive hash values from the NCMEC on Child Sexual Abuse Material (CSAM).

f. I4C

Indian Cybercrime Co-ordination Centre (I4C) was set up by the Ministry to provide a "framework and eco-system for law enforcement agencies for dealing with Cyber-crime in a coordinated and comprehensive manner".[171] This Centre is treated as the nodal point to curb cyber-crime in the country.

National Cyber-Crime Reporting Portal

Under the I4C, the Ministry launched cyber-crime.gov.in as a reporting portal for all cyber-crimes. The portal was launched following a direction by the Supreme Court in the case filed by Prajwala.[172] Initially launched to look at cases of CSAM and rape and gang rape videos, it has since expanded to address other cases as well. The Portal also encourages registration of complaints anonymously. Reports are forwarded to the concerned police stations for further action with options for tracking available on the portal.

B. Ministry of Personnel Public Grievances and Pensions:

Central Bureau of Investigation:

Under the Ministry of Personnel Pension and Public Grievances, the Central Bureau of Investigation (CBI) is the premier investigating agency of India. It was created under and operates within the mandate of the Delhi Special Police Establishment Act, 1946. The jurisdiction of the CBI is only to investigate cases in the Union Territories of India. However, with the permission of the State and the Central Government, it can be extended across the country. Over the years its mandate has expanded to investigate a variety of cases, including human trafficking and cyber-crimes on certain occasions.

CBI is the nodal police agency in India and coordinates investigation on behalf of Interpol Member Countries. In 2019, CBI had set up an, "Online Child Sexual Abuse and Exploitation (OCSAE) Prevention/Investigation Unit" to deal with cases relating to cases of CSAM. Besides collecting and disseminating information on CSAM online, the agency was to also take up cases relating to it. In 2022, the CBI conducted a massive pan India operation where its investigations led them to 56 locations across the country relating to CSAM.

During the course of the research, it was revealed that the agency had handled some critical cases relating to CEHT in a case of adoption and in a case of recruitment for armed conflict.

In March 2024, the CBI and Europol entered into a working arrangement to support the Member States of the European Union and Government of India in preventing and combating serious crime and terrorism including trafficking.

171 I4c.mha.gov.in

172 SMW (crl) No.3/2015; In re Prajwala

C. Ministry of Women and Child Development

Established as a separate Ministry in 2006, the Ministry of Women and Child Development (MWCD) was formerly under Ministry of Human Resources Development and addressed gaps in state actions for gender-equitable legislation and child-centered programs. Following a 1990 decision of the Supreme Court of India in Vishal Jeet vs Union of India,[173] MWCD formed a Central Advisory Committee on Trafficking in 1994, composed of state officials, civil society partners, police, and experts. The Committee, led by the Secretary of the Women and Child Department, evolved over time. In 1998, MWCD crafted a National Plan of Action (NPoA) to Combat Trafficking and Sexual Exploitation of Women and Children. As a pivotal agency, MWCD now plays a key role in formulating policies and schemes concerning the protection and development of women and children.

Some important schemes and initiatives under the aegis of MWCD are:

a) Ujjwala Scheme [174]

The MWCD Ujjwala scheme focuses on preventing and rehabilitating trafficking victims, employing measures such as community vigilance groups, and awareness programs. Funds are allocated to various stakeholders, ensuring a multi-level approach. Emphasis is placed on promoting victims' financial access by facilitating bank accounts. This comprehensive strategy aligns with academic discussions on human trafficking, reflecting the Ministry's commitment. The scheme addresses prevention, rescue, and long-term recovery, contributing to the broader discourse on combating human trafficking. The Scheme provides for setting up of two types of Homes for the rehabilitation and reintegration of the victims:

i. Protection & Rehabilitation Homes offer survivors institutional support, encompassing basic amenities, medical and legal aid, education, vocational training, and income generation skills

ii. Half-Way Homes empower gainfully employed victims, facilitating semi-independent living with minimal supervision, aiding their reintegration into the community with infrastructural support.

b) One Stop Centres

One Stop Centres (OSC) offer integrated support for women affected by violence, providing medical, legal, housing, and psychological assistance under the joint patronage of multiple ministries. They can be accessed by victims of trafficking as well.

c) Swadhar Greh

Swadhar Greh is an assistance program of the MWCD where it provides financial assistance to NGOs to run shelters for women in distress. The scheme's main objective[175] is to provide a transit shelter facility for any woman who finds herself in difficult circumstances and requires rehabilitation.

---

173 AIR 1990 SC 292

174 https://wcd.nic.in/sites/default/files/Ujjawala%20New%20Scheme.pdf

175 https://www.india.gov.in/spotlight/swadhar-greh-scheme

d) Support to Training and Employment Programme for Women (STEP) Scheme

The Ministry is administering 'Support to Training and Employment Programme for Women (STEP) Scheme' to provide skills that give employability to women and to provide competencies and skill that enable women to become self-employed/ entrepreneurs. This scheme, operational since the year 1986-87, provides support like a scholarship given directly to the institute that provides the training. The trainee-woman is given a transport allowance. The Scheme is intended to benefit women who are in the age group of 16 years and above across the country. The Scheme is administered through the NGO partners as well as the State Governments. Trafficked victims can also access the benefits of this Scheme.

e) Schemes for Children

1. National Plan of Action for Children: In 2016, the Ministry framed a National Plan of Action for Children.[176] This National plan includes addressing and preventing trafficking in persons. Some of its key focus areas are :-

- Ensure respect and sensitivity for all children without discrimination irrespective of factors of identity, gender, socioeconomic character, community or other status.
- Eliminate all forms of child labor till 14 years of age, and from hazardous industries till 15-18 years of age.
- Provide adequate and appropriate infrastructure and ensure safety and security of children in all residential care facilities including CCIs, Hostels and Ashram Shalas, established under domestic laws that house children.
- Undertake comprehensive fact-finding, research and analysis of data on child migration, all forms of child abuse, child trafficking, and all factors along with situations of vulnerability.
- Prevent crimes against children, especially sexual offenses and ensure prosecution of offenders.
- Ensure advocacy for public awareness, community vigilance and attentiveness to children's presence in every setting and situation such as neighbourhood, community, school, covering all public spaces and service points.
- Prevent child marriages.
- Prevent trafficking of children, take adequate measures for prevention, rescue and rehabilitation, re-integration of children and prosecution of traffickers.

2. Child Protection Services Scheme (previously known as Integrated Child Protection Scheme)

- Child Protection Services (CPS) operates under the Integrated Child Development Scheme (ICDS), offering preventive, statutory, and rehabilitation services to

176 National Plan of Action for Children, 2016, https://wcd.nic.in/sites/default/files/National%20Plan%20of%20Action%202016.pdf

vulnerable children. It provides financial support to State Governments and UT Administrations for service delivery through government bodies or NGOs, ensuring compliance with the Juvenile Justice (Care and Protection of Children) Act, 2015.

- Institutional Care Services under the CPS: During 2018-19, the Ministry has assisted 1511 Homes, 322 Specialized Adoption Agencies (SAAs) and 265 Open Shelters through State Governments/UT Administrations.
- Inspection and monitoring of CCIs: In order to ensure protection of children living in Child Care Institutions (CCIs), the Ministry has pursued with State/UTs Governments to conduct inspections and maintain the institutions in accordance with the vision of the JJ Model Rules, 2016. The Ministry has also advised the State Government to conduct background check of agencies managing CCIs and also ensure police verification of the staff. The Ministry has advised the States/UTs to take action for the welfare of children, in case of any eventuality while living in CCIs. Following the directions of the Supreme Court of India, the Ministry has consistently pursued with the States/UTs to ensure registration of all Child Care Institutions under the JJ act. So far, more than 8200 CCIs across the country have been registered under the JJ Act. 539 CCIs have been closed by the States/UTs after inspections on various grounds.

3. Child Helpline: The Child Helpline (1098) serves as a crucial component of the child protection system, covering approximately 65 percent of the country across 475 locations. Operating 24x7, this helpline is primarily facilitated by Childline India Foundation (CIF) and supports children in distress including cases of child trafficking.
4. Child Help Desks at Railway stations: The Ministry of WCD has framed Special Operating Procedures (SOPs) to be implemented with the help of Railways for rescue and rehabilitation of runaway, abandoned, kidnapped, trafficked children via railways. The Help Desks are set up at various railway stations for rescue and rehabilitation of such children.
5. Khoya-Paya: The Khoya-Paya portal developed by the Ministry of Women and Child Development and the Department of Electronics and Information Technology (DeitY) is a citizen based website which allows and facilitates the exchange information on missing and found children.

D. Ministry of External Affairs

The Ministry of External Affairs (MEA), serving as India's representative abroad, regulating emigration clearance through its overseas affairs wing, a critical measure in addressing Trafficking in Persons, particularly situations involving forced labor due to migration. Regulations mandate Emigration Clearance for Indian citizens below Grade 10 (those who have not completed basic schooling). In 2007, the Bureau of Immigration exempted individuals with valid non-employment visas to specified countries from seeking emigration clearance. The UAE, where a large number of skilled and unskilled workers migrate for employment is not among

the exempt nations. Directives and advisories issued by MEA, caution individuals with work permits about traffickers posing as employers or legitimate agents during travel.[177]

E. Ministry of Labor and Employment

The Ministry focuses on safeguarding workers' rights, developing schemes, policies, and legislation to prevent their compromise. It ensures social security and health services through the Employees' State Insurance Scheme (ESIC), extending beyond formal sector employees. The Ministry is committed to eliminating child labor, and introduced the Unorganised Workers Social Security Act, 2008, catering to the unorganized workers. Additionally, various beneficial schemes are implemented to support vulnerable workers, aligning with its overarching goal of worker protection and well-being which is extended also to labor trafficked persons.

F. Ministry of Electronics & Information Technology

Ministry of Electronics and Information Technology (MeitY) is responsible for implementing the Information Technology Act, 2000. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[178] regulate content on intermediary platforms. This Ministry is mandated to issue take down orders to various sites including the Internet Service Providers (ISPs) if the content is found to be violating any law. The Ministry also has a detailed protocol to issue these take down orders and ensure removal or disabling access to content especially harming minors under relevant sections and guidelines, including Measures to Curb Online CSAM.

12.2 Statutory Commissions

A. Human Rights Commission

Established in 1993 under the Protection of Human Rights Act, the National Human Rights Commission (NHRC) is an autonomous body in India with a Central and State structure. Chaired by a retired Supreme Court Judge, NHRC investigates, hears cases, conducts research, provides trainings, and issues recommendations, including ordering compensation. In collaboration with UNIFEM (now UN Women) and the Institute of Social Sciences, NHRC conducted a field research on Trafficking in Persons in 2004, releasing a comprehensive report. This is one of the most exhaustive pan-India action research on human trafficking to date in India.

B. Women's Commission

The National Commission for Women (NCW), a statutory body located in Delhi, focuses

177 The guidelines can be accessed through the official website www.mea.nic.in

178 The Guidelines Have Been Made Under Sub-Section (1), Clauses (Z) And (Zg) Of Sub-Section (2) Of Section 87 Of The Information Technology Act, 2000 (21 Of 2000), And In Supersession Of The Information Technology (Intermediaries Guidelines) Rules, 2011.

on women's rights, handles individual grievances, and conducts research projects, etc. The Commission, operating at the central level, also addresses issues like trafficking victims. As an advisory body, it collaborates with State Commissions established in each state through state-enacted statutes.

In 2018, the Commission launched "Digital Shakti" to support women on the digital aspects. The initiative works towards helping women report online abuse, access redressal mechanisms, understand data privacy, and use of technology for their benefit. It is a digital literacy and online safety program. Through the four phases of the campaign, over 4.5 lakh girls, women and netizens across the country have been sensitized with the aim to build resilience in online spaces.

C. Children's Commission

Established in 2005, the National Commission for Protection of Child Rights (NCPCR) is akin to the Women's Commissions, addressing children's issues, conducting research, training, and making recommendations to the government. Mandated by law, NCPCR monitors the implementation of the Protection of Children from Sexual Offences Act (POCSO) and, in compliance with the Supreme Court directives, conducts a social audit of all Child Care Institutions nationwide. The Commission plays a vital role in safeguarding children's rights and ensuring statutory compliance.

POCSO e-Box for Children suffering Sexual Abuse: To facilitate reporting of sexual abuse, especially when children may find it challenging to voice their concerns, the National Commission for Protection of Child Rights (NCPCR) offers an internet-based platform called POCSO e-Box. This allows children or their representatives to file anonymous complaints, and upon submission, a trained counsellor promptly contacts the child, provides support, and, if necessary, registers a formal complaint on their behalf. In the year 2020, NCPCR devised comprehensive directives entitled, "Cyber Safety and Security of Children," delineating the fundamental tenets of cyber safety and cyber security, explicating prevalent threats therein, and elucidating the pertinent legislative framework governing cyber safety. Subsequently, these directives were assimilated into the "Manual on Safety and Security of Schools". The Commission has actively worked towards disseminating this in various schools. In the month of February 2024, NCPCR established a Cyber Cell within the POCSO Division to monitor and identify harmful online content, including CSAM, posing a threat to children's safety. The Cell promptly reports the identified cases to the concerned police officials under Section 19 of the POCSO Act and requests the platform to share detailed information with law enforcement authorities.

Two significant interventions of the Commission that deserve mention here are:

1) In the month of February 2024, NCPCR took cognizance on a complaint regarding 'Ullu App', alleging that it contains sexually explicit and profoundly objectionable content accessible to its subscribers, including minors. The Commission subsequently issued notices to Google, iOS, and the Ministry of Information and Broadcasting (MIB), urging them to take appropriate action.

2) Similarly, in the month of February 2024, the Commission received a complaint regarding the distressing participation of children in illicit online gambling activities facilitated by websites and applications operating within the country, thereby posing a substantial threat to the welfare of minors. Consequently, the Commission took cognizance and issued notice to the Ministry of Electronics & Information Technology (MeitY) for appropriate action.

12.3 Institutional Framework Under Relevant Laws

12.3.1 Care and Protection of Children

Under the JJ Act, children earmarked for protective shelters are directed to the Child Welfare Committee (CWC), which oversees a plethora of CCIs managed by both the state and civil society partners. The coordinated efforts of the CWC, law enforcement, and social workers contribute to a comprehensive and protective strategy within the framework of the JJ Act. Any child victim of trafficking is admitted to a Child Care Institution only on the direction of CWC.

12.3.2 Protective Shelter for Women

Adult women rescued from sex trafficking can also be placed in protective shelters.[179] The Immoral Traffic Prevention Act, 1956 designates shelters as "protective homes" for adult women managed by the state or civil society organizations.

12.3.3 Legal Aid

Legal aid, a statutory entitlement under the National Legal Services Act, 1987, is constitutionally mandated by Article 39-A to ensure justice accessibility regardless of economic or other constraints. The Legal Services Authorities Act, 1987 operationalizes this mandate through a three-tier system comprising the National Legal Services Authority (NALSA), State Legal Services Authority (SLSA) for each state, and District Legal Services Authority (DLSA) for each district.

The National Legal Services Authority (NALSA) Victims of Trafficking and Commercial Sexual Exploitation Scheme, 2015[180] that was drafted in response to Prajwala's Public Interest Litigation 56/2002; aims to furnish legal services to trafficking victims during prevention, rescue, and rehabilitation stages. The scheme outlines a due diligence mechanism for DLSAs, in collaboration with NGOs facilitating trafficked women in accessing entitlements like interim and final compensation, food security, social security, pension, educational schemes, including bridge schools, housing subsidy, etc.

The Action Plan to lend assistance to victims of trafficking under the Scheme includes the following steps:

179 Section 17, Immoral Traffic (Prevention) Act

180 https://nalsa.gov.in/sites/default/files/document/scheme/Victims%20of%20Trafficking%20and%20Commercial%20Sexual%20Exploitation.pdf

1. Outreach program with NGOs and Community Based Organizations (CBOs) through UNICEF, UNODC, State Department of Women and Child, National Aids Control Organisation and the State and District Aids Control Societies.
2. Inter-departmental convergence at all levels in order to put in place a comprehensive response.

The Scheme specifically stressed that with regard to trafficking in persons, Legal Services Authorities have the following functions:

1. District Authorities, based on information from AHTUs and NGOs/CSOs, should map out vulnerable areas and populations within their jurisdictions.
2. Once vulnerable areas have been identified, prevention schemes must be rolled out to spread awareness. This awareness should be spread by a team of panel lawyers and social workers.
3. Carrying out due diligence in order to ensure that vulnerable populations have access to social welfare schemes.
4. Special training on trafficking issues imparted by the State and District Authorities to PLVs who are attached to police stations to deal with cases of missing children.

The NALSA (Victims of Trafficking and Commercial Sexual Exploitation) Scheme, 2015 requires impanelled lawyers and Para Legal Volunteers (PLVs) to aid trafficking victims in legal proceedings with FIR registration, opposing bail, obtaining court orders for witness protection, and applying for compensation. District Authorities are obligated to track and follow up on victims for at least three years, ensuring their proper rehabilitation and reintegration.

12.4 Existing Legal Framework:

12.4.1 The Constitution of India

Articles 23[181] and 24[182] of the Indian Constitution independently and cumulatively address the Fundamental Right Against Exploitation in Chapter III of the Indian Constitution, while the basis for anti-trafficking laws in our country.

Article 23 targets and prohibits trafficking in human beings and forced labor. This provision is enjoined with various directive principles such as Article 43[183] that tries to eliminate two kinds of social evils namely, trafficking in human beings and forced labor.

Article 24 of the Indian Constitution specifically recognises the vulnerability of children and

181 Article 23 of the Indian Constitution imposes a prohibition of traffic in human beings and forced labor

182 Article 24 of the Indian Constitution mandates a prohibition in the employment of children younger than 14 years in factories, etc.

183 Article 43 of the Indian Constitution states that, "The State shall endeavour to secure, by suitable legislation or economic organisation or in any other way, to all workers, agricultural, industrial or otherwise, work, a living wage, conditions of work ensuring a decent standard of life and full enjoyment of leisure and social and cultural opportunities and, in particular, the State shall endeavour to promote cottage industries on an individual or co-operative basis in rural areas."

prohibits the employment of children younger than 14 in factories, mines, or any kind of hazardous work.

In addition to the rights against exploitation, there are other articles that enable the Indian state to enact and implement laws that safeguard the interests of the victims of trafficking. Some examples of the same are Article 15(3)[184], Article 38(1)[185] and Article 51(c)[186].

12.4.2 General Law Provisions

Bharatiya Nyaya Sanhita, 2023 (BNS)

India's main penal statute, the Bhartiya Nyaya Sanhita (BNS), which succeeds the Indian Penal Code, addresses Offenses against the Human Body in Chapter VI. Some relevant Sections that directly target the menace of human trafficking in its various shades are:-

i. Section 95 Hiring, employing or engaging a child to commit an offence;[186a]

ii. Section 96 i.e. procuration of a minor Child;[187]

iii. Section 98 i.e. selling minor for purpose of prostitution;[188]

iv. Sections 99 i.e. buying minors for the purpose of prostitution;[189]

v. Sections 141 i.e. Kidnapping or abducting in order to subject person to grievous hurt, slavery, etc.;[190]

---

184 Article 15(3) is a facet of Article 15.i.e. Right to Equality of Indian Constitution, which enables the state to make special provisions for women and children.

185 Article 38(1) which is a Directive Principal of State Policy states that, "The State shall strive to promote the welfare of the people by securing and protecting as effectively as it may a social order in which justice, social, economic and political, shall inform all the institutions of the national life".

186 Article 51(c), which is a Directive Principal of State Policy reiterates the Indian State's obligations to foster respect for international law and treaty obligations in the dealings of organized peoples with one another.

186a Section 95 of BNS states that ,"Whoever hires, employs or engages any child to commit an offence shall be punished with imprisonment of either description which shall not be less than three years but which may extend to ten years, and with fine; and if the offence be committed shall also be punished with the punishment provided for that offence as if the offence has been committed by such person himself."

187 Section 96 of BNS states that, "Whoever, by any means whatsoever, induces any child to go from any place or to do any act with intent that such child may be, or knowing that it is likely that such child will be, forced or seduced to illicit intercourse with another person shall be punishable with imprisonment which may extend to ten years, and shall also be liable to fine."

188 Section 98 of BNS states that, " Whoever sells, lets to hire, or otherwise disposes of any child with intent that such child shall at any age be employed or used for the purpose of prostitution or illicit intercourse with any person or for any unlawful and immoral purpose, or knowing it to be likely that such child will at any age be employed or used for any such purpose, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine. "

189 Section 99 of BNS states that, "Whoever buys, hires or otherwise obtains possession of any child with intent that such child shall at any age be employed or used for the purpose of prostitution or illicit intercourse with any person or for any unlawful and immoral purpose, or knowing it to be likely that such child will at any age be employed or used for any such purpose, shall be punished with imprisonment of either description for a term which shall not be less than seven years but which may extend to fourteen years, and shall also be liable to fine."

190 Section 141 of BNS states that, "Whoever imports into India from any country outside India any girl under the age of twenty-one years or any boy under the age of eighteen years with intent that girl or boy may be, or knowing it to be likely that girl or boy will be, forced or seduced to illicit intercourse with another person, shall be punishable with imprisonment which may extend to ten years and shall also be liable to fine."

vi. Section 140(4) i.e Kidnapping or abducting any person for slavery etc;[191]

vii. Sections 142 i.e. wrongfully concealing or keeping in confinement, kidnapped or abducted person;[192]

viii. Sections 143 i.e. trafficking of persons;[193]

ix. Sections 144 i.e. punishment for exploitation of trafficked persons;

x. Sections 145 i.e. habitual dealing in slaves[194] and ;

xi. Sections 146 i.e. unlawful compulsory labor[195]

---

191 Section 140(4) of BNS states that, "Whoever kidnaps or abducts any person in order that such person may be subjected, or may be so disposed of as to be put in danger of being subjected to grievous hurt, or slavery, or to the unnatural lust of any person, or knowing it to be likely that such person will be so subjected or disposed of, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine."

192 Section 142 BNS states that, "Whoever, knowing that any person has been kidnapped or has been abducted, wrongfully conceals or confines such person, shall be punished in the same manner as if he had kidnapped or abducted such person with the same intention or knowledge, or for the same purpose as that with or for which he conceals or detains such person in confinement."

193 Section 143 BNS State that " Whoever, for the purpose of exploitation recruits, transports, harbours, transfers, or receives a person or persons, by—

a. using threats, or

b. using force, or any other form of coercion, or

c. by abduction, or

d. by practising fraud, or deception, or

e. by abuse of power, or

f. by inducement, including the giving or receiving of payments or benefits, in order to achieve the consent of any person having control over the person recruited, transported, harboured, transferred or received,

(2) Whoever commits the offence of trafficking shall be punished with rigorous imprisonment for a term which shall not be less than seven years, but which may extend to ten years, and shall also be liable to fine.

(3) Where the offence involves the trafficking of more than one person, it shall be punishable with rigorous imprisonment for a term which shall not be less than ten years but which may extend to imprisonment for life, and shall also be liable to fine.

(4) Where the offence involves the trafficking of a child, it shall be punishable with rigorous imprisonment for a term which shall not be less than ten years, but which may extend to imprisonment for life, and shall also be liable to fine.

(5) Where the offence involves the trafficking of more than one child, it shall be punishable with rigorous imprisonment for a term which shall not be less than fourteen years, but which may extend to imprisonment for life, and shall also be liable to fine.

(6) If a person is convicted of the offence of trafficking of a child on more than one occasion, then such person shall be punished with imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, and shall also be liable to fine.

(7) When a public servant or a police officer is involved in the trafficking of any person then, such public servant or police officer shall be punished with imprisonment for life, which shall mean imprisonment for the remainder of that person's natural life, and shall also be liable to fine

193a Section 144 of BNS states that, "(1)Whoever, knowingly or having reason to believe that a child has been trafficked, engages such child for sexual exploitation in any manner, shall be punished with rigorous imprisonment for a term which shall not be less than five years, but which may extend to ten years, and shall also be liable to fine. (2) Whoever, knowingly or having reason to believe that a person has been trafficked, engages such person for sexual exploitation in any manner, shall be punished with rigorous imprisonment for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine."

194 Section 145 of BNS State that , "Whoever habitually imports, exports, removes, buys, sells, traffics or deals in slaves, shall be punished with imprisonment for life, or with imprisonment of either description for a term not exceeding ten years, and shall also be liable to fine."

195 Section 146 of BNS State that , "Whoever unlawfully compels any person to labour against the will of that person, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both."

A new and novel incorporation in the BNS has been Section 111 which deals with "Organised Crimes". Section 111 provides an expansive definition of organized crime. The activities incorporated within the ambit of this section are "continuing unlawful activity" including "kidnapping, robbery cyber-crimes, trafficking of persons, drugs, weapons or illicit goods or services, human trafficking for prostitution or ransom."[196]

The following table provides an overview of the provisions in the Bharatiya Nyaya Sanhita (BNS), formulated in 2023 and enacted in 2024, compared to the Indian Penal Code (IPC), which was enacted in 1860 and remained in effect until June 2024.

INDIAN PENAL CODE AND BHARATIYA NYAYA SANHITA		
Section of BNS	**Comparable IPC Section**	**Wordings of the Section**
I. Section 96 of BNS Procuration of child	Section 366A	Whoever, by any means whatsoever, induces any child to go from any place or to do any act with intent that such child may be, or knowing that it is likely that such child will be, forced or seduced to illicit intercourse with another person shall be punishable with imprisonment which may extend to ten years, and shall also be liable to fine.
II. Section 98 Selling child for purpose of prostitution	Section 372	Whoever sells, lets to hire, or otherwise disposes of any child with intent that such child shall at any age be employed or used for the purpose of prostitution or illicit intercourse with any person or for any unlawful and immoral purpose, or knowing it to be likely that such child will at any age be employed or used for any such purpose, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.
III. Section 99 Buying minor for purposes of prostitution	Section 373	Whoever buys, hires or otherwise obtains possession of any child with intent that such child shall at any age be employed or used for the purpose of prostitution or illicit intercourse with any person or for any unlawful and immoral purpose, or knowing it to be likely that such child will at any age be employed or used for any such purpose, shall be punished with imprisonment of either description for a term which shall not be less than seven years but which may extend to fourteen years, and shall also be liable to fine.

196 Section 111 of the Bharatiya Nyaya Sanhita

IV.	Section 111 of BNS Organised Crime	None	Any continuing unlawful activity including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cyber-crimes, trafficking of persons, drugs, weapons or illicit goods or services, human trafficking for prostitution or ransom, by any person or a group of persons acting in concert, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate, by use of violence, threat of violence, intimidation, coercion, or by any other unlawful means to obtain direct or indirect material benefit including a financial benefit, shall constitute organised crime.
V.	Section 144(4) Kidnapping or abducting in order to murder or for ransom, etc	Section 367 Kidnapping or abducting in order to subject person to grievous hurt, slavery, etc.—	Whoever kidnaps or abducts any person in order that such person may be subjected, or may be so disposed of as to be put in danger of being subjected to grievous hurt, or slavery, or to the unnatural lust of any person, or knowing it to be likely that such person will be so subjected or disposed of, shall be punished with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine. • Needs to be read along with Section 359 IPC i.e. explains that there are two kinds of kidnapping (within India and outside) and 137(1)a BNS
VI.	Section 141 Importing girls or boys	Section 366B	Whoever imports into India from any country outside India any girl under the age of twenty-one years or any boy under the age of eighteen years with intent that girl or boy may be, or knowing it to be likely that girl or boy will be, forced or seduced to illicit intercourse with another person, shall be punishable with imprisonment which may extend to ten years and shall also be liable to fine.
VII.	Section 142 Wrongfully concealing or keeping in confinement, kidnapped or abducted person.	Section 368	Whoever, knowing that any person has been kidnapped or has been abducted, wrongfully conceals or confines such person, shall be punished in the same manner as if he had kidnapped or abducted such person with the same intention or knowledge, or for the same purpose as that with or for which he conceals or detains such person in confinement.

VIII.	Section 143 Trafficking of person.	Section 370	Trafficking of human persons. Not reproduced for the sake of brevity • Explanation 1.—The expression "exploitation" shall include any act of physical exploitation or any form of sexual exploitation, slavery or practices similar to slavery, servitude, beggary or forced removal of organs. • Explanation 2.—The consent of the victim is immaterial in determining the offense of trafficking.
IX.	Section 144 Exploitation of a trafficked person	Section 370A	(1) Whoever, knowingly or having reason to believe that a child has been trafficked, engages such child for sexual exploitation in any manner, shall be punished with rigorous imprisonment for a term which shall not be less than five years, but which may extend to ten years, and shall also be liable to fine. (2) Whoever, knowingly or having reason to believe that a person has been trafficked, engages such person for sexual exploitation in any manner, shall be punished with rigorous imprisonment for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.
X.	Section 145 Habitual dealing in slaves	Section 371	Whoever habitually imports, exports, removes, buys, sells, traffics or deals in slaves, shall be punished with imprisonment for life, or with imprisonment of either description for a term not exceeding ten years, and shall also be liable to fines.
XI.	Section 146 Unlawful compulsory labor	Section 374	Whoever unlawfully compels any person to labor against the will of that person, shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.

12.4.3 Special Laws

a. Immoral Traffic (Prevention) Act, 1956

The primary purpose for the enactment of ITPA was to address trafficking of women and children for CSE. This was in keeping with India's international obligations as a signatory of the United Nations International Convention for the "Suppression of Women in Traffic in Persons and of the Exploitation in Others" in New York on 9th May 1950. The Act primarily targets collective and/or organized procuration, exploitation and prostitution of women and children. It protects both adults and children against CSE.

b. Information Technology Act, 2000

The Information Technology Act is the primary legislation which regulates digital realm in India. It is both substantive as well as procedural and lists the various penal offenses that covers using or involving a computed device or in the digital realm. In addition to the Act itself a number of rules and guidelines made under this Act provide the online institutional structure that laid down the foundation of the country's response to CEHT. There are two layers within this institutional structure set up by the IT Act.

The first layer deals with the criminalization and penalization of certain acts. Some examples of the same are breach of data, using a computer for unlawful purposes, distribution and publication of obscene content, child pornography etc. The most relevant Sections with reference to trafficking would be Sections 67,[197] 67A,[198] and 67B.[199] In particular when read with clause (d) of Section 67B i.e. whoever "facilitates abusing children online", a constructive interpretation of the term should also encompass acts of trafficking children online. On a plain reading of the text what stands out is that under this Section, even viewing child pornography has been made a punishable offense, indicating the intent of the legislature to have a zero tolerance approach towards CSAM and treating it as a contraband.

The second layer provides the regulatory framework. In addition to the provisions of this act, the Central government in exercise of the powers conferred by this Act[200] has made rules. The aim of these rules has been to involve all stakeholders. With respect to trafficking of human beings and particularly children with respect to online abuse of children, the Central Government in April 2017 passed an order on Measures to Curb Online Child Sexual Abuse Material that are to be followed by ISPs. This builds upon Section 67B of the IT Act which prohibits the viewing, publication or transmission of material depicting children in sexually explicit acts or conduct in electronic form.

Furthermore the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 are one of the most significant steps in the direction of imposition of liability, and ensuring social media intermediaries are required to undertake due diligence such as deployment of technology-based measures to identify certain types of content for significant social media intermediaries.[201] They are also required to identify the first originator of information available on its platform[202] and appoint personnel for compliance with these guidelines.[203] Section 79 of the IT Act when read with the 2021 Guidelines qualifies the immunity and safe harbor available to intermediaries by a great extent. Internet Service Providers (ISPs)

197 Section 67 of the IT Act, 2000 prescribes the punishment for publishing or transmitting obscene material in electronic form

198 Section 67A of the IT Act, 2000 prescribes the punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form

199 Section 67A of the IT Act, 2000 prescribes the punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

200 Under clause (zg) of sub-section 2 of section 87 of the Information Technology Act , the Central government has the power to make Rules.

201 Rule 4(4) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

202 Rule 4(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

203 Rule 3(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

are obligated to remove or disable access to content which qualifies as paedophilic or harms minors in any way under Section 79(2)(c) read with Section 2(1)(w) of the IT Act and Rule 3(b) ii of the 2021 Intermediary Guidelines.

Takedown Process

A conjoint reading of Section 79(3)b of the Act and Rule 3(1)(d) of 2021 Guidelines brings out that an intermediary after getting "actual knowledge" through a court order or upon being notified by its agency or appropriate government should not publish, host or store any unlawful information and should compulsorily remove or disable access to unlawful content within a time period of 36 hours from the receipt of such a direction. Further, they may also voluntarily take down any prohibited information. The safe harbour protection would not be in any manner or from, be diluted for any compliance with takedown requests or voluntary removal.

Point of Contact with the Social Media Intermediary

Under the 2021 Guidelines all intermediaries were required to not only appoint a grievance officer but in addition to their appointment they were mandated to give details of the said officer on their website so that they may be contacted or approached to report any violation. Additionally, an intermediary is required to formulate a grievance redressal mechanism, acknowledge receipt of user complaints within 24 hours and resolve them within 15 days. They are also required to provide any information or assistance to any law enforcement agency for prosecution, investigation, verification of identity, prevention etc.[204]

In addition to the aforementioned guidelines significant social media intermediaries[205] under Rule 4 are also required to comply with additional due diligence requirements. They are required to appoint Chief Compliance Officer, Nodal Contact Person and Resident Grievance officer and these individuals must reside in India. It further stipulates that the Chief Compliance Officer and Nodal Contact Person cannot be the same person.

Blocking of Websites

The blocking of websites is governed by the two following provisions :

1. Information Technology Act, 2000 (Section 69 A)
2. Information Technology (Procedure and Safeguards for Blocing for Access of Information by Public) Rules, 2009[206]

---

204 Rule 3(1)j of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

205 Rule 2(1)v the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

206 These rules have been made under clause (z) of sub-section (2) of section 87, to be read with sub-section (2) of section 69A of the Information Technology Act, 2000

CSAM and pornography and blocking of websites

As per information provided by MeitY, a total of 1,065 websites were restricted between 2015 and 2022. In 2018, MEITY enforced the blocking of 857 websites following a directive from the Uttarakhand High Court [WP (PIL) No. 158/2018]. This court order mandated the government to restrict websites or any online content displaying pornography, particularly child pornography. Additionally, in 2016, the Additional Chief Metropolitan Magistrate in Mumbai blocked 238 websites for offenses related to obscenity, pornography, and child sexual abuse.[207]

Content Blocking Procedure under Intermediary Guidelines

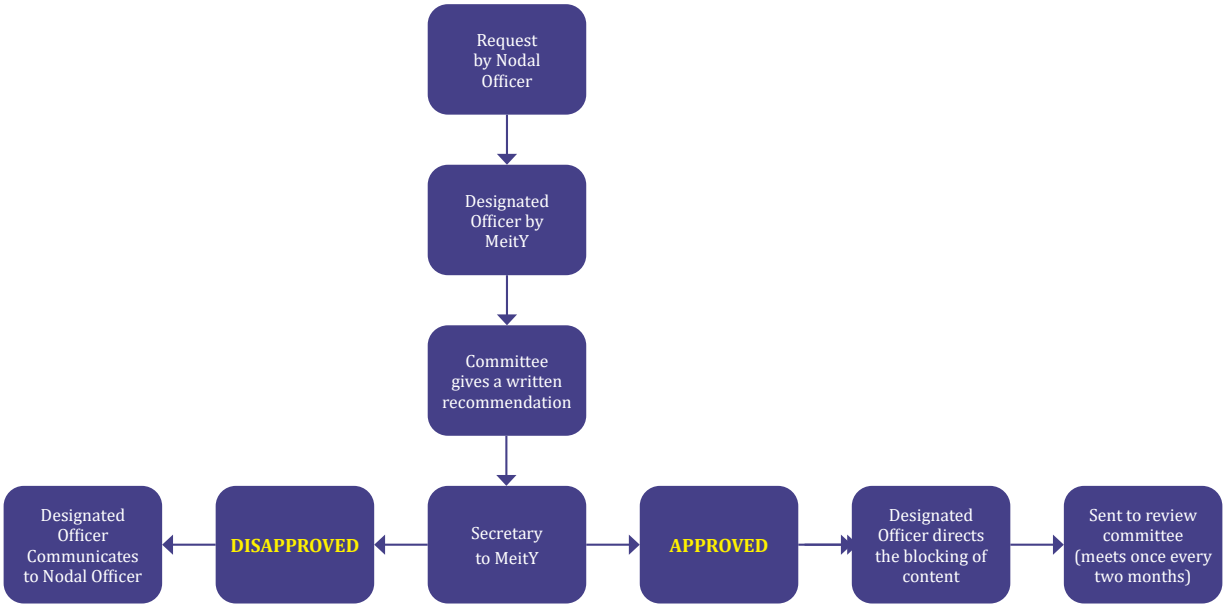
Rule 14 of the 2021 guidelines outlines the establishment of an Inter-Departmental Committee tasked with reviewing complaints or grievances. Upon scrutinizing a complaint related to Code of Ethics violations, the Committee may propose various recommendations. These suggestions include, but are not limited to:

i. altering or removing content to prevent incitement;

ii. recommending action under section 69A(1) of the Act, if necessary.

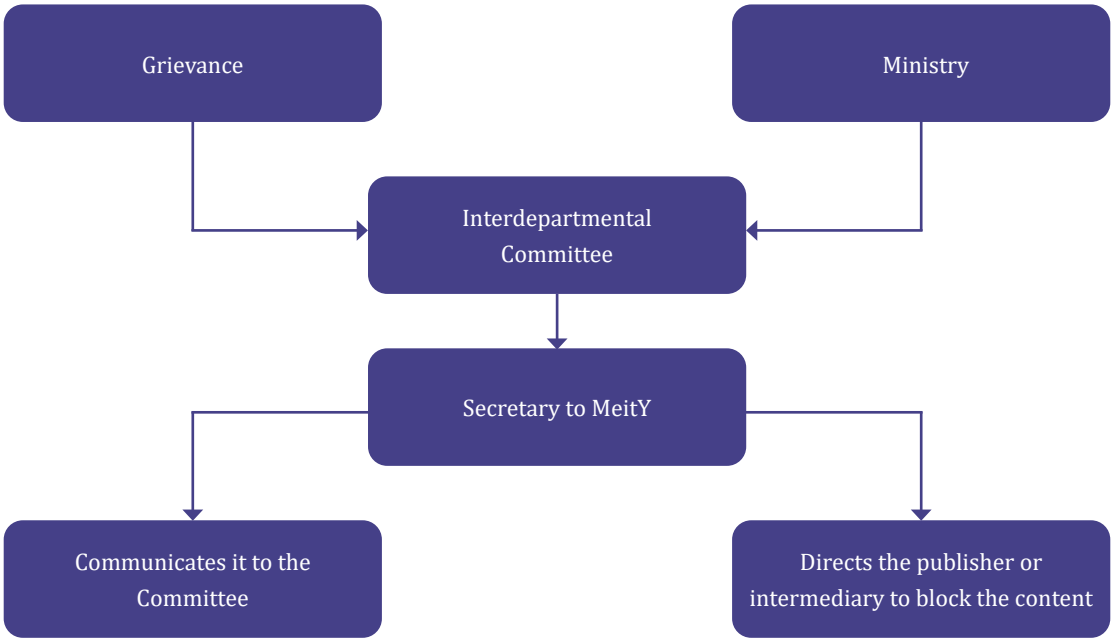
Upon receiving a recommendation, the Secretary to the MIB will issue an order following a procedure akin to the Blocking Rules, 2009. The Authorized Officer forwards the recommendation to the Secretary for approval or disapproval. After approval, the government agency or intermediary is directed to delete, modify, or block the content.

Blocking Procedure under the Information Technology (Blocking Rules), 2009



207 Finding 404: A Report On Website Blocking In India, Available at https://sflc.in/finding-404-report-website-blocking-india/

Blocking Procedure as Per the 2021 Guidelines



Proposed Digital India Act, 2023

MeitY in March of 2023 released a proposal for a Digital India Act that sought to replace the existing Information Technology Act. While there is a recognition that the digitalization of the economy and the increased penetration and usage of the internet have empowered citizens, these advancements have also introduced multiple challenges, such as ambiguity, security concerns for women and children, organized information wars, and the circulation of hate speech. Furthermore, the goal is to update the Indian information technology regulatory framework to keep pace with the latest global developments while ensuring user safety, open internet access, easy adjudication, resolution, and accessibility.

c. Protection of Children from Sexual Offences(POCSO) Act, 2012

This is an Act dealing with sexual offenses against children. While there is no specific provision in this Act dealing with trafficking in persons, it is pertinent to read the statement of objects of this act. The statement of objects highlights the obligations under the Convention on the Rights of the Child. Of particular importance are the measures enshrined in the convention which a state needs to undertake in order to prevent:-

(a) the inducement or coercion of a child to engage in any unlawful sexual activity;

(b) the exploitative use of children in prostitution or other unlawful sexual practices;

(c) the exploitative use of children in pornographic performances and materials;.

This emphasises how POCSO Act provides a penal framework against the exploitation and trafficking of children as well as online sexual abuse of children, and this Act does so in

two ways. Firstly, it categories sexual assault as penetrative and ordinary "sexual assault", and within those categorizations there is a further categorization of aggravated penetrative sexual assault and aggravated sexual assault, indicating the intent of the legislature to provide for a more stringent standard of punishment of certain categories of people who, broadly speaking, are either in a fiduciary relationship with the child or do so in a manner which may subject the child to a grievous bodily injury.

The latter is more likely when children are subject to trafficking for the purpose of prostitution. Secondly, the law has been moulded in a manner for it to enable it to have linkages with other laws. For instance Section 11[208] i.e. Sexual Harassment clauses (i), (iii) and (iv) and Section 13[209] i.e. use of child for pornographic purposes have been worded to recognise and criminalize the use of internet and media for sexual harassment and grooming of children which is a precursor to their trafficking.

Similarly, Section 16 criminalizes the act of abetment of an offense under POCSO Act, which when read along with explanations I, II and III[210] of the same Section, creates a harmonious linkage with provisions related to kidnapping and trafficking in the Bharatiya Nyaya Sanhita. In particular, a conjoint reading of this provision along with Section 111 of the BNS i.e. organized crime would enable the criminalization of the Act of human trafficking of children as well as usage of technology for the same.

Similarly, under Section 28 of POCSO, designated Courts have been given the jurisdiction to try offenses punishable with Section 67B of the IT Act.

d. The Juvenile Justice Act, 2015

Section 2(14) of the JJ Act provides a very comprehensive definition of a child in need of care and protection. It is pertinent to note that it states that sub-sub section (ix) defines a child as someone, "who is found vulnerable and [has been or is being or is likely to be] inducted into drug abuse or trafficking."[211]

Similarly Section 81[212] runs mutatis mutandis with IPC provisions on kidnapping and completely prohibits sale and/or procurement of children for any purpose.

---

208 Section 11, POCSO Act Sexual harassment— A person is said to commit sexual harassment upon a child when such person with sexual intent -
- (i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or
- (iii) shows any object to a child in any form or media for pornographic purposes; or
- (iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means

209 Section 13 of POCSO Act criminalizes the use of child for pornographic purposes. And states that whoever, uses a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification,

210 "Whoever employ, harbours, receives or transports a child, by means of threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or of a position, vulnerability or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of any offence under this Act, is said to aid the doing of that act."

211 The Juvenile Justice (Care and Protection of Children) Act, 2015

212 Section 81 of the JJ Act states that, "Any person who sells or buys a child for any purpose shall be punishable with rigorous imprisonment for a term which may extend to five years and shall also be liable to fine of one lakh rupees."

e. The Transplantation of Human Organs and Tissues Act, 1994

The Transplantation Act tackles a unique dimension of human trafficking i.e. trafficking of human beings for the purpose of harvesting their organs. This Act places a number of limits on the removal as well as transplantation of human organs and/or tissues.[213] It also prohibits the removal or transplantation of human organs or tissues for any purpose other than therapeutic purposes[214]. Section 19 is another integral section as it provides punishment for the commercial dealing of human organs.[215]

f. National Investigation Agency Act, 2008

The NIA Act was enacted to establish a national-level agency responsible for investigating and prosecuting offenses that affect India's sovereignty, security, and integrity. This includes fostering amicable relations with foreign nations and addressing offenses outlined in Acts that enforce international treaties, agreements, conventions, and resolutions of the United Nations, its affiliated agencies, and other global organizations, along with related or consequential matters. Section 8[216] of the Act empowers the agency to investigate any offense that has been committed in connection with a Scheduled offense. Furthermore after the 2019 Amendment to the NIA Act, Section 370 and 370A of the Indian Penal Code (Section 143 and 144 of BNS) i.e. offenses related to the commission of human trafficking have been added to para 8 (b) of the Schedule. This empowers the Central government to go after transnational criminal syndicates that operate in a cartelized manner.

g. Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act (PMLA) is another significant Act which gives teeth to the anti-trafficking legal framework of the Indian legal system.[217] A closer reading of the provisions of the Act as well as Schedule A tells us that the Act has attempted to criminalize various aspects of organized criminal activities that are concerned with human trafficking. A perusal of Schedule A of PMLA shows us how the Act weaves together various laws that criminalize human trafficking in India. Some relevant provisions mentioned in the Schedule of the Act are:

i. Para 1, wherein 364A of IPC i.e. provision related to kidnapping for ransom etc has been mentioned.

---

213 Section 9 of the Transplantation of Human Organs and Tissues Act, 1994 provides for restrictions on removal and transplantation of 2[human organs or tissues or both]

214 Section 11 of the Transplantation of Human Organs and Tissues Act, 1994 prohibits "removal or transplantation of [human organs or tissues or both] for any purpose other than therapeutic purposes…"

215 Section 19 of the Transplantation of Human Organs and Tissues Act, 1994 prescribes the punishment for commercial dealings in human organs. "Whoever—(a) makes or receives any payment for the supply of, or for an offer to supply, any human organ….."

216 Section 8 of the National Investigation Agency Act empowers the NIA to investigate connected offenses.

217 Section 4 of PMLA states that,"Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine."

ii. Para 14 which talks about the offenses under The Child Labor (Prohibition And Regulation) Act, 1986. The Section that has been included in the Schedule is Section 14[218].

iii. Para 15 which talks about the offenses under The Transplantation Of Human Organs Act, 1994. Within this the Sections which have been included in the Schedule are Section 18[219], 19[220] and 20[221].

iv. Para 16 which deals with the offenses under the Juvenile Justice (Care And Protection Of Children) Act, 2000. Sections incorporated in the Schedule are 23[222], 24[223] 25 and 26[224].

h. Digital Personal Data Protection Act, 2023

The DPDP Act keeps in mind the vulnerability of children in comparison to adults and has embedded within itself certain special provisions with respect to children. Some of these provisions are:

1. Section 9(1) that stipulates the manner of obtaining verifiable parental or guardian consent prior to processing any personal data of a child and a person with disability, by a Data Fiduciary.
2. Section 9(2) prohibits the processing of data of a child by a data fiduciary in a manner that is likely to have a detrimental effect on the child.
3. Section 9(3) states that a data fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

A notable feature of the Act is the provision of massive monetary penalties on data fiduciaries for the contravention of the provisions of the Act. As provided in the schedule of the Act, the breach of obligations under Section 9 of the Act may attract penalties worth two hundred crore rupees.

12.5 Other Laws

In addition to the aforementioned laws there are other laws which target the differential aspects of human trafficking in India. They can be classified into two categories i.e. (i) Acts which generally provide safety mechanisms under Article 23 and are of a general nature and (ii)Acts which

218 Section 14 of Child Labour (Prohibition Act) lays down the punishment for employment of any child to work in contravention of the provisions of section 3.

219 Section 18 of the Transplantation of Human Organs Act states the "punishment for removal of human organ without authority".

220 Section 19 of Transplantation of Human Organs Act i.e. the punishment for commercial dealings in human organs.

221 Section 20 of the Transplantation of Human Organs Act prescribes the punishment for contravention of any other provisions of this Act.

222 Section 23 of the JJ Act prescribes the punishment for cruelty to juvenile or child.

223 Section 23 of the JJ Act prescribes the punishment for employment of juvenile or child for begging.

224 Section 26 of the JJ Act prescribes the punishment for exploitation of juvenile or child employee.

specifically target exploitation of children under the mandate of Article 24.

i. Acts which provide safety mechanisms under Article 23 and are of a general nature

Some examples of such legislations are the Bonded Labor System (Abolition) Act, 1976,[225] Minimum Wages Act, 1948, Factories Act, 1948, Mines Act, 1952, Merchant Shipping Act, 1958, Plantation Labor Act, 1951 Motor Transport Workers Act, 1951, Apprentices Act, 1961 Bidi and Cigar Workers Act, 1966, Contract Labor Act, 1970, Equal Remuneration Act, 1976, Transplantation of Human Organs Act, 1994.

ii. Acts which specifically target exploitation of children under the mandate of Article 24

Some examples of such legislations are the Child Labor (Prohibition and Regulation) Act, 1986[226] and its further amendments, Employment of Children Act, 1938, The Prohibition of Child Marriage Act, 2006[227]

Additionally, some State governments have also enacted specific legislations to deal with the issue. The Punjab Prevention of Human Smuggling Act, 2012 is one such example. Section 2 (g) of the Act expansively defines smuggling as, "human smuggling" shall mean and include illegally exporting, sending or transporting persons out of India or any type of facilitation thereto by receiving money from them or their parents, relatives or any other person interested in their welfare, by inducing, alluring or deceiving or cheating."[228] Section 13 of the Act lays down the punishment for contravention of the provisions of this Act.

12.6 The Government Bills

There have been recurrent attempts by the Indian Parliament to address the pervasive issue of human trafficking. This is evident in the series of bills proposed, with the most recent being the Trafficking in Persons (Prevention, Care and Rehabilitation) Bill, 2021. This legislative endeavour emphasizes the Indian State's commitment to establishing a centralized system aimed at framing measures for the prohibition of human trafficking. Noteworthy antecedents to this legislative pursuit include the Trafficking in Persons (Prevention, Care and Rehabilitation) Bill, 2016, and its successor, the Trafficking in Persons (Prevention, Care and Rehabilitation) Bill, 2018, both of which, unfortunately, have lapsed.

The proposed 2021 Bill introduces key provisions, including the establishment of District Anti-Human Trafficking Committee and National Anti-Human Trafficking Committee, forming an interlocking legal framework characterized by an expansive definition of human trafficking.

225 Section 4 of Bonded Labour System (Abolition) Act, 1976 states that, "abolition of bonded labour system.—(1) On the commencement of this Act, the bonded labour system shall stand abolished and every bonded labourer shall, on such commencement, stand freed and discharged from any obligation to render any bonded labour.."

226 Section 3 of Child Labour (Prohibition and Regulation) Act, 1986 provides for the prohibition of employment of children in certain occupations and processes. "No child shall be employed or permitted to work in any of the occupations set forth in Part A of the Schedule …."

227 Section 12 of the Prohibition of Child Marriage Act, 2006 provides for the marriage of a minor child to be void in certain circumstances. In particular, clause (c) of the Act states that, "Where a child, being a minor(c) is sold for the purpose of marriage; and made to go through a form of marriage or if the minor is married after which the minor is sold or trafficked or used for immoral purposes, such marriage shall be null and void."

228 Section 2(g) The Punjab Prevention of Human Smuggling Act, 2012

Section 3 of the Bill delineates measures for the prevention and combating of trafficking in persons, encompassing various offenses under the Act, while Section 5 specifically addresses the role and functions of the National Anti-Human Trafficking Committee.

12.7 Gaps in the Legal and Institutional Framework

Despite an elaborate institutional framework, there are significant gaps in supporting and preventing CEHT. As the research has shown and has been detailed in previous chapters, technology has penetrated human trafficking and its tentacles have rapidly enveloped the entire expanse of known trafficking spaces. The institutional framework to address CEHT in India is still in its nascent stage. At the time of writing this report, even though there is an understanding of TIP within the system, there is not yet a holistic understanding of CEHT. Cyber-crimes are being considered through a lens bereft of human trafficking. The executive is not completely convinced that a person committing financial cyber-crimes could be a victim of forced criminality having been trafficked at first. Similarly, even in other manifestations of CEHT, the understanding that it is TIP with strong involvement of cyber space is not yet being comprehended. Hence those victims are not treated as victims of TIP and are not offered any support that the law otherwise provides for trafficked victims.

There is a large gap in creating human resources to address CEHT. There is no cadre of officers to deal with CEHT even though it requires a certain skill set to be able to handle a case under CEHT. Understanding CEHT is also different amongst the personnel. There is a need to rationalize and have one common intervention strategy.

As far as the legal framework is concerned, while there are multiple legislations dealing with various offshoots of human trafficking, there are gaps in the same being able to address the inter-woven linkages in trafficking in persons and prosecute traffickers at every stage of a person being trafficked.

A few major gaps in the legal framework about CEHT are as follows:

a) Over the last decade, awareness of cyber-crimes has significantly increased, and the government has implemented several response mechanisms. However, the legal framework has yet to address the complex issue of CEHT and its rapid growth, including recent manifestations like cyber scamming and armed conflict.

b) The legal interventions are fragmented and are designed and planned without factoring in the intricate nature of the organized crime of human trafficking and especially CEHT. The statutory support system offering victims temporary shelter, support for prosecution, and in some cases rehabilitation, are almost non-existent for newer forms of CEHT. Very rarely is this support commensurate to years of exploitation suffered, the complex psychological harm one is subjected to, monetarily compensation for, the lost time, and the effective rehabilitation for life.

c) The existing mechanism is not yet geared to recognize the complex interplay of technology and its manipulation by the trafficker. The traffickers can misuse these opportunities to manoeuvre the legal system and stay out of the reach of law enforcement. It is both in

terms of technical expertise and legal sanctions not yet ready to intervene and overtake the traffickers.

d) Formal government structures work with clear division of roles and responsibilities. Technology is unfortunately still seen from an administrative lens, ignoring that technology can offer its support to criminal networks to thrive. The merger of technology and crime is seamless for traffickers, but the matching merger of the ministries of technology and law enforcement has not been as seamless.

e) There is a lack of clear legislation on certain kinds of cyber-crimes combined with lack of understanding in extending existing laws to CEHT. The legal provisions to address various manifestations of cyber-crime and cyber-enabled human trafficking and the manner in which it is used by the traffickers are not covered in any legislation.

f) The existing law fails to take cognizance of how CEHT operates, factoring in the digital involvement as well as the aggravated form it takes. It fails to take into account the role of the digital media in the conduct of the crime and fix penal accountability in cases of non-cooperation.

g) Both the Penal Code and the IT Act do not provide for any administrative process for supporting the victim. Victims of CEHT, who may be trafficked for serious offenses do not have any statutory support structures.

h) The existing law protects the technology service providers or the intermediaries as they are called. "Harboring" is ordinarily a serious offense. In the digital crime scene, the agency that "harbors" is the intermediary who is the medium used to store/ access/contact/threaten/ circulate material. Instead of making them liable, the 2021 intermediary guidelines under the IT Act completely exonerates platform accountability even for content hosting platforms.

i) There is a lack of effective mutual legal assistance treaties for cases of human trafficking as CEHT has been documented to be operated from different jurisdictions

j) There is a critical gap in the uniform understanding of the preservation of digital evidence. Due to the way how data can be manipulated, there is a serious lacuna in rules on how digital evidence needs to be preserved and the certification process as prescribed under Section 65B of the Indian Evidence Act. Law enforcement is still not adept at preserving the evidence and getting legally admissible certification.[229]

12.8 Conclusion

Research showed that there is an elaborate institutional framework and legal framework in India. However, they are not fully equipped to address the challenges thrown by CEHT. Bureaucratic divisions continue to be a major challenge to address CEHT. The Indian Ministry, which deals with technology, has largely administrative powers and all criminal cases get diverted to a completely different wing of the government. None of the ministries are fully equipped or adept at understanding technology and there is no structured system of coordination between the

229 Challenges faced by law enforcement is discussed in detail in chapter

departments. However, CEHT must be taken seriously and these administrative hurdles are to be addressed to curtail the number of cases.

There is a need to reinforce the fact that they are created for the trafficked and hence their infrastructures need to have the capacity to deal with the trafficked at every stage.

Chapter

13

Technology Firms and CEHT

Chapter 13

Technology Firms and CEHT

13.1 Introduction

Right from the introduction of this research report, there is a clear understanding that technological revolution is an inevitable reality and the digital landscape has drastically changed with widespread internet adoption globally, including in India. There is no doubt that internet affordability has been crucial, reaching remote areas and low-income groups. Smartphones have replaced PCs and laptops as the preferred device for internet access. Beyond business and education, the internet now offers diverse services like communication and entertainment. Free cyber services from tech firms have driven massive adoption, despite initial expectations of fees due to high operational costs. These companies monetize through other means, like user data and continuous profiling, rather than charging directly. Major platforms such as Google, Facebook, Instagram, and WhatsApp offer free use while generating billions in revenue by capturing and expanding their user base through continuous innovation and feature updates.

While this research primarily looks at how technology has enabled organized crime like human trafficking, it is also imperative to look at how technology can be used to combat this crime by leveraging technological innovations and feature updates, as an ethical business practice to safegaurd these platforms from possible misuse. This necessitates a nuanced understanding of the current resources and their impact on our daily lives in areas such as communication, entertainment, banking, matrimony, job placements, and business communication. It also requires identifying the grey zones that can be misused and examining the existing efforts to safeguard cyberspace. Information received during the course of data collection, consultation with global experts and secondary research on various technological initiatives has been summarized in this chapter.

13.1.1 Communication and Social Media

The advent of social media platforms facilitated by cyber technology has completely changed the way the world communicates. Instant messaging apps like WhatsApp and Telegram have transformed communication by enabling text, image, and video sharing, group chats, and free voice/video calls. Email is now primarily used for official communication, as these platforms also support file sharing. Social media platforms such as Facebook facilitate personal connections and networking, with communities forming around shared interests. Instagram and Twitter boast large user base globally and in India. Businesses leverage these platforms for targeted advertising,

capitalizing on their extensive reach. Social media's allowance of pseudonymous identities fosters expressive freedom and mitigates privacy concerns.

13.1.2 Entertainment and gaming

The digital era has revolutionized entertainment access, offering 24/7 content on smartphones. YouTube hosts a vast array of free videos, while streaming services like Netflix, Prime, and Hotstar provide on-demand viewing. Music apps like Gaana and Spotify cater to personalized playlists. TikTok pioneered user-generated content, inspiring platforms like YouTube shorts, Facebook reels, and Instagram reels. Online and offline gaming apps like Roblox, PUBG, and Ludo redefine leisure activities, fostering social interaction through text and voice features in virtual spaces.

13.1.3 Online banking, payments and digital marketplace

Cyber technologies have revolutionized banking, eliminating queues and checks with online transactions. UPI payments have transformed the retail sector to the extent that even street vendors accept payments via fintech platforms. Digital giants like Amazon and Flipkart dominate online marketplaces. Platforms like OLX, Quikr, and Locanto facilitate peer-to-peer transactions and classified ads for a wide range of products and services.

13.1.4 Online match making sites and job exchanges

Cyber technologies unite people globally through platforms like Shaadi.com, Jeevansaathi.com for matrimonial searches and Tinder, Bumble for casual relationships. Naukri.com, labornet.in, connects job seekers and providers, while initiatives like nsdcindia.org, eshram.gov.in, aid India's unorganised sector.

13.1.5 Business collaboration and educational tools

Video-conferencing apps like Zoom, Meet, and Skype enable large-scale telecollaboration, offering free versions with limited features widely adopted for remote teaching. Cyber technology has revolutionized education with Google and similar search engines as virtual libraries, providing vast knowledge access. Apps aid study and assessment. These technologies exemplify digital transformation across travel, health, e-Governance, and social security.

13.2 Abuse of cyber technologies for malicious purposes

Traditional human approach in designing anything is to focus on solving a problem and leveraging the functionality of the solution/tool. Rarely a thought is spared on securing the developed tool against unintended usage or for malicious purposes. Cyber technologies are no different and here too, criminals proved that they are amongst the early adopters of technologies to device new ways of carrying out crimes. This section does not aim to discuss the acts of cyber hackers who target

businesses, people, groups or nations for varied intentions and often employing their in-depth and intricate technical skills. Rather, we will focus on loopholes and gaps in commonly available cyber platforms that are being exploited by even not so technically proficient criminals to further their acts of crimes very specifically organized crimes such as human trafficking.

13.2.1 Access to profiles and data of unknown people

Despite profile settings aimed at user control, few communication platforms or the social media platforms allow strangers to view and often access detailed personal information, thus creating a fertile ground for criminals. Default settings are often used due to the complexity of adjusting them regularly. Users frequently overlook security risks and lack judgment on appropriate sharing. Criminals exploit social media to study, target, befriend, and manipulate victims. Instances reported during interactions with police officers in West Bengal involved women lured into romantic relationships online, coerced into elopement, and subjected to sexual exploitation. Predators identify vulnerable individuals through social media profiles, targeting those displaying loneliness or few social connections. In Madhya Pradesh, victims were selected based on their public persona in photos and manipulated into situations of sex trafficking.

13.2.2 Anonymity

The most important feature that technology provides is anonymity which facilitates criminal activities by allowing users to create fake identities with false details and someone else's photo, making it difficult for law enforcement to trace them. This invisibility in cyber space empowers criminals who prefer virtual actions to avoid detection. Instances include fake identities on social media or dating sites to manipulate victims into trusting relationships, and exploiting their vulnerabilities. Criminals also impersonate law enforcement to intimidate and victimize individuals. In a case from Madhya Pradesh, a fraudster posed as a cyber police inspector from Pakistan to coerce a victim into sending nude photos. Another case from Rajasthan, involved a man using someone's photos to deceive women online.

13.2.3 Encryption

Cyber apps and websites now use end-to-end encryption and VPN services for added security, reassuring users but, also aiding criminals in evading law enforcement. This enables free communication and sharing of illicit content among criminals. Police officers from multiple states, including Punjab, Madhya Pradesh, Jharkhand, Odisha, Assam, and Andhra Pradesh, note that monitoring VPNs and encryption exceeds their capabilities. The officers from Gujarat highlighted VPNs as favored tools for professional cyber criminals, while officers from Maharashtra cited legal challenges due to VPN companies lacking Indian nodal officers. These issues are not the fault of technological platforms, as they uphold social responsibility with community guidelines supporting freedom of expression and anonymity. Although, encryption is implemented to safeguard against hackers and essential for social networking, yet it has come to be exploited by criminals.

13.2.4 Operation of multiple user IDs/accounts by a single person from single IP address/device

Traffickers exploit social media by operating multiple fake accounts on a single device or IP address to contact numerous victims simultaneously. This enables them to scale their operations without constraints. The officers from West Bengal noted traffickers managing 8-10 accounts on one device, demonstrating how they engage potential victims continuously.

13.2.5 Location tracking

Criminals misuse smartphone tracking features meant for minors and lost devices to monitor victims' whereabouts covertly. They install monitoring apps on victims' devices or deceive them into installing such apps. In a West Bengal revenge porn criminal case, the accused installed software that tracked the victim, during their previous relationship, to spy on and harass the victim after the relationship soured.

13.2.6 Fake advertisements

Advertising on technology platforms, particularly social media, is a significant revenue stream due to their extensive reach and targeted advertising capabilities. However, criminals exploit these platforms by posting fake job opportunities, modeling or acting gigs, etc. These fraudulent ads are not limited to social media but also extend to messaging apps, where traffickers randomly target recipients in hopes of eliciting responses.

A case shared by officers from West Bengal illustrates the dangers a college girl responded to a Facebook ad inviting young women to audition for a film role. Upon arrival at the specified location, she was drugged and coerced into participating in a pornographic video. Similar incidents have been reported in Telangana, Maharashtra, and Kerala, where educated young individuals were deceived with fake job offers, sent abroad to countries like Thailand or Cambodia, and then forced into committing cyber-crimes.

13.2.7 Operation of websites

Criminals, especially those involved in CEHT, are using cyber platforms to contact their customers too. Examples include posting online classified advertisements. Also, certain criminal groups run their own websites to provide labor services, etc.

It may be noted that the issues highlighted are not unique to cyber space. Fake advertisements and classified posts are old modus operandi that were made in print media too and now adapted to cyber space. The service provider (print media or technology platform) cannot verify veracity of advertisements made on their platform. It is for the end user to exercise caution and judgement.

Punjab had registered a case wherein a doctor had hired a child labor for household work, being provided by a Delhi based agency that advertised their services through their company website. Similarly, Gujarat had reported a case wherein agencies advertised child adoption services,

including new born children, through their website which led to exposure of the child trafficking racket.

13.2.8 Manipulating search results of popular search engines search

Criminals manipulate search results of commonly used search engines through advertisements or optimize their website for better search engine results, by displaying false information as top search results. They typically display contact details of fraudulent customer care services, leading unsuspecting users to believe the displayed information and thus become victims of fraud.

Cases of fraud through manipulating search engine results have been among the cases investigated by the Punjab police, wherein, Google search result rankings have been manipulated to direct unsuspecting people to fraudulent customer care numbers leading to financial losses for people.

13.2.9 Out of band communication on gaming apps

Online gaming apps allowing multiplayer interactions also include text-chat and voice features that are exploited by criminals for covert communication outside monitored channels. Officers from Odisha noted traffickers using Free-Fire for confidential communication, highlighting the need to mitigate such platform features prone to misuse, while ensuring legitimate user protection.

13.3 Existing safeguards on technology platforms

Having analyzed the loopholes in existing technological platforms that facilitates or encourages its usage for malicious purposes by the traffickers and criminals, it is pertinent to state that many technology firms have taken notice of abuse of their platforms for unintended purposes and have created various mechanisms/safe guards to limit abuse of their platforms. They also claim to pay special heed towards protecting women and children online.

Facebook, for example employs a sophisticated algorithm to detect and remove harmful contents such as hate speech, misinformation, and other malicious posts in order to minimize their impact on users. For protecting women and children, algorithms also detect contents including sexual violence, child exploitation and revenge porn. In addition, users can also report fake profiles, suspicious activity, inappropriate and abusive contents, which are subsequently reviewed by Facebook's review teams. Actions could include account suspension or even deletion.

WhatsApp employs machine learning algorithms to detect and block spam messages, phishing messages, and suspicious links. WhatsApp also provides the user with an option of flagging and reporting inappropriate messages and fake or malicious user accounts.[230]

YouTube identifies harmful videos through a mechanism of user reporting and automated

230 Reporting/ Blocking a Profile on WhatsApp- https://faq.whatsapp.com/414631957536067

systems.[231] Contents violating community guidelines are removed or age-restricted.

Similar steps have been undertaken by many platforms in an attempt to ensure that their platform is not employed for malicious intent. Typically, this includes the use of AI to detect harmful content violating their guidelines, and a user reporting mechanism.[232] The reported content/profile is reviewed by a team. The review, typically conducted through an algorithm and rarely by a human reviewer, is carried out within the scope of the company's community guidelines. It has been observed that technology firms usually follow global parameters, which often differ from regional conditions and local government regulation.

Although technical platforms pledge to make the online environment safe, yet the above measures have proved to be inadequate to check traffickers and criminals from perpetrating crimes using these platforms. Further, their support to law enforcement is also as per their own interpretation of the situation, and not necessarily as required by the requesting agency. Looking holistically, it appears that for the technology platforms to have community guidelines and a stated mission to make online environment safe, is aimed solely at flying below the radar of legal and regulatory compliances. When it comes to operations, the business interests seem to be get prioritized over the greater societal good.

13.4 Technological Innovations to counter Trafficking

Several technological innovations have been designed and rolled out in different parts of the world as a means to strengthen counter trafficking efforts. These innovations developed in collaboration with technological firms have been widely used by law enforcers and NGOs in prevention, crime detection and victim protection.

13.4.1 Web scraping

Web scraping automates law enforcement searches for exploitative content, particularly sexual exploitation, by scanning the internet using automated tools. Data gathered undergoes manual review, leading to actions such as content removal. Hashing technology assigns unique digital fingerprints to files, aiding law enforcement in identifying copies of reported exploitative content across devices and platforms. Advancements allow detection of resized or modified files based on similar hash matches. International experts, including those from the United States, UK, and Austria, utilize web scraping, web crawlers, and hashing technologies extensively. In the Philippines, experts use pen drive tools containing hashes of known exploitative materials for onsite forensics.

AI-enabled face detection enables law enforcement agencies to identify victims and perpetrators of exploitation on various internet platforms. In some jurisdictions, satellite imagery tracks containers suspected of transporting trafficking victims for labor exploitation.

231 How does YouTube manage harmful content?-https://www.youtube.com/intl/ALL_in/howyoutubeworks/our-commitments/managing-harmful-content/

232 Content moderation- https://en.wikipedia.org/wiki/Content_moderation

13.4.2 Traffic Jam

Traffic Jam,[233] a software tool developed by Marinus Analytics, uses AI to detect human trafficking indicators, aiding law enforcement and NGOs globally. It accelerates investigations by mapping locations like brothels, identifying traffickers, and locating victims, reducing case assembly time from 2 years to 3 months. U.S. investigative agencies highlight Traffic Jam as a key tool in combating human trafficking.

13.4.3 Sweat & Toil

Developed by the U.S. Department of Labor, the Sweat & Toil app[234] informs consumers about items created through child labor or forced labor. By using this app, consumers can make more informed buying decisions and support ethical practices.

13.4.4 StopNCII.org

Operated by the Revenge Porn Helpline (RPH), which is part of SWGfL (South West Grid for Learning), an international charity with the mission to ensure online safety. StopNCII.org is a free tool designed to support victims of Non-Consensual Intimate Image (NCII) abuse. The victims can anonymously generate and submit a hash of the intimate images or videos from their device using this tool. The hash is shared with the participating companies who in turn use these hashes to detect and remove non-consensual intimate images from their respective platforms, thereby preventing them being shared online.

13.4.5 Project Arachnid

Project Arachnid,[235] led by the Canadian Centre for Child Protection (C3P), targets the spread of CSAM online. It uses hashing technology to swiftly identify and send removal notices to Electronic Service Providers (ESPs), matching images or videos against a database to detect exact or resized matches. The initiative collaborates with 15 hotlines and child protection organizations across 14 countries to classify suspect content and issue removal notices. Additionally, Project Arachnid offers the 'Shield by Project Arachnid' API for companies aiming to prevent CSAM dissemination on their platforms. In the Philippines, telecom providers subscribe to watch groups that monitor and report inappropriate content URLs for blocking.

13.4.6 Plotting heatmaps on Open Street Map - Love Justice International

Love Justice International (LJI) is an NGO engaged in fighting human trafficking, especially pertaining to illegal migrants. It has used Open Street Map to draw heatmaps of the routes of

233 Traffic Jam- https://www.marinusanalytics.com/traffic-jam

234 Sweat and Toil- https://www.dol.gov/general/apps/ilab

235 Project Arachnid- https://www.projectarachnid.ca/en/

trafficking based on observed patterns. Thereafter, employing the machine learning algorithms and predictive analysis, it predicts the route likely to be used next for transportation of human trafficking victims. The interception mechanisms of law enforcement are thus deployed accordingly.

13.4.7 Khoya-Paya Portal

Khoya-Paya Portal is India's national system for tracking missing and vulnerable children. Developed by the Ministry of Women and Child Development with DeitY, it enables citizens to report missing children or sightings. Information is moderated and made public quickly. Parents can register details of missing children, and the portal compares these against sightings to aid in rescues of missing children.

13.4.8 GPower

GPower, a mobile initiative by Accenture Labs and CINI, aids vulnerable adolescent girls in India, especially those from impoverished backgrounds facing risks like abuse, trafficking, and child labor. Initially piloted in 20 West Bengal villages, GPower uses a mobile app given to village teachers to collect real-time data on health, nutrition, protection, and education. Machine learning models analyze responses to assess vulnerability, aiming for early intervention to prevent issues such as child marriage and trafficking.

13.4.9 SafetoNet.com

SafeToNet is an initiative that aims to keep children safe online. It rapidly detects and blocks adult content and child abuse material while respecting the child's privacy. This technology works on images, videos, and live streams, instantly spotting new child abuse material. Mention of SafetoNet.com was also made by experts from the Philippines, expressing their intent and efforts to use the platform for protecting Filipino children. SafeToNet integrates into the device's operating systems of all device manufacturers, making their products inherently safe by rejecting harmful or illegal sexual content. It can be deployed within existing visual inspection pipelines to monitor and block all streamed harmful or illegal sexual content before it reaches the device. App manufacturers can embed SafeToNet to prevent harmful or illegal visual content in uploaded or camera-captured content.

13.5 Contribution by Technological Companies to fight CEHT

Several technology firms acknowledging the gravity of the problem of human trafficking have slowly started taking proactive measures as a corporate response to evolve counter trafficking interventions. Such activities are largely undertaken by their social welfare wing as part of the Corporate Social Responsibility (CSR), and are mostly independent from their core operations.

A few such initiatives are listed below.

13.5.1 Tech Against Trafficking

Tech Against Trafficking (TAT) is a coalition of technological leaders like Amazon, BT, Microsoft, and Salesforce, united to combat human trafficking and modern slavery through technology. TAT collaborates with experts, civil society, law enforcement, academia, and survivors to scale tech solutions. It supports apps for identifying sex trafficking victims, satellite imagery to locate forced labor victims on fishing vessels, and web scraping tools to aid law enforcement in rescuing exploited children. TAT now operates under the Global Business Coalition Against Trafficking (GBCAT), uniting companies to fight trafficking in their operations and supply chains.

13.5.2 Actions by Meta

Meta has constituted a Safety Advisory Board in its mission to ensure a safe and respectful online environment for its users. The board consists of independent online safety organizations and experts. Its mission is to contribute insights, expertise, and perspectives on online safety issues. The Safety Advisory Board's insights are aimed to help Meta develop sophisticated technology to detect and prevent abuse. It also informs on the creation of clear policies about what should be allowed or not allowed on Meta's platforms.[236]

Meta is also collaborating with various governments and ministries in India and other countries, to ensure the safety and security of women and young children on online platforms. They advocate for age verification and comprehensive measures to prevent online harms.

In contributions specific to counter CEHT, Facebook, one of the meta platforms, collaborates with NGOs as trusted flaggers, uses AI to detect suspicious content, and provides resources for victims.

13.5.3 Actions by Google

Google's approach to women and children safety is through supporting various community programs, including education, digital literacy, and access to technology. They collaborate with schools, non-profits, and local organizations to bridge the digital divide and empower deprived communities. 'Be Internet Awesome'[237] is one of multifaceted programs by Google to educate and empower children about online safety by being smart, alert, strong, kind, and brave, when online.

In contributions specific to counter CEHT, Google has collaborated with project Thorn, to create a safer world for all kids by combating child sexual exploitation. It uses ML for victim identification, grooming prevention, and eliminating CSAM from the internet. To counter the threats to children through misuse of Generative AI technologies, project Thorn is also collaborating with organizations such as All Tech Is Human, Google, OpenAI, and StabilityAI.[238]

---

236 Safety Advisory Board- https://en-gb.facebook.com/help/www/222332597793306/

237 Be Internet Awesome- https://beinternetawesome.withgoogle.com/en_in

238 Thorn- https://www.thorn.org/blog/a-safety-by-design-conversation-with-thorn-all-tech-is-human-google-openai-and-stabilityai/

Google LLC's Victim Identification Team has created over 250 high priority CyberTips pursuant to U.S. law enforcement that identifies abusers and victims of child sexual abuse in India that can be used to expedite rescues and arrests.

13.5.4 Actions by Apple

Apple has taken various measures under the umbrella name of 'child safety initiatives'[239] that focus on protecting children from exploitation, promoting online safety, and preventing the spread of harmful material.

The Communication Safety features in Messages ensure that children receive warnings if they receive or attempt to send images or videos containing nudity. The content is blurred, and children are reassured that it's okay not to view such material. Importantly, the operating system analyzes image and video attachments locally without sending information off the device, ensuring privacy.

Apple has also implemented technology to detect and prevent the spread of CSAM. The iCloud Photo Library scans photos stored in iCloud to identify known CSAM images. If CSAM is detected, Apple notifies the National Center for Missing and Exploited Children (NCMEC) while maintaining user privacy.

Apple is also countering CEHT by addressing the demand or of the customers/ consumers. When users search for queries related to child exploitation using Siri/ Safari/Spotlight, these tools intervene emphasizing the harmful nature of such content and offering assistance. Use of tools like Spotlight by the U.S. law enforcement was mentioned during expert interaction with the study team.

13.5.5 Actions by Microsoft

Microsoft's chat software code named "Project Artemis," is designed to detect grooming of victims through chatting/messaging. Built in 2018 in collaboration with The Meet Group, Roblox, Kik and Thorn, Project Artemis evaluates and rates characteristics of conversations to assign a probability rating for possible grooming, which is then flagged and sent to human moderators for review. It recognizes specific words and speech patterns using AI technology such as Natural Language Processing (NLP), providing a more accurate approach to evaluating nuanced conversations on chat platforms. This tool is a significant step forward in preventing grooming conversations from escalating on gaming and chat platforms and could be effectively leveraged on hotspots.[240]

Microsoft also developed a tool PhotoDNA with the primary purpose to aid in finding and removing known images of child exploitation. PhotoDNA creates a unique digital signature (known as a "hash") of an image. This hash is then compared against signatures of other photos to find copies of the same image. When matched with a database containing hashes of previously identified

239 Child Safety Initiatives- https://www.apple.com/child-safety/

240 Project Artemis- https://www.psychologytoday.com/us/blog/modern-day-slavery/202111/using-the-power-technology-fight-online-human-trafficking

illegal images, PhotoDNA helps detect, disrupt, and report the distribution of child exploitation material. Microsoft donated PhotoDNA to the NCMEC. PhotoDNA is also being widely incorporated into innovative visual image and forensic tools used by law enforcement agencies worldwide.

13.6 Technology as a Disabler

Through the efforts of governments and various NGOs, several technology firms have come together to collaborate with each other to create platforms to counter CEHT and prevent misuse of their services. Technology giants such as Google, Meta, X (formerly Twitter), TikTok and others are collaborating to combat deepfakes, the AI generated audios and videos. Deepfakes have the potential to influence public perception and also in coercing a target/victim of CEHT into exploitation.

Foreign experts from United States, UK, and the Philippines, during interaction with the study team expressed that they are also collaborating with the technology giants to harness their capabilities for making suitable tools to counter CEHT. Experts from Austria shared that the European Union, recognizing the role that technology companies can play in both facilitating and combating criminal activities on their platforms, is pushing for accountability from technology firms. Further, they are also observing a noticeable shift in the willingness of technology companies to cooperate and be seen as responsible entities.

Experts from Austria shared about their close working relationship with an adult service provider, a German website/app kaufmir.com (translates to Buy me .com), wherein they ensured an emergency button was added to the interface. This button is to be used by the service buyer to raise a silent alarm along with sending a short message to the legal department of police. The button is to be used when the buyer suspects that the girl/woman offering sex services is possibly doing so under coercion and is likely a HT victim. The legal department thereafter alerts the AHTU on their hotline.

The source for technological expertise to counter CEHT is not limited to technology firms only. Talent from universities and from the general population can also be tapped. The Austrian expert informed about hackathons where techies from 20 European countries participated to investigate online platforms that identify/confirm their usage for HT, identify traffickers and victims. Similarly, UNODC organizes 'DataJams' with IBM, a technology giant, and NGOs too, where students compete online to develop technology-based solutions to identify and protect victims of trafficking and support prosecutions.[241]

Experts from the Philippines mentioned a unique instance of the responsible behavior by a technology company. Kumu, a social networking app popular in the Philippines, also supported live video streaming/ sharing, but stopped its operation/services after makers realized that their platform was prone to be misused. Makers are trying to secure their app against potential misuse and have suspended operations until then.

The possibilities are unlimited if there is a will to fight the common enemy. Technological solutions can be used to awaken the communities on the dangers of human trafficking, detect the

241 UNODC- https://www.unodc.org/unodc/en/human-trafficking/Webstories2021/the-role-of-technology-in-human-trafficking.html

crime, safeguard the rights of the victims and effectively support prosecution. A few representative examples are listed below.

13.6.1 Awareness Campaigns: Promoting awareness about the tactics used by traffickers, red flags to watch for, and resources for victims can empower individuals to recognize and avoid potential exploitation. Develop educational materials, including brochures, videos, and online resources, to raise awareness about CEHT and its indicators. Collaborate with schools, community organizations, and law enforcement agencies to disseminate educational materials and conduct training sessions.

13.6.2 Capacity Building: Providing training and resources to law enforcement agencies, frontline workers, and community organizations enhances their ability to identify and respond to CEHT effectively. Offer training programs, workshops, and webinars for law enforcement officers, social workers, healthcare professionals, and other frontline workers. Partner with experts in the field to develop comprehensive training that is tailored to the specific needs of different sectors.

13.6.3 Collaboration with the Technology Sector: Engaging with the technology companies to develop upgraded tools and protocols that prevent the misuse of their platforms for trafficking purposes, such as implementing AI algorithms to flag suspicious activities or content.

13.6.4 Crime Detection Strategies and Tools

1. Anonymous Reporting: Establishing hotlines and online reporting mechanisms where individuals can report suspected cases of CEHT anonymously, facilitating early intervention and support for victims.
2. Data Analytics: Leveraging data analytics and artificial intelligence to analyze patterns and detect anomalies indicative of CEHT, such as unusual financial transactions or online communications.
    - Data Collection: Gather historical data related to trafficking incidents, online behavior, and communication patterns.
    - Feature Extraction: Identify relevant features (e.g., keywords, IP addresses, time stamps) from the data.
    - Model Training: Train ML models (e.g., decision trees, neural networks) on labeled data to recognize patterns associated with CEHT.
    - Real-Time Monitoring: Continuously analyze incoming data to detect anomalies or suspicious patterns.
    - Alert Generation: Set up alerts when the model identifies potential CEHT activities.
3. Social Media Monitoring:
    - Platform Integration: Collaborate with social media platforms to access their APIs.
    - Keyword-Based Monitoring: Use NLP to identify trafficking-related keywords, phrases, and hashtags.

- Image Analysis: Analyze images and videos for signs of trafficking (e.g., explicit content, coercion).
- Automated Reporting: Automatically report suspicious content to platform moderators and law enforcement.

4. Natural Language Processing (NLP):
   - Chatbot Development: Create AI-powered chatbots that engage with users on social media or messaging apps.
   - Intent Recognition: Train NLP models to recognize trafficking-related intent in conversations.
   - Resource Provision: Chatbots can provide victims with helpline numbers, safety tips, and legal information.
   - Flagging Suspicious Conversations: Alert law enforcement when potential trafficking discussions occur.
5. Recognition:
   - Image Database: Collect a diverse dataset of trafficking-related images.
   - Convolutional Neural Networks (CNNs): Train CNNs to classify images as exploitative or non-exploitative.
   - Automated Content Moderation: Integrate image recognition into platforms to automatically flag illegal content.
6. Network Analysis:
   - Data Crawling: Collect data from websites, forums, and social networks.
   - Graph Theory Algorithms: Apply algorithms (e.g., centrality, community detection, etc.) to identify key nodes and connections.
   - Visualization: Create network graphs to visualize trafficking networks.
   - Collaboration with Law Enforcement: Share network insights with relevant agencies.
7. Predictive Modelling:
   - Geospatial Data: Gather data on trafficking incidents, demographics, and economic factors. Use this data for predictive analysis and modelling.
   - Spatial Analysis: Use GIS tools to identify potential hotspots.
   - Machine Learning Models: Train models to predict future CEHT occurrences based on historical data (e.g., use Geospatial data)

13.6.5. Dark Web Monitoring: Monitoring the dark web, where illicit activities often occur, for indicators of CEHT activities, such as online advertisements for trafficking or the sale of exploitative content.

13.6.6 Digital Forensics: Conducting digital forensic investigations to gather evidence of CEHT activities, such as tracing online communications or recovering deleted files.

13.6.7 MIT Lincoln Laboratory Tools: MIT has developed tools[242] to automate aspects of investigating human trafficking, including network analysis, text/image data analysis, and survivor interaction training.

13.6.8 Human Trafficking Search: Provides resources and information related to human trafficking, including CEHT.[243]

13.6.9 AI Technology and Counter Trafficking Efforts

1. Victim Identification and Rescue
    - Image and Video Analysis: AI can analyze images and videos from social media, surveillance footage, and other sources to identify potential victims of human trafficking.
    - Facial Recognition: Advanced facial recognition systems can help match missing person's reports with individuals seen in trafficking situations.
2. Pattern Recognition and Predictive Analytics
    - Behavioral Analysis: ML algorithms can analyze online behavior patterns to identify traffickers and potential victims based on their online activities.
    - Predictive Modelling: AI can predict hotspots for human trafficking by analyzing data from various sources, such as crime reports, migration patterns, and economic conditions.
3. Natural Language Processing
    - Social Media Monitoring: NLP can be used to scan social media platforms for language patterns and keywords associated with trafficking activities.
    - Text Analysis: AI can analyze text from online ads, chat logs, and other digital communications to identify potential trafficking cases.
4. Data Integration and Analysis
    - Multi-source Data Aggregation: AI can integrate data from various sources, such as law enforcement databases, non-profit organizations, and international agencies, to provide a comprehensive view of trafficking networks.
    - Network Analysis: AI can map and analyze the networks of traffickers and their associates, identifying key players and connections.

---

242 Turning technology against human traffickers. https://news.mit.edu/2021/turning-technology-against-human-traffickers-0506

243 Online and technology-facilitated trafficking in human beings. https://humantraffickingsearch.org/resource/online-and-technology-facilitated-trafficking-in-human-beings/

5. Automated Reporting and Alerts
    - Real-time Alerts: AI systems can provide real-time alerts to law enforcement and NGOs when suspicious activities are detected.
    - Automated Reporting Tools: AI can generate detailed reports and insights from the data collected, helping authorities to take timely and informed actions.
6. Support for Victims
    - Chatbots and Virtual Assistants: AI-powered chatbots can provide immediate assistance to trafficking victims, offering them information and support discreetly.
    - Rehabilitation Programs: AI can help tailor rehabilitation and support programs for rescued victims by analyzing their specific needs and backgrounds.
7. Supply Chain Monitoring
    - Ethical Sourcing: AI can help companies monitor their supply chains to ensure they are free from forced labor and trafficking.
    - Risk Assessment: AI tools can assess the risk of trafficking in different parts of a supply chain, helping companies to take proactive measures.
8. Educational and Awareness Campaigns
    - Content Personalization: AI can personalize educational content and awareness campaigns to target specific demographics and regions more effectively.
    - Impact Assessment: AI can measure the impact of awareness campaigns by analyzing social media and other public data.
9. Law Enforcement Support
    - Case Management: AI can assist law enforcement in managing human trafficking cases, prioritizing leads, and organizing evidence.
    - Resource Allocation: Predictive analytics can help allocate resources more effectively by identifying areas with a higher likelihood of trafficking activities.
10. Collaboration Platforms
    - Information Sharing: AI can facilitate secure information sharing between different stakeholders, such as law enforcement, NGOs, and international agencies.
11. Coordination of Efforts
    - AI tools can help coordinate efforts between various organizations involved in combating human trafficking, ensuring a unified approach.

13.7 Conclusion

Technology companies can play vital roles in combating CEHT at multiple levels. At operational levels they can build safeguards to prevent and detect abuse of their platforms. Such safeguards are essentially a work in progress and need to evolve continuously according to the prevailing modus operandi of traffickers/criminals. Technology companies can also contribute towards countering CEHT by supporting law enforcement agencies and NGOs in various forms through their technical expertise and funds to support relief programs.

Despite numerous efforts, involving various activities, tools, NGOs, government bodies, and programs aimed at combating (CEHT, effectiveness remains a challenge. Criminals leverage advanced technology, financial resources, and other means to circumvent existing systems and policies. To effectively control and eliminate CEHT, it is imperative to adopt a multi-faceted approach:

- Enhanced Collaboration: Strengthen collaboration among international agencies, law enforcement, technology companies, and NGOs to share information, resources, and expertise in real-time.
- Advanced Technology Deployment: Utilize cutting-edge technologies such as AI, ML, blockchain, and Big Data Analytics to detect, prevent, and prosecute CEHT activities.
- Legislative Frameworks: Enact and enforce robust laws and regulations that specifically target CEHT, ensuring penalties are severe enough to deter perpetrators.
- Capacity Building: Invest in training and capacity-building programs for law enforcement, judicial personnel, and frontline workers to effectively identify and respond to CEHT cases.
- Victim Support and Rehabilitation: Prioritize victim-centered approaches, providing comprehensive support, rehabilitation, and reintegration services to survivors of CEHT.
- Public Awareness and Education: Increase awareness among the general public, vulnerable populations, and businesses about the dangers of CEHT and how to report suspicious activities.
- Monitoring and Evaluation: Implement rigorous monitoring and evaluation mechanisms to assess the effectiveness of interventions and adjust strategies accordingly.

By integrating these strategies and maintaining a dynamic approach to evolving technological advancements and criminal tactics, it is possible to make significant strides towards controlling and ultimately eliminating CEHT.

Chapter

14

Civil Society Organizations(CSOs) and CEHT

Chapter 14

Civil Society Organizations(CSOs) and CEHT

14.1 Introduction

The pivotal role of NGOs or the CSOs in counter trafficking interventions has been reiterated multiple times in this research report. This has been reaffirmed by global experts and the law enforcers across the country. The inclusion of CSOs is seen as essential for the implementation of any viable strategy to combat human trafficking, and while political discourse offers many terms that are used interchangeably, the UN refers to civil society as the "third sector" (along with government and business). The essential role civil society plays in countering human trafficking is recognized in the main legal instruments against trafficking, namely the Protocol to Prevent, Suppress, and Punish Trafficking in Persons, especially Women and Children (Protocol against Trafficking in Persons) and the Council of Europe Convention on Action against Trafficking in Human Beings (Council of Europe Convention).

While traditionally, responses to human trafficking functioned within the paradigm of these 3 Ps i.e., Prevention, Protection, and Prosecution, yet as our understanding of human trafficking as an organized crime evolved, so did the global call for an organized response i.e. the 4th P - Partnership. The partnership and contributions of CSOs worldwide have played an important role in filling critical gaps in the fight against human trafficking, validating the need for stakeholders to come together with their specialized skills, expertise and no longer operate in silos.

In recognition of the central role played by CSOs in countering human trafficking, the United Nations Voluntary Trust Fund for Victims of Trafficking in Persons, Especially Women and Children (UNVTF) was established in July 2010 by the UN General Assembly. Administered by the United Nations Office on Drugs and Crime (UNODC), the Trust Fund's mandate is to provide humanitarian, legal, and financial aid to victims of trafficking in persons through awarding of multi-year grants to CSOs, who are on the frontlines tackling human trafficking. The CSOs provide critical assistance to victims including shelter, health services, psychosocial support, education, vocational training, and access to financial inclusion.

Several landmark legal cases highlight the critical role of CSOs in the emerging human trafficking landscape where technology has interwoven itself at every stage of the crime. The *Mariposa Case* in Austria involved a perpetrator challenging the integrity of the victims based on their online activities and stands as a landmark legal battle against CEHT. This was a pathbreaking case as digital evidence was collected by the case worker and the psycho-social worker of the

NGO- LEFÖ-IBF,[244] who worked hard to convince the police to look at the digital evidence and to take appropriate action as the culprits were all in Venezuela and the victims were in Austria. It brought to light the importance of victim-sensitive practices, collaborative efforts with CSOs, and comprehensive legal measures to address the challenges posed by human trafficking in the digital age. Efforts of organizations such as International Justice Mission, Prajwala, Thorn, and many other worldwide organizations has changed the course of anti-trafficking interventions in the world especially in the realm of CEHT.

The past decades have seen tremendous initiatives undertaken by the civil society across the globe in addressing the various issues of human trafficking. NGOs have combined forces with the police, lawyers, the judiciary, media, and the corporate sector, and involved them in strategies and processes for prevention, protection, rehabilitation, prosecution, and advocacy. The engagement and cooperation of civil society actors in anti-trafficking efforts became all the more relevant because of the complexity and ever-changing characteristics of the crime. Technological advances, including mobile connectivity, internet availability, and usage, have led to increased advancements, but have also created opportunities for predatory traffickers, and modified the form of abuse for those trafficked.

This chapters looks at the role of various CSOs both international and national in addressing CEHT and the experience of some Indian CSOs dealing with CEHT cases.

14.2 International CSOs and their Initiatives

14.2.1 National Centre for Missing and Exploited Children

The National Centre for Missing & Exploited Children (NCMEC) founded in 1984 by the United States Congress, is a private, non-profit organization that plays a crucial role in countering child abuse and human trafficking. NCMEC operates the Cyber Tipline which was established by Congress to process reports of child sexual exploitation (including sexual abuse, online enticement, and contact offenses); it reviews these reports and shares them with the appropriate law enforcement agency or Internet Crimes Against Children (ICAC) task force.

Recognizing the increasing role of technology in facilitating the crime of human trafficking, in 2023, NCMEC announced its release of the 'Take It Down' tool, a free-to-use service that allows users to anonymously report and remove "nude, partially nude, or sexually explicit images or videos" of underage individuals found on social media, blocking the content from being shared. Adults who appeared in such content when they were under the age of 18 can also use the service. Meta provided initial funding to create the service, while platforms such as Facebook, Instagram, OnlyFans, Pornhub, and Yubo have integrated the tool into their platforms.

14.2.2 POLARIS

Polaris, named after the North Star, a historical symbol of freedom, is leading a survivor-

244 LEFÖ IBF– is a non-profit, non-governmental organization founded in 1985 by a group of politically exiled Latin American women living in Vienna.

centered, justice-and-equity-driven movement to end human trafficking. Since 2007, Polaris has operated the U.S. National Human Trafficking Hotline, connecting victims and survivors to support and services, and helping communities hold traffickers accountable. Polaris also maintains the U.S. National Referral Directory and the Global Modern Slavery Directory, ensuring that partners everywhere have access to the information and resources they need.

14.2.3 ECPAT International

The International NGO, Ending Child Prostitution in Asian Tourism (ECPAT), seeks to end the sexual exploitation of children, including child sexual exploitation through prostitution, trafficking online, and in the context of travel and tourism, functions with a membership of 125 CSOs in 104 countries.

14.2.4 The International Centre for Missing & Exploited Children[245]

The International Centre for Missing & Exploited Children (ICMEC) is a CSO working against child sexual exploitation, abuse, and the risk of children going missing. It is headquartered in the United States, and works with partners around the world to develop research, technology, and educational resources, to aid in the search and recovery of children who are missing, fight online exploitation online, and empower professionals, institutions, and communities to safeguard children from all forms of sexual abuse. ICMEC started a project in July 2022 to combat online sexual crimes against children (OSCE), in partnership with NGOs and local police forces. ICMEC's 48-month project provides police units with the necessary specialized hardware, software, training, and technical assistance to effectively investigate OSCE, and support victims of sexual exploitation.

To ensure that cases of OCSE can be brought to trial and successfully reach conviction and sentencing, ICMEC has also been training prosecutors and judges. Their training is based on a victim-centric approach, including interview techniques to prevent revictimization. The project is funded by the U.S. Department of the State's Office to Monitor and Combat Trafficking in Persons and is implemented in partnership with the law enforcement and Cyber Peace Foundation.

Similarly, the work by International Justice Mission (IJM), terre des hommes (TDH), Save the Children, LEFÖ-IBF, Thorn etc., have called for strong action and coordination across borders and jurisdictions, to prevent and counter CEHT.

14.2.5 Terre des Hommes

Terre des Hommes Netherlands is an international NGO dedicated to preventing child exploitation, intervening in exploitative situations, and ensuring children's safety and development. Their primary focus is combating various forms of exploitation such as sexual exploitation, severe child labor, trafficking, and addressing issues like sexual and reproductive health rights and child protection during a crisis. They partner with local organizations, and implement projects to tackle these challenges. In February of 2023, Terre des Hommes Netherlands, together with the Bidlisiw

245 International Centre for Missing & Exploited Children (icmec.org)

Foundation, initiated a three-year project named "Safety for Children and their Rights Online (SCROL)" in the Philippines. The objective of this program was to guarantee the safeguarding of children from online sexual exploitation, and to establish secure family and community surroundings for them. Through its collaboration with local organizations, communities, government bodies, and the internet and technology industry, the three-year program aims to ensure that all the children are protected from online sexual exploitation and are in a safe family and community environment. The SCROL program, funded by the Dutch Postcode Lottery (NPL), operates in Cambodia, Nepal, the Philippines, and Kenya, as part of this effort.[246]

14.3 CSO Initiatives in India to Combat CEHT

In India, the partnership the CSOs have provided independently and in collaboration with state partners has brought out pioneering legal and institutional changes in the country. Several CSOs across India have played a ground-breaking role in identifying cases and bringing these to the notice of government authorities leading to policy and legislative enhancements in the anti-trafficking sector.

Across the nation several credible CSOs have played a critical role in implementing prevention interventions, initiating rescue operations, and providing holistic victim services. CSOs have also played a pivotal role in bringing to light the newer emerging dimensions of human trafficking, especially those that are technology-enabled, and have at their end put in efforts to evolve responses, and advocated for legal and policy reforms. Many of the landmark judgments in India related to strengthening the responses to human trafficking flow from such innovative actions of the CSOs.

Some of the prominent initiatives including legal efforts of CSOs across the country in countering human trafficking, CEHT, cyber safety, and cyber-crimes against children are summarized herewith.

14.3.1 Bachpan Bachao Andolan

Bachpan Bachao Andolan[247] (BBA) filed a petition in 2006, in the Supreme Court, highlighting serious violations and abuse of children who are forcefully detained in circuses. BBA found that most were trafficked from poverty-stricken areas of Nepal as well as from backward districts of India. The Supreme Court, on this petition, directed the Central Government to issue suitable notifications prohibiting the employment of children in circuses and recommend suitable schemes for their rehabilitation.

In 2012, BBA filed a Public Interest Litigation (PIL) in the Supreme Court stating that over one lakh children go missing in the country every year. The Supreme Court, vide order dated 17.01.2013, made it mandatory for police to register a FIR whenever a case of a missing child is reported to the police with the assumption that they were victims of kidnapping and trafficking.

246 https://www.terredeshommes.nl/en/latest/programme-launched-to-stop-online-exploitation-of-children-in-the-philippines-on#:~:text=Terre%20des%20Hommes%20Netherlands%20in,a%20safe%20family%20and%20community

247 Home – Bachpan Bachao Andolan (bba.org.in)

Furthermore, directions were also given for the preparation of a SOP to deal with cases of missing children, appointment, and training of Special Child Welfare Officers in every police station, and maintenance of records of recovered children along with their photographs.

14.3.2 Prerana[248]

The case *Prerana v State of Maharashtra* was a significant legal matter in which, Prerana, an NGO, had filed a petition in public interest to protect children and minor girls rescued from the flesh trade. The case aimed to address the issue of pimps and brothel keepers attempting to re-acquire possession of these girls after they were rescued. There are only two categories of children that courts in India have looked at, a) children who are trafficked and, b) children who need care and protection (those vulnerable to being trafficked). *Prerana v State of Maharashtra* case holds that children who are trafficked should also be considered children in need of care and protection, and not children in conflict with law.

In 2016, Prerana launched India's first Online Hotline through its Aarambh Initiative to report CSAM, in partnership with the UK-based Internet Watch Foundation.

14.3.3 Prajwala

Prajwala is the first CSO to legally demand for a comprehensive legislation to combat human trafficking. In *Prajwala vs Union of India* case, the implementation of the victim's protocol was demanded. In a Writ Petition filed by Prajwala[249] before the Hon'ble Supreme Court (WP No. 56/2004 titled *Prajwala vs Union of India & Others*), the final ruling in December 2015 directed to frame comprehensive legislation on human trafficking, and setting up of an Organized Crime Investigation Agency. NALSA in response to this public interest litigation framed the scheme namely, NALSA (Victims of Trafficking and Commercial Sexual Exploitation) Scheme, 2015 focusing on the prevention of trafficking, and restoration and rehabilitation of victims of trafficking. In another case, Prajwala's WP 1467/04 in Delhi High Court led to allowing video conferencing to be used for recording evidence of trafficked victims.

In 2015, the Hon'ble Supreme Court of India took suo moto notice of a letter written by Prajwala to the Chief Justice of India which was admitted as WP(Crl) 3/2015) pursuant to the videos of sexual violence circulated on social media platforms. Subsequently, in 2017, the court passed an order to constitute a committee under the Ministry of Information Technology to assist and advise the court for ensuring the non-circulation of videos depicting rape, gang rape, and child pornography, and made it completely unavailable for circulation. One of the recommendations from this was the need to create a Central Reporting Mechanism (India's hotline portal), as has been done in other countries, like in the United States with NCMEC. The landmark outcome in this case was the establishment of the cyber-crime portal by the Government which is the first of its kind reporting portal, and the establishment of the Indian Cyber-Crime Coordination Centre (I4C).

248 Prerana Anti-Trafficking, Mumbai (preranaantitrafficking.org)

249 Prajwala - Home (prajwalaindia.com)

14.3.4 CyberPeace Foundation[250]

CyberPeace Foundation (CPF) is a non-partisan civil society organization, a think tank of cyber security and policy experts with the vision of pioneering CyberPeace Initiatives to build collective resiliency against cyber-crimes and global threats of cyber warfare.

As a lead in CyberPeace advocacy, CPF is committed to advancing the ethos of, "Technology for Good" across international borders. The foundation's key areas of work include technology governance, policy evaluation, and advocacy, as well as capacity and capability enhancement, facilitated through partnerships with governmental bodies, academic institutions, and civil society organizations.

Some leading initiatives undertaken by the organization in recent times are:

i. eRaksha Competition Launch 2023-24, CyberPeace and National Council of Educational Research and Training

ii. PSA for #OnlineChildSafety, with CyberPeace & Missing Children

iii. Cyber Safety Awareness sessions, National Bal Bhavan, New Delhi

14.3.5 India Child Protection Fund[251]

The India Child Protection Fund (ICPF) partners with LEA across various states to combat Online Child Sexual Exploitation and Abuse (OCSEA) which encompasses sextortion, grooming, and other forms of digital harm with a focus on promoting both digital and online safety of children.

Objectives:

- Enable a paradigm shift in the understanding of OCSEA by advocating it as an organized economic crime.
- Bring forth functional changes in the behaviour of offenders, community, and children by increasing awareness.
- Create a legal deterrent through enhanced detection mechanisms for online and human interface.
- Develop capacities of LEAs, Prosecution, and Judiciary to combat OCSEA effectively.
- Increase accountability of ISPs and Online Social Platforms.

ICPF adopts a multi-pronged strategy in states with a high prevalence of crime against children, focused on Prevention and Deterrence, Detection and Reporting, and Response and Support. The first approach targets the setting up of dedicated CSAM units within LEAs, and aims to improve their efficiency by enabling them with tools, techniques, and tactics. The result is a higher capacity within cyber-crime units to detect, disrupt, and prosecute offenders. The second approach calls for organizing awareness campaigns in communities and schools through traditional means as

250 Uniting for Global Cyber Resilience | CyberPeace

251 Child protection india | India Child Protection Fund | Fund | ICPF |

well as social media. This is done in order to create virtuous cycles of both increased reporting and deterrence to potential perpetrators. The third approach was created with the intention of creating a system where all stakeholders understand and perform their roles. ICPF also advocates for increased accountability of intermediaries such as social media platforms. Through its partners ICPF ensures proper systems are in place for victims to access legal assistance, mental health, and rehabilitation support that provides for the healing of victims.

14.3.6 Akancha Srivastava Foundation[252]

Akancha Srivastava established the non-profit organization in 2017 following an encounter with intense cyber stalking. Motivated by this experience, she resolved to champion this cause, and spearhead India's campaign against cyber harassment. The social initiative called "Akancha Against Harassment" is dedicated to combating cyber harassment and empowering individuals to safeguard themselves against various forms of online abuse, including cyber stalking, bullying, cyber grooming, voyeurism, and revenge pornography. The Foundation provides various resources to support this mission, including a 24x7 helpline endorsed and backed by law enforcement agencies across India.

The organization raises awareness through the following channels:

i. Chatbot: Launched in 2018, this interactive tool educates users about cyber harassment and offers guidance on how to address it. It includes an SOS feature to connect users with the foundation for assistance.

ii. Workshops: These educational sessions are held in schools, colleges, and other institutions to inform and empower participants.

iii. Podcasts: Featuring guests from diverse backgrounds such as law enforcement, government officials, educators, legal professionals, mental health experts, and fitness professionals, these podcasts delve into various aspects of cyber safety and inform listeners about their rights and relevant laws.

14.3.7 The Centre for Cyber Victim Counselling[253]

Centre for Cyber Victim Counselling or CCVC was founded in 2009 by Professor Debarati Halder and Professor K. Jaishankar. It is an NGO that works for the victims of cyber-crime in India and helps the victim understand the nature of the crime that has happened to them as well as helping them to initiate action against the offender. Furthermore, they guide the victim to understand the present legal scenario and help them reach the police when needed. Highlights of their goals:

- To counsel victims of cyber-crime, and to work for the prevention of crime in cyber space.
- To protect potential victims from cyber-crimes.

252 https://akanchaagainstharassment.com/

253 Centre for Cyber Victim Counselling (CCVC) - Helping Cyber Crime Victims (cybervictims.org)

- To disseminate the knowledge of Cyber-Crime Laws and to undertake preventive measures.
- To publish journals, newsletters, books, pamphlets, booklets, and other periodicals. Besides these, they also develop audio-visual materials on cyber-crime, and distribute the same to increase and improve the awareness of cyber-crime in India.
- To hold conferences, seminars, symposia, workshops, and other scientific meetings and dissemination of information on cyber-crime, and for spreading awareness about cyber-crime and preventive measures.

14.3.8 The RATI Foundation for Social Change[254]

RATI foundation, formerly Aarambh India is headquartered in Mumbai, focused on establishing safe environments and communities to protect children from sexual violence. Their efforts encompass various approaches, including offering direct support to victims, addressing digital safety concerns, enhancing child protection systems within governmental and non-governmental entities, educating stakeholders, advocating evidence-based policies to policymakers, fostering networks among organizations nationwide, and creating communication materials.

Additionally, they collaborate with the UK-based IWF to operate India's first internet hotline for reporting instances of CSAM discovered online.[255] In May 2016, in partnership with IWF they launched India's first reporting button for child sexual abuse images and videos on the Internet. The reporting button enables citizens of India to report child sexual abuse images and videos in a safe and anonymous environment. If the content is found to be illegal it will be blocked and taken down irrespective of where it is being hosted. National Hotline for Reporting Child Sexual Abuse Imagery works closely with government, police, and the internet industry in India.

India's first online resource center on CSA is www.aarambhindia.org. It is an attempt to create a comprehensive, interactive and up-to-date resource pool and directory. It encompasses everything from the fundamentals of CSA to its various complexities.[256]

14.3.9 Bodhini[257]

Bodhini is an NGO working in the space of online safety, body safety, healing and wellness since 2014. Bodhini works mainly on educating individuals to use online space safely and helps them to move forward with positivity and healing, firmly believing that every individual has a right to a life free from fear, thus carrying the tagline of, "freedom from fear".

254 Home - Rati Foundation

255 https://aarambhindia.org/about/#y-aarambh

256 ABOUT | Aarambh India

257 NGO in Kerala, Kochi | Working in the space of online safety, body safety and healing. (bodhini.in)

14.3.10 International Justice Mission

Since 2011, IJM India has been working with the government to address human trafficking and has collaborated with the government on Judicial Colloquiums, workshops, and trainings for State and District government officials, public prosecutors and police officers. IJM supports government efforts in the implementation of protection programmes to combat human trafficking and provides subject matter expertise for successful and sustainable solutions towards building a safe and self-reliant country.

IJM works with the state and central government as well as with the AHTU and police to ensure justice for victims of trafficking of both sex trafficking and bonded labor. They work alongside government officials and grassroots organizations to rescue and rehabilitate victims, prosecute offenders, and train public justice officials.

IJM has assisted the police in rescuing victims of trafficking who have been sexually exploited for commercial purposes by collaborating with the local police and AHTU. They also help rescue victims of bonded labor by collaborating with State and District government officials, police and police units like the AHTU, and quasi-judicial bodies like the NHRC.

14.3.11 Impulse NGO Network

Impulse NGO Network (INGON) is a non-profit organization founded in 1993. The software, Impulse Case Management Centre (ICMC), developed by this organization, is at the heart of their work. ICMC records, compiles, and keeps track of all relevant information on human trafficking cases. ICMC created a case database system to provide updated information on human trafficking cases and on suspected human traffickers that is also continuously shared with AHTUs across India. Once a trafficked person's case is reported, ICMC then focuses on meeting the needs of such victims starting with informing law enforcement of a rescue, followed by post-rescue counselling, medical care, legal aid, rehabilitation, repatriation, reintegration, and re-compensation. All AHTUs have a specific user account provided by the system, thus enabling them to view and edit only cases that have been registered or referred to them. This ensures that necessary confidentiality and privacy standards are followed. The software also has an alert-feature that indicates if another unit is, or has been, managing a case involving the same trafficked victim or the same trafficker.

14.3.12 Shakti Vahini

Shakti Vahini works closely with law enforcement agencies including AHTUs to reduce demand on human trafficking by facilitating and promoting investigations in cases of trafficking for sexual exploitation, bonded labor, child labor, and forced marriages, resulting in prosecution of traffickers and breaking of the organized crime.

India Cyber TIP Helpline is an initiative of Shakti Vahini, to facilitate victims/complainants to report cyber-crime complaints online to various law enforcement agencies. India Cyber TIP Helpline works in partnership with various Cyber Nodal Agencies of State Police across the country. This initiative caters to complaints pertaining to cyber-crimes with special focus on cyber-crimes against women and children. Complaints reported on this Helpline are reported promptly to law

enforcement agencies/police based on the information available in the complaints. India Cyber TIP Helpline also follows up the cases and ensures strict action through partnership with various state police agencies.

14.3.13 Bal Kalyan Sangh

Since 2011, Bal Kalyan Sangh (BKS) is a nodal organization for Childline India, which is a project of the Ministry of Women and Child Development. Childline is India's first 24-hour free emergency phone service for children in need of care and protection. BKS is running two Children's Home in Jharkhand with the support of Department of Women, Child Development and Social Security, Government of Jharkhand. Both Homes are Residential Childcare Institution for Child in Need of Care and Protection.

BKS is also running a State Resource Centre at Ranchi and Integrated Resource-cum-Rehabilitation Centre (IRRC) project at New Delhi, supported by the Department of Women, Child Development and Social Security, Govt. of Jharkhand. The objective of the establishment of these two coordination Centres is to facilitate rescue of victims, identify survivors staying in various shelter homes of Delhi, and coordinate with local administration and other stakeholders to facilitate support services like medical examination, lodging of FIR, wage compensation, legal aid, and ensure safe repatriation to home state.

14.3.14 Jan Jagran Sansthan

Jan Jagran Sansthan (JJS) was initiated in the year 1980 as a local non-governmental organization to strengthen women and child protection in Bihar. Due to its demonstrated capacities to transform the population living in marginalized and vulnerable situations; within a decade, JJS was known as a state level institution in Bihar, and within a few years it had increased its reach across Jharkhand, Haryana, and Chhattisgarh, to focus on the development of primarily Dalits, minorities and tribal population. At present, the organization is playing a pivotal role in stoppage of trafficked women and children along the borders of Nepal and Bangladesh.

14.4 Cyber-Enabled Human Trafficking - The Grassroot Experience of CSOs

In order to understand the nature of cases that CSOs have encountered on the ground related to CEHT, a special consultation was held with select organizations who had actually dealt with such cases. The aim was to understand the crime from the CSO perspective and corroborate with the findings gained from the law enforcement officers.

The framework for the discussions centered on the following themes:

A. **Real Time Case Experiences** on the ways and means by which cyber technologies have been used in committing the crime.

B. **Involvement of Technology Enablers and Technology Companies**, whether certain technologies, by their very design, are facilitating human trafficking and are CSOs able to identify this, and if any action has been taken by them against any Technology Company.

C. **Technological Solutions and Innovations**, which has enabled prevention or facilitated rescue work of potential and real victims of CEHT.

D. **Partnerships and Alliances** which CSOs have engaged in with law enforcement agencies, at the ministerial level or with technology companies such as Facebook, Instagram, Twitter, etc.

A. CEHT Case Experiences

Discussion with the CSO partners brought to light seven cases of human trafficking and a public interest litigation, whereby different social media platforms and messaging apps such as Facebook, Instagram, Whatsapp, and PUBG (a gaming platform) were used in the process of spotting, recruiting, and exploiting victims for purposes of sexual and labor exploitation.

Case 1: Sex Trafficking via Social Media

This case (156/2017 Palghar Session Court) involved a young teenage girl who had expressed her love to dance on social media and was approached on Facebook by a so-called dance group member to come to Mumbai to pursue her talent and then got trapped in a sex trafficking racket. The modus operandi being used by the traffickers was to use girls who had already been trapped by them to recruit other girls to travel to Mumbai for auditions, and thus establish a "peer to peer communication" mode to instil confidence and trust, i.e., a victim being forced to bring in another victim. An ad agency was also involved in the uploading of dance videos.

With the ease of technology, traffickers in this case were able to identify and transfer victims without the need for physical movement. The ticket bookings for the travel were done online, with no cash payment involved, thus leaving no trail anywhere.

IJM in collaboration with the law enforcement and through the use of surveillance, Facebook analysis, and open-source intelligence[258] were able to crack this case within a year and half long operation, resulting in the arrest of 18 people. Facebook analysis revealed that the trafficking ring had groups operating online to spot and recruit vulnerable victims. This particular operation was being run by a Bangladesh trafficking network in Mumbai who were yearly exploiting over 400 girls using social media apps, such as Facebook, to spot and recruit vulnerable girls. Once these girls were trapped, they were used to lure further victims into traveling to Mumbai to pursue their passion by sharing fake success stories.

Interestingly, the kingpin of this trafficking operation showed that his income was the result of earnings as a vegetable vendor and one of his accounts had close to ₹92,00,000/- (USD 110,164) which he claimed was earned from selling vegetables across states in India.

Case 2: Grooming on Social Media

Through Facebook a minor girl was befriended by a person living in Bangalore and groomed online for 3 months. After gaining her trust, the accused exchanged numbers with her and started chatting with her on WhatsApp. He made her to believe that he would provide her with employment

258 Open-source intelligence (OSINT) is the collection and analysis of data gathered from open sources (covert sources and publicly available information; PAI) to produce actionable intelligence.

and without informing her family the girl travelled to meet with him, where she was put in a hotel and was about to be trafficked to another country but was rescued in time. It was found that the travel and hotel bookings were done through an international number, indicative of an international ring. This case (Laitumkhrah Police Station Case No HPR7/2017) was handled by INGON.

Case 3: Cross-Border Trafficking via Social Media

Girls from Nepal were being trafficked to Myanmar through the Moreh border. Girls were recruited through Facebook, and either offered a marriage proposal or employment. In this instance the young girl was offered a job and asked to travel to Delhi. All her messaging accounts were blocked by the trafficker, except Facebook, through which she managed to contact friends for help and was rescued with the support of INGON.

Case 4: Instant Messaging App and Child Trafficking

A 14-year-old vulnerable girl from rural Jharkhand would talk to her neighbour over WhatsApp about her poor financial situation. The accused gained her confidence and told her to come to Delhi. Once she reached Delhi, she was housed in a placement agency known to the accused and was abused physically, and later kept in domestic servitude in a remote location. The victim was from a rural background and did not know anyone to contact or any details of her surroundings/owner. She only knew her teacher and contacted her who in turn contacted Bal Kalyan Sangh through their helpline and the victim was rescued by Delhi Police by their consolidated efforts.

Case 5: Luring by Love on Social Media

A young vulnerable 15-16 year old minor girl fell in love with a boy she met on Facebook who lured her into coming to Delhi for a better life. The accused would speak to her in her regional language which led her to trust him easily. Once she travelled to Delhi, she was housed in a placement agency, and sexually abused. She was rescued with the support of the Bal Kalyan Sangh.

Case 6: Instagram and Trafficking

The victim was a 17-year-old minor girl, who was a resident of Jalpaiguri, West Bengal. She wanted to pursue her career as a dance professional and used to actively post her dance videos on Instagram. It was through this social media platform that she met the accused, who posed himself as a dance teacher in New Delhi. He presented himself as being one of the participants at the India's Got Talent, and promised her a career as a professional dancer in the city. Without informing her parents, she came to Delhi and on reaching Delhi she was confined by the accused and forced into sexual exploitation. From Jalpaiguri, she was first trafficked to Bulandshahr (District in Uttar Pradesh) and from there to New Delhi, where she was rescued in a joint rescue operation by Shakti Vahini along with the New Delhi Crime Branch (Jalpaiguri; Rajganj P.S Case No: 248/2021).

Case 7: Online Gaming and Trafficking

A minor girl of 15-16 years of age, was lured through the online gaming platform PUB-G, into coming to Delhi by two men, with whom she used to frequently play on the gaming platform. The rescue in the case was conducted by Shakti Vahini in coordination with the Delhi Commission for Women and the IGI Airport Police officials. As soon as her flight landed at the airport, the minor girl was immediately rescued from the Terminal 3, IGI Airport before she could be pushed into exploitation (Jalpaiguri; Dhupguri P.S Case No. 45/ 2024).

Case 8: Escort Services and Sex Trafficking

PIL filed in Bombay High Court over sex rackets being run under the guise of escort services.

The State was pulled up by the Court for its poor investigation into online advertisements offering escort services which was a front for running sex rackets, which led to IJM being contacted by the Mumbai Police. After scraping over 500 websites, it was observed that a single individual was creating and operating multiple profiles, and was using cash deposit machines, whereby the kingpin would withdraw money elsewhere and was used an old Nokia handset to avoid being traced. Investigations resulted in multiple individuals who were a part of this entire chain being caught.

IJM also shared an online website known as, International Sex Guide used by frequent travellers that provides information to customers on where they can access girls, etc. This was a paid service which provided photos of girls, details of hotels, pimps, etc city wise. Customers could also communicate with each other and share their experiences.

B. Role and Accountability of Technology Enablers

It was observed by the CSOs that while previously recruitment involved physical movement, now social media apps were being easily used to spot and recruit victims. Due to the ease and anonymity offered by encryption, it has become increasingly difficult to track conversations. Instant Messaging Apps such as WhatsApp are used to share images of girls and payments are also made online. Opening fake accounts and creating fake profiles is simple as no identity verification is required.

Moreover, post-Covid-19 pandemic a huge increase was seen in cases of child trafficking and exploitation, due to increased online activity of children. Through these cases, traffickers are also seen to be highly organized with clear bifurcation of roles and functions such as bar owners, pimps, taxi owners, etc.

BKS shared that many of these placement agencies are established under names of "Tribal Welfare Trust" or use names of prominent tribal people such as Birsa Munda (tribal reformer, religious leader, and freedom fighter belonging to the Munda tribe). The trust of the victim is gained by becoming friends with them and entering into a romantic relationship with them.

In the case involving the escort services websites, IJM shared that Maharashtra Cyber Police had deposited the URL of such websites in Court and got them blocked, and no ownership was taken by the website operators. While it was observed, that when one website was shut down, another opened in its place, and the Court stressed tha this could not be taken as a reason to not take action, but rather need to be highly vigilant in tracking and tracing these cyber criminals.

The accountability of technology enablers is a critical component to focus on as they can play a significant role in detection and removal of content, and also provide assistance to LEA in investigation of such crimes. However, it was noticed that none of the CSOs had attempted to make technology firms accountable for the safety of their platforms. The focus has largely been on the rescue and provision of protection services to the victims. As observed through the interactions, the ways and means in which technology has been misused and fixing accountability on the technology firms in facilitating such crimes has not been a part of CSO interventions.

C. Tech Solutions and Innovations

A major lacuna observation was that law enforcement lags in terms of technological know-how, and needs to be brought up to date with the latest technological developments, through training and capacity building, which is being provided by CSOs.

IJM shared that Open-SourceAI intelligence is a very potent tool that can be used to conduct a preliminary enquiry on the suspects and victims as well as create a database. Efforts are also ongoing to customize tools and set up a Resource Centre to function as a Trafficking Database of customers, establishments, traffickers, etc. IJM is also working towards skill upgradation programs for LEA. INGON shared that it has software that documents all cases and tracks the face of the accused. As mentioned previously, ICMC is a case database that provides updated information on human trafficking cases and on suspected human traffickers, which is also continuously shared with AHTUs across India. Shakti Vahini and Impulse are trusted Facebook Flaggers.

D. Partnerships and Alliances

IJM provides training and capacity building to Law Enforcement Officers, teaching them google dorking i.e. an advanced level of google search and training. Furthermore, focus is on proactive investigation whereby Investigative agencies are being taught to look for transactions that are fraudulent e.g. multiple transactions taking place during the nights. It has been observed that call data records are not sufficient for courts as they are merely supportive evidence.

As Impulse and Shakti Vahini are trusted flaggers of Facebook, any message flagged by them is looked into on priority basis by the technology company, and the location of the victim can then be shared with the law enforcement. In a case where a girl was traveling by train via Vizag, she was quickly intercepted, and rescued by the use of this flagging technology.

Shakti Vahini is operating the CyberTipline since the Covid-19 pandemic. They have a strong partnership with National Commission for Protection of Child Rights and State Police for carrying out interstate rescue operations. In a case where a child victim was in Netherlands and the perpetrator who created the CSAM content was in Gurgaon, Shakti Vahini coordinated with Gurgaon police to crack the case.

BKS too operates a toll-free number and TIP line, and is involved in providing training and capacity building for law enforcement.

14.5 Insights from CSO Interactions

As is evident, CSOs are an indispensable component of the anti-trafficking efforts globally and in India, supplementing the efforts of relevant stakeholders, from prevention to rescue to prosecution and rehabilitation. However, interactions with CSOs revealed that many organizations are still at a nascent stage of understanding of the forms and manifestations of CEHT, and are yet to integrate this lens into how such cases are to be viewed and investigated, in collaboration with the law enforcement and criminal justice machinery. Further, while the focus of CSOs in the country is shifting towards exploring and understanding the role of the digital medium in facilitating and

commissioning crimes, the understanding largely remained limited to crimes against children i.e. CSAM and OCSE.

The strengths and gaps in CSO efforts can be summarised as follows:

The strengths:

- Policy and Legislative Advocacy, as evidenced through the legislative actions of NGOs such as Prajwala, Prerna, BBA, etc.
- Prevention and Awareness Campaigns, as seen in the work of Cyber Peace Foundation, ICPF, Shakti Vahini, etc.
- Intelligence Gathering and Crime Detection, as most CSOs are trusted members of the community and in many instances survivors are also a vital source of intelligence.
- Rescue operations in partnership with LEA (inter and intra state).
- Training and capacity building of law enforcement officers and other stakeholders, as witnessed through the efforts of IJM, Shakti Vahini, BKS, Prajwala, etc.
- Provision of shelter homes, victim assistance and protection services.
- Running of Helplines and Cyber TIP lines, such as those set up by Shakti Vahini, BKS, Rati Foundation, etc.
- Running of Resource Centres and setting up of Data Management Centres.
- Partnership with Technology companies such as Facebook, in identifying and flagging inappropriate content, identifying location of victim, etc, as evidenced by the case work of INGON and Shakti Vahini.
- Assisting law enforcement in surveillance and investigation, using technology tools such as open-source intelligence, web scraping, Facebook analysis, etc as evidenced by the successful operation of IJM in supporting the cracking of a Bangladesh trafficking racket operating in Mumbai.

The gaps:

- Low levels of awareness, understanding, and reporting of human trafficking cases as CEHT. The need to include looking at technology as a facilitator/enabler.
- Lack of understanding of roles and responsibilities of the Technology Enablers/Platforms in combating CEHT.
- The scale of CSO responses is not proportionate to the scale and magnitude of the fast growing problem.
- The geographical coverage of responses and interventions is not uniform, with focus being in the areas where few NGOs are working on this issue are centered/located.

- Limited capacity to identify, investigate, prosecute, and adjudicate CEHT by key stakeholders
- Understand and establish linkages with other crimes.

However, despite these limitations, CSOs remain at the center of anti-trafficking operations playing a critical role in victim protection and assistance.

Against this backdrop and seeing the road ahead, it is of utmost importance to institutionalize, that is, to regulate and guide the working relationship between law enforcement and the criminal justice machinery and CSOs. This should be done with a view to prevent the crimes, better protect and assist trafficked survivors, create an environment in which they feel safe and secure to participate in the criminal investigation, and where all stakeholders come together as one to end CEHT.

Chapter

15

International Initiatives and CEHT

Chapter 15

International Initiatives and CEHT

15.1 Introduction

One of the key findings that emerged during the course of the research was the universal access that traffickers have enabling them to operate with impunity, raising several questions on the efficacy of international initiatives in countering trafficking. Thus an effort was made apart from engaging with practitioners globally to undertake a brief desk review of existing international initiatives.

In the upcoming chapter, we explore a range of international initiatives and institutions engaged in combating CEHT. These initiatives encompass efforts by the United Nations agencies, regional organizations, law enforcement agencies, and civil society groups to address various facets of CEHT, including prevention, investigation, victim support, and policy advocacy. The initiatives included in the chapter are not exhaustive, but provide an overview of the initiatives taken globally and give a bird's eye view on the possible gaps that needs to be plugged.

15.2 Multi-Lateral Initiatives

A. The United Nation's Commission On Crime Prevention and Criminal Justice (CCPCJ)

One of the most significant organizations that have systematically targeted CEHT is the United Nation's Commission on Crime Prevention and Criminal Justice (CCPCJ). The Commission falls under the United Nation's Economic and Social Council. The Commission established by the Economic and Social Council (ECOSOC) resolution 1992/1, was upon request of General Assembly (GA) resolution 46/152, as one of its functional commissions. The Commission functions as the main policymaking entity within the United Nations concerning crime prevention and criminal justice. Its mandates and priorities, outlined in the resolution 1992/22 by ECOSOC, encompass enhancing global efforts against both national and transnational crime, and improving the effectiveness and fairness of the criminal justice systems. Additionally, the CCPCJ serves as a platform for member states to exchange knowledge, expertise, and information to develop strategies at both national and international levels for combating crime.[258]

It convenes regular annual sessions along with intersessional meetings, and towards the conclusion of each year, holds a reconvened session to address administrative and budgetary

258 https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html

matters as the governing body of the UN's crime prevention and criminal justice program. In their twenty-seventh session held in Vienna, Austria, from May 14-18, 2018, the Commission systematically and categorically adopted various draft resolutions that highlight the interlinkages of the abuse of technology for facilitating the trafficking of human beings.

Some of the important draft resolutions and decisions are:

1. Draft Resolution on, "Preventing and combating trafficking in persons facilitated by the criminal misuse of information and communications technologies."[259]

   It aimed to recognizing that traffickers are taking advantage of information and communications technologies to reach larger audiences and to carry out criminal activities more quickly and efficiently.[260]

2. Draft Resolution on, "Improving the protection of children against trafficking in persons, including by addressing the criminal misuse of information and communications technologies."[261]

   This draft resolution aimed at improving the protection of children against trafficking in persons including by addressing the criminal misuse of information and communications technologies

3. Draft Resolution on, "Strengthening measures against trafficking in persons"

   This draft resolution sought to draw attention to the need to address the new challenges generated by the rapid development and potential for criminal misuse of the Internet and other information and communications technologies that are used to facilitate trafficking in persons, including for the purpose of exploiting women and children, and to recruit and harbor victims. It does however factor in that, information and communications technologies can assist law enforcement and criminal justice authorities in preventing and combating trafficking in persons.[262]

B. The United Nations Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime (UNODC) is a specialized agency of the United Nations responsible for addressing issues related to drugs, crime, corruption, and terrorism. Established in 1997 through a merger of the United Nations Drug Control Programme and the Centre for International Crime Prevention, UNODC operates across the globe to support member states in their efforts to tackle transnational threats to security and stability. Within the UN system, the UNODC is the custodian of the UN Convention against transnational organized crime. In addition to the above, Resolution 27/2 of 2018 of the CCPCJ, has mandated UNODC to, "continue providing

259 Draft resolution No E/CN.15/2018/L.2/Rev.1 available at https://undocs.org/Home/Mobile?FinalSymbol=E%2FCN.15%2F2018%2FL.2%2FRev.1&Language=E&DeviceType=Desktop&LangRequested=False

260 https://documents.un.org/doc/undoc/ltd/v18/032/95/pdf/v1803295.pdf?token=HPu1nk4XE1EPEKvtwj&fe=true

261 Draft resolution No E/CN.15/2018/L.3/Rev.1 available at https://undocs.org/Home/Mobile?FinalSymbol=E%2FCN.15%2F2018%2FL.3%2FREV.1&Language=E&DeviceType=Desktop&LangRequested=False

262 Draft Resolution No. E/CN.15/2018/L.8/REV.1 available at https://documents.un.org/doc/undoc/ltd/v18/034/05/pdf/v1803405.pdf?token=zHqR5frqIiJrgOWwgB&fe=true

within its existing mandate, technical assistance and training to Member States, in particular developing countries, at their request, to improve and build capacities to prevent and combat trafficking in persons that is facilitated by the criminal misuse of information and communications technologies, and to utilize technology to prevent and address such trafficking."[263]

Article 32 of the UN Convention against Transnational Organized Crime mandates creation of a working group on Trafficking in Persons. The group has official representation from Member States including India. The issue of technology penetrating into human trafficking has been acknowledged by the working group on trafficking for more than 10 years and in 2013 during the time of the fourth meeting of the working group, while looking at addressing the demand in trafficking, the committee noted as under:

"*33. States parties should take into consideration new methods of recruiting victims of trafficking in persons and take measures to develop targeted awareness-raising campaigns and specialized training for law enforcement and criminal justice practitioners on issues such as the use of the internet by traffickers, in particular to recruit children.*"[264]

In 2021, the group deliberated on, "Successful strategies for addressing the use of technology to facilitate the trafficking in persons and to prevent and investigate trafficking in persons." Key recommendations that emerged from this working group was primarily recommending to the States to acknowledge CEHT and use technological tools to raise awareness of trafficking, use it to gather evidence, prevent crime and learn the trends.[265]

UNODC also brings out a Global Report on Trafficking in Persons every year documenting cases of trafficking, trends and patterns, national interventions, etc. The Global report of 2020 extensively documented CEHT. In 2021 a Report on the Effects of the Covid-19 pandemic on Trafficking in Persons elucidated how traffickers exploit crises and capitalize on online platforms to perpetuate trafficking crimes.[266]

In September 2023 with support from the Canadian Government, UNODC released a policy report titled, "Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia."

In cooperation with the People's Republic of China, UNODC and ASEAN finalized a strategic plan to combat transnational crime in forced criminality in casinos and online scams.

- *Submissions and Publications:*

  UNODC actively contributes to the global discourse on human trafficking through submissions to key reports and publications. For instance, the agency's submission to the Report of the UN Special Rapporteur on Contemporary Forms of Slavery highlights the misuse of technology

263 Unodc.org; E/CN.15/2018/L.2/Rev.1 Preventing and Combatting trafficking in persons facilitated by criminal misuse of information and communications technology; May 16, 2018

264 Report on the meeting of the Working Group on Trafficking in Persons held in Vienna from 6 to 8 November 2013; accessed from CTOC/COP/WG.4/2021/2 on April 1, 2024.

265 Background paper for the Working Group on Trafficking in Persons, unodc.org; accessed on April 1,2024

266 https://unodc.org/documents/human-trafficking/2021/The_effects_of_the_COVID-19_pandemic_on_trafficking_in_persons.pdf

in facilitating trafficking crimes.[267] It also produces briefs and practical guides, such as the Practical Guide for Requesting Electronic Evidence across Borders,[268] to support practitioners and policymakers in addressing CEHT.

- *UNODC Education Initiatives:*

Under the Education for Justice (E4J) initiative,[269] UNODC develops educational resources to raise awareness and build capacity in addressing human trafficking and cyber-crime. The university module series on trafficking in persons and cyber-crime equips academics with tools to educate students about the multifaceted challenges posed by CEHT. Through these initiatives, UNODC aims to empower stakeholders with knowledge and skills essential for combating human trafficking effectively. In addition to the above, it also engages with local governments to provide capacity- building sessions bringing in regional and international experts.

- *South Asian Initiatives*

The Covid-19 pandemic presented unfathomable challenges in the area of law enforcement and governance. In particular, when it comes to CEHT the pandemic triggered an unprecedented (mis)use of modern communication technologies and the online realm for illicit activities such as human trafficking. One such peculiar challenge presented by this situation was ensuring continuity in the education of children while protecting them from online predatory behaviour. Another overbearing aspect of this situation was the fact that the challenges presented by the pandemic greatly limited the capacity of the state and NGOs to counter criminals and protect victims. UNODC recognized the pressing need for advanced capacity-building efforts to tackle emerging threats, particularly CEHT.

To address this, they conducted a series of trainings across six South Asian countries from September to December 2020. These trainings, supported by the Swedish Government, focused on strengthening national and regional responses. They were conducted either online or in a hybrid format, combining local and online sessions to accommodate diverse participants. The trainings targeted a wide range of stakeholders, including law enforcement officials, border guards, NGOs, and government representatives. Discussions during the sessions highlighted the importance of leveraging technology to combat trafficking and emphasized evidence-based, coordinated responses for comprehensive victim protection.[270]

C. Special Rapporteur On Trafficking In Persons Especially Women And Children

At its 60th Session, the Office of the United Nations High Commissioner for Human Rights (OHCHR) decided to appoint for a three-year period a Special Rapporteur on Trafficking in Persons especially for women and children. The period gained extension from time to time, and in June 2023 it received extension for another three years. Within the UN system, there is a belief that the Special

267 https://www.ohchr.org/sites/default/files/documents/issues/slavery/sr/cfi78thga/submissions/submission-slavery-ga78-un-unodc.pdf

268 https://www.unodc.org/documents/treaties/WG_TiP_2021/CTOC_COP_WG.4_2021_2/ctoc_cop_wg.4_2021_2_E.pdf

269 https://www.unodc.org/e4j/

270 https://www.unodc.org/southasia//frontpage/2020/December/south-asia_-unodc-trains-frontline-responders--law-enforcement-to-counter-cyber-enabled-human-trafficking-amid-Covid-19.html

Rapporteur is the, "only exclusively focused international human rights mechanism for combating human trafficking".[271] The Office takes action on violations committed against trafficked persons and on situations in which there has been a failure to protect their human rights; undertakes country visits to study the situation and formulate recommendations and submits annual reports to the UN Human Rights Council and the General Assembly.

OHCHR released a briefing paper addressing human rights concerns arising from online scam/fraud operations, particularly in Southeast Asia. This paper highlights the link between online scams/frauds and human trafficking since early 2021 and provides recommendations based on international human rights standards.[272]

D. International Organization for Migration (IOM)

The International Organization for Migration (IOM) is an intergovernmental organization in the field of migration. It supports migrant population around the world in diverse ways with safe migration policies/practices being top on the agenda. It is part of the UN system as a related organization. In view of the intrinsic connection between migration and trafficking, IOM has been addressing human trafficking as part of its initiatives. Over the years, it has also undertaken significant initiatives to combat CEHT, addressing emerging challenges in Southeast Asia. In the last few years, IOM has published various reports on trafficking.

In March 2023, IOM published a situation analysis on Trafficking in Persons for the purpose of forced criminality. This was followed by the second regional situation analysis on Trafficking in Persons for forced criminality in Southeast Asia's online scamming centers. This analysis offers practitioners, policymakers, and the donor community a concise overview of counter-trafficking initiatives in the region. The report provides valuable insights into the prevalence of trafficking for forced criminality, particularly in online scamming centers, and offers recommendations for addressing this issue.[273]

In addition to the above, IOM has been providing direct support to victims of CEHT in partnership with local governments in Indonesia and Thailand. In the region, IOM has been a key player is promoting initiatives to address CEHT. According to the organization, the initiatives summarized are as under:

- Implementation of existing ASEAN instruments, such as the ASEAN Convention Against Trafficking in Persons.
- Establish Partnerships with the private sector, civil society organizations, and academia to foster innovative solutions, and develop preventive measures.
- Mutual legal assistance in TIP cases through the effective implementation of ASEAN Treaty on Mutual Legal Assistance in Criminal Matters.
- Setting a minimum standard of protection at the regional level for victims of trafficking.

271 Ohchr.org>special-procedures; accessed on April 1, 2024

272 https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

273 https://roasiapacific.iom.int/sites/g/files/tmzbdl671/files/documents/2024-03/iom-southeast-asia-trafficking-for-forced-criminality-update_december-2023-1.pdf

- Initiate development of a regional referral mechanism through leveraging existing ASEAN mechanisms to avoid revictimization, re-traumatization, and the continuing exploitation of victims.[274]

IOM has been a key player in the formation of the ASEAN Leaders declaration on combatting trafficking in persons caused by the abuse of technology.

In the last few years, IOM has been proactive in addressing CEHT especially cases of cyber scamming which includes participating in key meetings with the governments, spearheading dialogue, providing support to victims, strategizing interventions and providing overall support to all key stakeholders.

E. The International Criminal Police Organization (INTERPOL)

INTERPOL, established in 1923, is the world's largest international police organization, facilitating cross-border police cooperation and crime prevention efforts among its 195 member countries. Its mission includes combating a wide range of criminal activities, with a particular focus on human trafficking, migrant smuggling, and child sexual exploitation. INTERPOL has undertaken significant initiatives to combat CEHT, recognizing the challenges posed by the digital era. These initiatives include:

- *Publishes News Articles regarding CEHT:*

  INTERPOL issued a series of news articles addressing the interconnected nature of human trafficking and financial crime. These articles serve as a global warning, emphasizing the need for heightened vigilance and international cooperation to combat fraudulent activities linked to human trafficking. By raising awareness through its news publications, INTERPOL aims to mobilize law enforcement agencies and the public in the fight against CEHT.[275]

  In the year 2023 the Organization issued an Orange Notice to its membership on the trend of large-scale cyber-enabled human trafficking where victims are lured through fake job ads to online scam centers and forced to commit cyber-enabled financial crime on an industrial scale. They issued a global warning regarding a serious and imminent threat to public safety.

- *Operations Targeting Human Trafficking Networks*:

  INTERPOL, as the world's largest international police organization, conducts numerous operations aimed at combating various forms of transnational crime. Among these operations, two notable initiatives stand out: Operation Storm Makers and Operation Narsil.

  - Operation Storm Makers:

    Operation Storm Makers, aimed at dismantling criminal networks involved in migrant smuggling and human trafficking. This operation resulted in 121 arrests

274 IOM situation report, February 2024; roasiapacific.iom.int;

275 https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud

across 25 countries, demonstrating INTERPOL's commitment to disrupting transnational trafficking networks and protecting vulnerable individuals.[276]

- Operation Narsil:

  Operation Narsil is a two-year global operation targeting networks of child sexual abuse websites generating profits from advertising. This operation, conducted from December 2021 to July 2023, focused on dismantling the websites and the finance mechanisms used by their administrators. Operation Narsil showcases INTERPOL's proactive approach to combating online child exploitation and disrupting criminal activities on the internet.[277]

- *Proposal for a Comprehensive International Convention*:

  INTERPOL has proposed a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. This proposal reflects INTERPOL's commitment to enhancing international mechanisms for police cooperation in addressing emerging threats in the digital realm. By advocating for this convention, INTERPOL aims to promote the interests and needs of the global law enforcement community in combatting cyber-enabled crimes, including human trafficking and online exploitation.[278]

F. The Inter-Agency Coordination Group against Trafficking in Persons (ICAT)

The Inter-Agency Coordination Group against Trafficking in Persons (ICAT) is a policy forum established by the UN General Assembly with a mandate to enhance coordination among UN agencies and other relevant international organizations. Its primary objective is to facilitate a holistic and comprehensive approach to preventing and combating trafficking in persons, including the protection and support of victims.

ICAT has undertaken initiatives to combat cyber-enabled human trafficking, recognizing the challenges posed by the digital era. These initiatives include:

- *Policy Advocacy and Statements*:

  ICAT issued a joint statement on the World Day against Trafficking in Persons, held on 30 July 2022. In this statement, ICAT called upon states to harness the opportunities presented by technology to counter trafficking in persons. By advocating for the strategic use of technology, ICAT aims to enhance efforts to combat human trafficking globally.[279]

---

276 https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-issues-global-warning-on-human-trafficking-fueled-fraud

277 https://www.interpol.int/en/News-and-Events/News/2023/Operation-Narsil-disrupts-network-of-child-abuse-websites-designed-to-generate-profits-from-advertising

278 https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Multi-Stakeholders/INTERPOL_Contribution_to_the_AHC_Concluding_Session.pdf

279 https://icat.un.org/sites/g/files/tmzbdl461/files/publications/icat_statement_wdat_2022.pdf

- *Reports and publications*:

  ICAT published its annual report for the year 2022, detailing the collaborative efforts of ICAT entities to coordinate and bring greater coherence to the UN's response to trafficking in persons. The report highlights ICAT's emphasis on addressing vulnerability to trafficking by advocating for the inclusion of survivors' voices and perspectives.[280]

  Additionally, ICAT published an issue brief called "Human Trafficking And Technology: Trends, Challenges And Opportunities" which discussed the various ways in which technology is being used at every stage of HT today.[281]

G. The GLO.ACT Women's Network

The Women's Network of Gender Champions against Human Trafficking and Migrant Smuggling comprises female officials and male advocates for women's rights across various sectors such as policy making, justice, law enforcement, and civil society. Established on June 29, 2020, the Network aims to address the gender disparities within institutions combating Trafficking in Persons (TIP) and Smuggling of Migrants (SOM). By empowering women in leadership roles, the Network seeks to create more resilient and peaceful societies less susceptible to exploitation and trafficking threats.[282]

On March 9, 2023, the GLO.ACT Women's Network organized a workshop to explore the role of technology in both enabling and combating TIP. The session, conducted via Zoom was attended by 36 members (26 female/10 male) of the GLO.ACT Women's Network, aiming to enhance understanding of technology's impact on TIP. The workshop featured two sessions: 'Cyber/online enabled TIP' led by UNODC Crime Research expert Giulia Serio, and 'Technology as an opportunity' conducted by Director of Cyber, Investigations & Intelligence Jon Blake, MBCS.

GLO.ACT-Asia and the Middle East is a four-year initiative jointly implemented by the European Union (EU) and UNODC, with the International Organization for Migration (IOM) in partnership. It aims to combat trafficking and smuggling in targeted countries through strategic interventions, policy development, capability enhancement, and victim assistance. The project prioritizes Human Rights and Gender Equality across all activities.[283]

15.3 Specific Regional Initiatives

There have been initiatives specifically undertaken in certain regions to address CEHT. We present a short introduction at how CEHT is dealt with in Europe, North America, the ASEAN member states and a few other regions.

---

280 https://icat.un.org/sites/g/files/tmzbdl461/files/publications/icat_2022_co-chairs_annual_report_6.pdf

281 https://icat.un.org/sites/g/files/tmzbdl461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf

282 https://www.unodc.org/unodc/en/human-trafficking/glo-act5/index2.html

283 https://www.unodc.org/unodc/en/human-trafficking/glo-act2/Countries/glo-act-womens-network-holds-a-seminar-on-cyber-enabled-human-trafficking.html

15.3.1 EUROPE

A. European Union Agency for Law Enforcement Cooperation (Europol)

Europol is the European Union's law enforcement agency, dedicated to assisting EU Member States in combating transnational crime and terrorism. Established in 1998, Europol facilitates cooperation among law enforcement authorities across Europe, providing operational support, expertise, and intelligence analysis to address various criminal threats, including human trafficking.

The initiatives relating to CEHT include:

- *Coordinated Operational Action*

  Europol, in collaboration with the Netherlands, coordinated a three-day operational action targeting online criminal activities facilitating human trafficking. Known as the 2023 Hackathon, this event brought together 85 experts, including law enforcement officers from 26 countries, representatives from international organizations such as the European Labor Authority, CEPOL, INTERPOL, and the OSCE.

  The Hackathon focused on addressing intelligence gaps in the recruitment of victims for the most frequently reported forms of human trafficking, including sexual and labor exploitation. This operational activity organized within the framework of EMPACT, was Europol's flagship initiative to combat organized crime.[284]

- *Collaboration with the CBI, India*

  In March 2024, EUROPOL and the Central Bureau of Investigation (CBI), India signed a working arrangement in order to support the Member States of the European Union and the Republic of India to prevent and combat serious crime and terrorism. The cooperation extends to exchange of knowledge, training, advice, and support in investigations. It has 30 different crime categories that include cyber-crime and human trafficking.

B. Council of Europe (CoE)

The Council of Europe is a European Human Rights organization comprising 46 member states, dedicated to upholding human rights, democracy, and the rule of law across Europe. Over the years, it has brought its members to commit to various initiatives key amongst them for the purposes of this report are the Lanzorate Convention on protecting children from sexual exploitation and abuse, Council of Europe Convention on action against human trafficking, Convention on cyber-crime. The CoE works in partnership with other international organizations, notably the Organization for Security and Co-operation in Europe (OSCE), to address this global challenge. The CoE also allows non-members to be signatories to its conventions. In line with that practice, the Lanzorate Convention is signed by Tunisia, the Convention on action against human trafficking is signed by Belarus and Israel, and the convention on cyber-crime is signed by the United States, Australia, and Japan.

---

284 https://www.europol.europa.eu/media-press/newsroom/news/targeted-human-traffickers-luring-victims-online#:~:text=Human%20traffickers%20use%20different%20methods,approaches%20to%20recruit%20their%20victims.

CoE was one of the first organizations to draw attention to the role of technology in human trafficking. To that end, it has undertaken various initiatives to combat cyber-enabled human trafficking, recognizing the challenges posed by the digital era. These initiatives include:

- *Council of Europe Group of Experts on Action against Trafficking (GRETA)*:

  GRETA supervises states' implementation of obligations contained in the Council of Europe Convention on Action against Trafficking in Human Beings. It conducts visits, draws up country reports evaluating legislative measures, and publishes general reports on its activities. GRETA plays a crucial role in monitoring and evaluating the effectiveness of measures taken by member states to combat human trafficking.[285]

- *Research and Study Initiatives*:

  The CoE conducted a comprehensive study called "Online and technology-facilitated trafficking in human beings, Summary and Recommendations" exploring operational and legal challenges faced by state parties and NGOs in detecting, investigating, and prosecuting online and technology-facilitated Trafficking in Human Beings (THB). Published in March 2022 by the Group of Experts on Action against Trafficking in Human Beings (GRETA), the study provides valuable insights into strategies, tools, and good practices adopted by state parties and NGOs to overcome these challenges and enhance their response to online THB.[286]

C. The Organization for Security and Co-operation in Europe (OSCE)

The Organization for Security and Co-operation in Europe (OSCE) is the world's largest regional security-oriented intergovernmental organization consisting of member states from Europe, North America, and Asia. Its mandate encompasses a wide range of issues, including arms control, terrorism, good governance, energy security, human trafficking, promotion of human rights, freedom of the press, and ensuring free and fair elections. As per its website, the organization helps to bridge differences, build trust, and foster cooperation within and between states.

In 2003, it set up the office of Special Representative and Co-ordinator for Combating THB to help the member states to devise action plans, policies, implement them for effectively addressing THB. Amongst various interventions, how technology can combat THB is being explored.

On human trafficking and more specifically, CEHT, some of the initiatives taken by OSCE are:

- *Research and Publication Initiatives*:

  i. The OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings (THB), in collaboration with Tech against Trafficking (TAT), published a study titled "Leveraging Innovation to Fight Trafficking in Human

285 https://www.coe.int/en/web/anti-human-trafficking/greta

286 https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c#:~:text=The%20CoE's%20Cybercrime%20(Budapest)%20Convention,Section%202%20of%20the%20Convention)

Beings: A Comprehensive Analysis of Technology Tools."[287] This publication describes initiatives developed to combat trafficking in persons and examines the ways technology is used or misused to facilitate human trafficking. It provides valuable insights into how stakeholders, including law enforcement, civil society, businesses, and academia, can harness technology to combat human trafficking effectively.

ii. In November 2023, a report titled "Mapping the online landscape of risks of trafficking in human beings on sexual services websites across the OSCE region" was published. This report identifies leading online sites and platforms selling sexual services where victims of CSE are advertised. It aims at providing help to identify victims of CSE on these sites. It is an exhaustive research report based on an exercise of mapping and analyzing nearly 3000 sex services website in the OSCE region.

iii. In June 2023, the OSCE published a report "Modernizing National Action Plans" which has analyzed existing National Action Plans (NAPs) to combat trafficking in the OSCE region especially looking at their structure, thematic priorities against persistent challenges and emerging trafficking trends. There is a special reference in the report about how NAPs addresses the issue of CEHT.

iv. In June 2022, the OSCE published a study titled "Policy responses to technology-facilitated trafficking in human beings: Analysis of current approaches and considerations for moving forward." This document is especially relevant to the present research as it examines states' and private sector's response to CEHT, and makes recommendations for policy and legislative responses by the OSCE states.

- *Training Initiatives:*

i. The OSCE Secretariat's Extra-Budgetary Support Programme for Ukraine organized a three-day training course in Lviv from 29 to 31 May 2023. The course aimed to improve the knowledge and skills of 30 law enforcement officers from the National Police of Ukraine (NPU) in countering cyber-crime. By providing specialized training, the OSCE contributes to enhancing the capacity of law enforcement agencies to combat cyber-enabled crimes, including those related to human trafficking.[288]

ii. The OSCE organized a hackathon in Albania which was an onsite learning initiative for detecting online human trafficking and child sexual exploitation. The participants included law enforcement officers, social workers, National Authority on Electronic Certification and Cyber-Security and CSOs. The objective was to increase awareness on CEHT especially of children.

15.3.2 NORTH AMERICA

A. United States of America

The United States has been leading the movement against trafficking globally. It has always

287 https://www.osce.org/cthb/455206

288 https://www.osce.org/support-programme-for-ukraine/545248

demonstrated a strong commitment to combating trafficking in persons, both domestically and internationally. The United States has also taken the initiative to implement several bills and acts to combat human trafficking and its detrimental, persisting effects. These provide a strong legislative foundation to combat CEHT

In 2000, in accordance with the Trafficking Victims Protection Act, the office to Monitor and Combat Trafficking in Persons was established, a TIP office. This office is responsible for bi-lateral and multi-lateral interventions, aid and public engagement in TIP. The office is organized in four sections: Reports and Political affairs, International Programs, Public engagement and intergovernmental affairs, and Resource management and planning.

Another legal development that has had far reaching consequences is the FOSTA-SESTA Act that was passed in April of the year 2018. The acronyms FOSTA stands for "The Fight Online Sex Trafficking Act", and SESTA, the "Stop Enabling Sex Traffickers Act". These two laws collectively aim to end illegal sex trafficking on the Internet. Another unique aspect of this framework is that web servers, providers, and publishers may face accountability and potential criminal penalties if they are discovered to have enabled illegal sex trafficking on their platforms. Consequently, web providers can face civil lawsuits and legal prosecution at both state and federal levels if they are believed to bear some responsibility, whether partial or full, for user-generated content and activities on their sites.[289]

Initiatives by the TIP Office in Combating Human Trafficking:[290]

- *Trafficking in Persons (TIP) Report:*

  As part of the activities of Reports and Political Affairs, an annual TIP Report is prepared. The report is a collection of materials through the embassies who in turn gather them by undertaking a desk review. The report analyses the material under the lens of the Palermo Protocol and encourages national governments to stand by their commitments made in the convention and the protocol. Reiterating the commitment of the US government to address trafficking, this report also comes with a ranking system that is linked to diplomatic sanctions. The 2023 report has extensively reported on CEHT more particularly on "online recruitment of vulnerable populations for forced labor and human trafficking and cyber scam operations.

- *International Programs*:

  TIP Office also provides funding to various international programs globally. According to the information available on its website, since 2001, the office has provided more than USD 265 million for over 945 initiatives across the world. These initiatives aim to increase awareness, build capacity, and protect vulnerable workers from exploitation. By addressing labor rights abuses and promoting ethical business practices, these programs contribute to the prevention of human trafficking in the context of global supply chains.

289 Dukes, Bridget, "The Cyberworld and Human Trafficking: A Double-Edged Sword" (2020). Cybersecurity Undergraduate Research. 3. https://digitalcommons.odu.edu/covacci-undergraduateresearch/2020fall/projects/3

290 https://www.state.gov/international-programs-office-to-monitor-and-combat-trafficking-in-persons/

- *Victim-Centred Services and Identification Training*:

  TIP Office programs support the capacity building of actors to identify victims and individuals at risk of trafficking. Additionally, they provide training to officials and other stakeholders on the provision of comprehensive, trauma-informed services to trafficking survivors. By prioritizing victim-centered approaches, these programs aim to ensure that survivors receive the support and assistance they need to recover and reintegrate into society.

- *Regional collaboration and dialogue*:

  The US government has been supporting various initiatives globally encouraging states to develop NPA to address CEHT.

  In addition to the above, the Mekong-U.S. Partnership is a collaborative effort aimed at addressing key policy and sustainability challenges in the Lower Mekong region. It facilitates dialogue and cooperation among stakeholders to tackle issues such as trafficking and cyber-enabled crime. The Partnership organized a series of seven conferences, known as Policy Dialogues, between the years of 2021 and 2023. These dialogues explore solutions to key policy and sustainability challenges in the Lower Mekong region. The sixth Policy Dialogue, held in Bangkok, Thailand from May 8-9, 2023, focused on addressing the challenges posed by non-traditional security issues such as trafficking and cyber-enabled crime. Specifically, the dialogue aimed to counter cyber-enabled crimes, and Trafficking In Persons, wildlife, narcotics, and other illicit goods in the Lower Mekong sub-region.[291]

- *Operation Innocent Images*:

  Every year, the United States Congress provides funding to the FBI for Operation Innocent Images, with recent allocations averaging around $10 million. The operation conducted undercover is organized to disrupt online groups and entities that target children for sexual exploitation and child pornography. Agents pose as children, and interact with suspected pedophiles online. Operation Innocent Images collaborates closely with the National Center for Missing and Exploited Children, which is dedicated to preventing the abduction, abuse, and exploitation of children globally.

- *Endangered Child Alert Program*:

  In 2005, the FBI launched the Endangered Child Alert Program (ECAP) with the aim of disrupting the online production of child pornography. This initiative involves releasing images of unidentified individuals, referred to as John/Jane Does, who appear in CSAM. These photos are posted on the FBI website, encouraging the public to identify and report them to law enforcement. Many of these images exhibit distinctive traits and attributes that facilitate easy identification of the individuals depicted. The Endangered Child Alert Program works directly with the National Centre for Missing and Exploited Children, as well.

291 https://www.stimson.org/2023/mekong-us-partnership-track-1-5-policy-dialogue-on-trafficking-and-cyber-enabled-crime-summary-report/

- *Operation Peer Pressure*:

  In 2003, the FBI launched Operation Peer Pressure to target individuals who utilize peer-to-peer (P2P) networks for sharing child pornography files. These networks enable the gathering and dissemination of such illicit material over the internet. Undercover agents engage in downloading images of child exploitation from the computers of offenders as a measure to halt the victimization of innocent children.

B. CANADA

i. Governments of Canada, France, and Quebec came together in 1994 to form the International Centre for Prevention of Crime. The Centre has included many members including non-governmental members from across the world. The Centre has a mission to promote safer and healthier societies. Their intervention and collaboration with the UNODC to address trafficking and more specifically to address CEHT is of relevance to this report. In 2021, the Centre along with UNODC organized a first virtual innovation competition to find technology based solutions to combat human trafficking.

ii. National Strategy to Combat Human Trafficking: The Canadian government has developed a five-year strategy to combat human trafficking in Canada. The strategy is seeking to address human trafficking in Canada, but it acknowledges that technology has seeped into the modus operandi of traffickers and speaks of collaborating with various stakeholders to combating it.

15.3.3 Association of Southeast Asian Nations (ASEAN)

The Association of Southeast Asian Nations (ASEAN) is a regional organization comprising ten member states in Southeast Asia. Established on August 8, 1967, ASEAN aims to foster economic growth, social progress, and cultural development among its member nations. The ASEAN member states include Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. ASEAN operates on the principles of mutual respect, non-interference in internal affairs, and peaceful resolution of disputes.

- *Declaration to Combat Trafficking in Persons Caused by Technology Abuse*:

  In a significant development, at the 42nd ASEAN Summit in Labuan Bajo, Indonesia, they released the ASEAN Leaders' Declaration on Combating Trafficking in Persons caused by the Abuse of Technology. This declaration represents a crucial step in addressing the growing concern of human trafficking facilitated by the misuse of technology. The ASEAN Leaders' Declaration outlines a comprehensive strategy to combat trafficking in persons caused by technology abuse.[292]

292 https://asean.org/wp-content/uploads/2023/05/06-ASEAN-Leaders-Declaration-on-Combating-TIP-Caused-by-the-Abuse-of-Technology_adopted.pdf

15.3.4 Others:

A. Tech Against Trafficking

Tech Against Trafficking is a coalition of technology companies, civil society organizations and international institutions collaborating with global experts to help eradicate human trafficking using technology. They formed this coalition in June 2018 with the primary objective to enhance technological interventions in addressing trafficking.

B. The Bali Process

The Bali process on People Smuggling, Trafficking In Persons, and related Transnational Crime is an initiative in the Asia-Pacific region which supports collaboration, dialogue and policy development relating to irregular migration. Established in 2002, this was co-chaired by the governments of Indonesia and Australia. This initiative has created valuable resources to address CEHT. In 2023, through its Regional Support Office (RSO), they brought out a policy brief on South East Asia's online Scam Centres titled "Trapped in Deceit". The report is part of its efforts to provide detailed data, analysis and policy recommendations to the members to combat trafficking and related transnational crime.

C. ASEAN-Australia Counter Trafficking

The Australian government has also made significant interventions in combating trafficking within Australia and in the ASEAN region. Within Australia, there is a NAP to combat modern slavery. In addition to that, Australia also has an international strategy to combat human trafficking and slavery. In March 2018, Australian Aid committed AUD 80 million to the collaboration with ASEAN to end Trafficking In Persons in the region. This led to the birth of ASEAN-ACT.

This initiative has consistently worked on addressing trafficking and brings out annual reports and also looks at the implementation of the ASEAN Convention Against Trafficking in Persons, especially women and children. The initiative acknowledges the use of technology by traffickers, and is involved in developing technological interventions to deal with human trafficking.

D. Virtual Global Taskforce 55 (VGT)

The Virtual Global Taskforce 55 (VGT) is an international coalition of law enforcement agencies formed in 2003 to combat online child abuse. Its members include the Australian High Tech Crime Centre, the UK's Child Exploitation and Online Protection Centre (CEOP), the Royal Canadian Mounted Police, US Immigration and Customs Enforcement, Italian law enforcement, New Zealand Police, the Ministry of Interior of the United Arab Emirates, Europol, and Interpol. VGT may extend its scope to combat trafficking in persons beyond child exploitation. Within Europol, the Analytical Work File (AWF) established in 2001 was to assist member states in combating criminal networks involved in the production, sale, or distribution of children for labor or pornography, yielding significant success. In Poland, the NGO 'La Strada' operates a website offering guidance for individuals seeking employment abroad and monitoring suspect job offers on online forums.

Similarly, in the UK, the NGO "Safe Modelling" provides detailed advice on avoiding fraudulent agencies through its website.[293]

15.4 Insights and findings

In conclusion, our exploration of the international initiatives and efforts to combat CEHT reinforces global acknowledgement of the problem and the efforts being made to address the same. Through the lens of various initiatives and institutions, we have witnessed the diverse approaches and strategies employed to address the multifaceted challenges posed by CEHT. At the heart of these international efforts lies a shared commitment to safeguard human rights, protect vulnerable individuals, and hold perpetrators of trafficking accountable. From the United Nations General Assembly to regional organizations such as the Council of Europe and ASEAN, stakeholders across the globe are working together to strengthen legal frameworks, enhance law enforcement capacities, and promote cross-border cooperation in combating CEHT and yet globally cyber enabled human trafficking is persistently on increase.

Some major gaps observed in international initiatives include:

1. Absence of uniform acknowledgement of the problem and the lack of a universal definition of cyber enabled human trafficking.
2. Most global approaches have been fragmented, limited to geographical boundaries, and not cohesive to address CEHT as a global concern as the scope of the problem is borderless.
3. There is little or no effort by global bodies to bring an international legislation that is binding for all countries ensuring multi-convergent response against CEHT, comprehensive victim protection, and mutual support and cooperation for prevention, protection, and prosecution in CEHT cases.
4. The global initiatives taken are barely keeping up with the rapid advent of the traffickers. Every innovation in technology is opening new doors to the traffickers, and throwing new challenges to anti-trafficking initiatives.
5. Little or no effort is made by trade based global bodies to bring technological firms under the accountability framework. Technology innovators, especially the large corporations, prioritize commercial gains over protection of people. Despite being aware of the rapid growth of the crime, these companies do not scale up protective measures against misuse. Accountability of the technology companies unfortunately is abysmally low in most jurisdictions and in many cases instead of partnering with the anti-trafficking initiatives, they become its first adversary. Even manufacturers of devices enabling usage of technology do not feature enough safeguards to prevent misuse and abuse.
6. Multi-lateral initiatives are yet to co-opt national governments to bring in national legislations to address CEHT.

293 https://www.cyberpeacecorps.in/cyber-enabled-human-trafficking-an-overview/#:~:text=It%20comprises%20the%20Australian%20High,Zealand%20Police%2C%20the%20Ministry%20of

7. Lack of collective global will is indicated by the absence of comprehensive global convention that makes it binding for member countries to put in place regional efforts and forge bi-lateral and multi-lateral agreement to address the problem.

Addressing CEHT, like addressing other organized crimes needs a concerted, cohesive global plan. At the time of writing this report, there is no global plan to address it. Law enforcement agencies lack the state-of-art technology that the traffickers access easily. It is very critical that these aspects should be addressed and a coordinated, protective mechanism needs to be developed keeping in mind the interests of the victim and thereby ceasing the trafficking process.

Chapter

16

Major Findings and Conclusion

Chapter 16

Major Findings and Conclusion

This chapter collates the major findings emerging from the consultation with global experts, data collection with the police officers, validation investigations, and the secondary research undertaken. While the lessons drawn from each of the stakeholders, validation investigations and various forms of CEHT studied in depth have been stated in their respective chapters, this chapter provides the broader findings taking all aspects into consideration. The conclusions drawn from the findings will act as a compass for the National Plan of Action (NPoA) meant to effectively address the emerging problem of CEHT in India.

Major Findings

1. In comparison to India, globally there is a wider recognition that cyber technology has accelerated human trafficking for various purposes of exploitation, and many countries have started to take proactive legal and policy measures to combat the same. The research brings to light that traditional forms of human trafficking continue unabated, and cyber technology has only accelerated the existing crime with a few newer forms added that target potentially anybody who has access to cyber technology.

2. It is widely acknowledged across the globe, including in India, of the concerning trend of CSAM generated and disseminated using cyber technology, raising concerns about increased child trafficking. Enforcement agencies agree that in order to address the reality of an increasing number of children being sexually abused and the fact that children are being used to create such content, newer strategies are essential.

3. Contrary to the popular perception that the dark web is a haven for nefarious criminal activities, including organized crimes, the study has shown that all means of human trafficking—such as recruitment, transfer, or harboring—are facilitated on the surface web through social media, job sites, matrimonial sites, dating sites, and similar platforms. Additionally, encrypted messaging apps have facilitated the sale of CSAM, organs, and infant babies.

4. Cyber technology has accelerated traditional purposes of human trafficking like commercial sexual exploitation, labor exploitation, organ trade, and illegal adoption. It has also triggered newer forms of exploitation by taking advantage of the geopolitical crisis of war and unrest, and increased online penetration into everyday life to lure and exploit young men to armed

conflict zones and fraudulently trap young computer-skilled individuals into committing online criminality, respectively.

5. The law enforcement mechanism in India is not familiar with the term CEHT as it is not recognized in any legal statute but has dealt with cases of human trafficking where cyber technology helped identify a potential victim or to groom, lure, intimidate and coerce a person in exploitative situations.

6. Disturbing linkages are emerging between CEHT and cyber-crimes such as fake loan apps, pig butchering, honey trapping, sextortion, and package fraud, which have the potential to become CEHT cases. While the location of perpetrators can vary, in most cases they are seen to be located within the country but not necessarily in the state to which the victim belongs or where the crime is being committed

7. The emerging CEHT cases are challenging existing narratives that presuppose poverty and economic vulnerability as the main precursors for trafficking, with cyber technology acting as an equalizer, making anybody using cyber technology in their day-to-day life a potential victim.

8. Cyber technology is expanding the reach of criminals, enabling the scanning of vulnerable populations across multiple geographical locations simultaneously, with social media platforms and instant messaging apps emerging as primary means of communication. Encryption tools like VPNs and TOR are the technologies used for communication by the traffickers. Digital payment apps like Paytm, Google Pay, and PhonePe provide a convenient mode of exchanging money. Criminals extensively use Mule bank accounts to receive illegally obtained funds. They often deceive or pay a small fee to the account holder.

9. The lack of a definition for CEHT has resulted in fragmented and inadequate legal responses, failing to address the gravity and extent of the crime. The statutory support system offers victims temporary shelter and support for prosecution, and, in some cases, rehabilitation is almost non-existent for newer forms of CEHT i.e. cyber scamming and armed conflict.

10. Law enforcement officers lack the required skills, expertise, resources, and infrastructure to collect Open-Source Intelligence (OSINT) as a means of early crime detection and intervention. While newer reporting mechanisms like cyber tip-lines have expanded the scope of reporting/detection of cases, police officers are still largely dependent on the traditional reporting methods, such as complaints by victims or their families and tip-offs from anonymous sources or concerned citizens.

11. Most AHTUs across the country are not designated police stations and lack the authority to investigate crimes. Their role is limited to crime detection and victim rescue, after which the case is transferred to the local police station. These stations are often not equipped to handle such cases, which require specialized investigation skills and are further impeded by administrative challenges. Cyber-Crime Police Stations, on the other hand, focus exclusively on cyber-crimes and do not address human trafficking cases. As a result, CEHT cases are never effectively investigated.

12. India not only has very few digital forensics labs and skilled personnel to man these labs, but there is also a critical gap in the uniform understanding of the preservation of digital evidence, impacting the effective investigation and prosecution of cases.

13. Technology firms have demonstrated a lack of transparency in their operations under the garb of privacy and freedom of speech/expression that has been effectively utilized and leveraged for criminal intentions. While communication platforms such as WhatsApp, Telegram, and Facebook Messenger serve as primary channels for recruitment, transportation, and coordination for harbouring victims, social media platforms such as Facebook, Instagram, TikTok, Dating Sites, and Online Gaming Applications serve as virtual hunting grounds for traffickers. AI poses additional challenges, particularly in generating CSAM that are hyper realistic and indistinguishable.

14. Globally, several technology firms are starting to recognize CEHT as a threat and have begun investing resources to develop technological solutions to counter the same. However, such initiatives are not part of their core business plan and are under the cover of the Corporate Social Responsibility (CSR) initiative, indicating business interests have precedence over human welfare. Furthermore, they continue to function with impunity as they are not held liable or accountable under the existing legal and policy framework.

15. Globally and in India, responses do not reflect the gravity of the situation and there has been little to no effort to establish an international statute that would be binding for all countries. Such a statute should ensure coordinated responses, comprehensive victim protection, and mutual support and cooperation for the prevention, protection, and prosecution in CEHT cases. Accountability among technology companies is unfortunately abysmally low in most jurisdictions, and it is observed that instead of partnering with anti-trafficking initiatives, they become their first adversaries.

16. There is a global consensus on the need for a partnership model in fighting CEHT with CSOs that will play a significant role in enhancing innovation and cooperation in combating CEHT.

Conclusion

The face of CEHT is changing by the minute and any research at its best can be only indicative of the current patterns and provide some understanding of the course of action that can be taken to address the problem. This action research has touched the tip of the gamut of possible reasons that provides a favourable ecosystem for traffickers to commit such crimes using cyber technology, and the victims to fall prey. Newer challenges are posed by AI, and its newest technology Generative AI, which can create realistic images and videos based on the vast amount of data available. However, governments across the globe are trying their best to curb cyber-enabled trafficking, yet the laws and processes applicable to curbing CEHT, seem to fall short at every step.

There is a critical need to increase digital awareness about financial fraud, job scams, match-making sites, and social media platforms for not just the vulnerable, but for anyone who lacks the idea of the misuse of digital technologies. There is also an urgent need for an ‘‘awareness push” at all levels from schools to colleges, to the job and matrimonial market, where even educated people with no economic and social vulnerabilities can fall prey to online traffickers. The situations can likely lead to much higher numbers that are underreported due to societal pressures.

The research has led to a deeper understanding of the problem and has revealed glaring gaps that need to be addressed to combat it. Some conclusions elicited from the research are:

1. There is an urgent need to conceptualize CEHT within an effective legal framework. This conceptualization should be comprehensive and encompass cross-border legal entities.
2. The newer forms of CEHT have highlighted the heightened vulnerability of men and boys, requiring the legal framework and sensitization of the criminal justice system towards including this population set as a vulnerable party.
3. The widespread ease of production and dissemination of CSAM on the surface web is a matter of grave concern. All stakeholders working on child safety must take urgent action and focus attention on this matter.
4. Digital use of technology has impacted all socioeconomic strata of society, and there is a need for screening and monitoring mechanisms to be in place, in addition to widespread awareness.
5. CEHT is generating revenue at all levels without leaving a trace. This can easily be tracked and traced by the monetary platforms and banking institutes. Yet, there is neither any willingness to monitor nor leverage tools such as AI, that are at one's disposal, to track and trace anomalies, or the movement of funds within and across borders.
6. There seems a singular lack of interest or motivation to provide support and rehabilitation for CEHT victims. Governments have not shown enough interest, nor have the legal enactments provided for the same, requiring the formulation and adoption of a protection framework for victims of CEHT.
7. Geographical boundaries are no longer a hindrance to online exploitation. This makes law enforcement investigations a major challenge. Although a shared commitment to safeguarding human rights, protecting vulnerable individuals, and holding perpetrators of trafficking accountable is being made by governments and key stakeholders across the globe, a concerted, cohesive global action plan is nevertheless lacking.

In conclusion, an adequately budgeted comprehensive NPoA that will act as a blueprint for the nation to address the organized crime of CEHT is the need of the hour. This will pave the way for concerted action by all stakeholders on a war footing and set in motion a series of interventions that will not only prevent this crime but also protect the victims and effectively prosecute the perpetrators.

Chapter

17

Recommendations

Chapter 17

Recommendations

Introduction

The extensive action research covering 15 states has given a clear understanding on the scope and extent of CEHT in India. Even though the problem is not legally acknowledged, its extent and diverse forms are clearly understood by all the frontline officers in the criminal justice system.

The understanding gained from the research, which also includes inputs received from global experts, has given deeper insights into the possible actions that can be taken to address this problem. In this chapter we will summarize the broad recommendations that have emerged from this detailed research. These recommendations will also form the core of the national plan of action that will be drafted as an outcome of this research.

The recommendations are broadly classified under:

a) Prevention

b) Crime Detection

c) Investigation

d) Prosecution

e) Victim Protection

f) Legal Reforms

g) Capacity Building

I. PREVENTION

For a victim of any heinous crime, the period that follows is filled with trauma and pain, with the process of recovery and healing being uncertain and taking its own course. In times when the rate of crime is fast increasing, a crime like CEHT has impacted a large number of people, with consequences that have far-reaching implications for our society. While all possible efforts must be made to prevent all forms of crime, preventing a crime as heinous and insidious as CEHT needs a specialized approach. Armed with an understanding of various vulnerable segments in the society, the following recommendations are made:

i. **Building an armour for students through education** – Develop age-appropriate content that should be integrated into the curriculum for students from primary to university level on online safety and the dangers of CEHT. This content should be reviewed and updated every year to ensure it remains current and relevant.

ii. **Building capacities of the grassroot communities** - Involve frontline workers in the community such as village volunteers, ASHA workers, Anganwadi workers, and the village panchayats to build community vigilance and preparedness to identify and deal with cyber-crimes and the modus operandi adopted in CEHT.

iii. **Information, education, and communication through preventive tools** - Develop and disseminate public service announcements through all available audio-visual means in regional languages on various ways in which cyber technology could be used for crimes, with special focus on cyber frauds and CEHT.

iv. **Integrating online safeguarding protocols** - Create technological solutions that can be integrated into all online platforms, ensuring a shield for any user. This will include among others:

- Mobile applications and online tools that will provide real-time assistance and resources for reporting suspicious online activities, fake websites, and accessing support services.
- Mechanisms to unmask and blacklist fraudulent websites and spreading awareness among job seekers to undertake necessary due diligence before accepting job offers.
- Measures such as age verification tools, content moderation algorithms, and reporting mechanisms to prevent online trafficking.
- Parental control software and monitoring tools that allow parents to supervise their minor children's online activities and protect them from potential risks.
- Safety control tools in all establishments which provide public access to cyber technologies such as cyber cafes, schools, and institutions having computer labs etc.

v. **Protecting financial institutions** - Recognizing that financial institutions are increasingly being manipulated and used to facilitate cyber-crimes and CEHT, it is imperative to develop mechanisms that will prevent this misuse by:

- Developing updated tools that can quickly intercept suspicious transactions.
- Imposing appropriate cooling-off period that will provide LEAs with reasonable response time to recover defrauded money.
- Putting in place strict regulatory provisions to prevent bank accounts with fake credentials.
- Evolving robust regulatory mechanisms including prohibiting anonymous usage of Know Your Customer (KYC) procedures to address issues like "mule SIM cards" and "mule bank accounts."

II. CRIME DETECTION

Early detection of any crime has the potential to minimize damage to both the victim and the state machinery. All efforts must be taken to build mechanisms that will enable all stakeholders including citizens and technology firms to immediately report to law enforcement any suspicious activity detected on any online platform. The enabling feature should ensure minimum repercussion and a safe ecosystem for those reporting such suspicious activities, thus incentivizing and encouraging institutions and individuals to actively report infractions to law enforcement agencies. The recommendations for early crime detection include:

i. Making it mandatory for all technology firms to report real-time any crime detected relating to CEHT and child sex abuse material to an Indian law enforcement nodal agency.

ii. All online platforms should have in-built mechanism for any user to report any suspicious activity with an option for anonymous reporting.

iii. Creation of a centralized repository of CEHT investigative resources to generate knowledge on emerging trends modus operandi adopted by offenders. Up-to-date information on the rapidly changing patterns of technology use and the technological landscape, which can be accessed by all stakeholders in the criminal justice system.

iv. Implement real-time data analytics tools to monitor and analyze internet traffic for potential CEHT indicators.

v. Develop AI-powered detection systems using information from OSINT resources, to identify and flag suspicious online activities related to human trafficking.

vi. Develop technology tools for predictive policing to check CEHT.

vii. Evolve protocols and guidelines for information sharing on suspected CEHT cases and criminal networks with international agencies for early intervention.

III. INVESTIGATION

Deterrence in any crime can be achieved only by effective time-bound investigation that is able to trace, track, and apprehend the entire chain of criminals and the network responsible for committing the offence. While law and order are state subjects, the crime of CEHT is borderless and requires mechanisms that will facilitate intra-state, inter-state, and international protocols that will enable law enforcers to investigate these crimes effectively. The recommendations in this section look at standard operating procedures for effective mutual cooperation at the local, national, and international levels and mandatory guidelines for technology firms to assist in investigation and protocols for digital evidence management.

i. Evolve intra-state and inter-state protocols through mutual regional cooperation, which are passed as executive orders for time-sensitive investigation and collection of evidence in CEHT cases.

ii. Build international cooperation mechanisms to enhance coordination and facilitate

joint investigations into transnational criminal networks, entailing multi-stakeholder collaboration.

iii. Develop tools for investigation that use blockchain technology to secure and manage digital evidence related to CEHT cases, ensuring its integrity and traceability.

iv. Ensure robust forensic evidence management with adequate cyber forensic labs with advanced forensics resources, infrastructure, and specialized manpower in all states, which is proportionate to the volume of cases and demographic requirements.

v. Develop comprehensive SOPs on seizure/ collection, custody/ handling, analyzing and preserving of digital evidence, including following certification processes to present evidence in courts.

IV. PROSECUTION

The existing rate of conviction in cyber-crimes is a cause for great concern. In CEHT cases, various technological features such as ability to create fake profiles, encryption that allows private untraceable communication, disappearing features etc. provide the traffickers enabling environment to conceal their identity and mislead the investigation. Long delays in court procedures, lack of preparedness of prosecuting and judicial officers to appreciate digital evidence further aggravates the matter, giving the offenders a loophole to escape the long arms of the law. Effective prosecution in such crimes also requires infrastructural capacities for the criminal justice system to effectively function. The recommendations in this section look into all such aspects:

i. Setting up special courts to deal with CEHT cases, which are equipped with facilities and advanced technology for presenting digital evidence.

ii. Building courtroom infrastructure that is witness-friendly and provides for witness privacy and protection.

iii. Evolve comprehensive prosecutorial guidelines for CEHT cases to ensure consistent and effective legal strategies across jurisdictions.

iv. Ensure special provisions in witness protection programs to safeguard individuals who testify in CEHT cases, providing safe homes and identity protection, if needed.

V. VICTIM PROTECTION

The damage to a trafficked individual's body, mind, and soul cannot be quantified. When the element of technology is added to this crime, the potential for lack of closure is high, given the context where content involving the victim is available in perpetuity, constantly re-victimizing the victim for a long time. There is a need to evolve customized victim-support programs that recognize the unique characteristic of CEHT and its impact on a victim's mind. When technology is used to commit the crime, it keeps the person in a state of physical or emotional captivity. This section looks at institutional and non-institutional interventions that is trauma-informed, which is geared towards supporting any human being who is removed from a situation of trafficked exploitation:

i. Set up 'Integrated Victim Support Centre (IVSC)' for victims of CEHT, both national and foreign, which is gender-neutral and includes hotline, trauma-informed support services such as psycho-social care, medical care, specialized counseling, legal aid, and institutional and non-institutional rehabilitation, reintegration and repatriation support.

ii. Develop special 'Victim Witness Protection Scheme' that provides for identity protection, safe homes if there is threat perception, compensation for loss of wages due to court procedures, small financial relief to start life afresh, and support for legal representation.

iii. Evolve a comprehensive 'victim compensation scheme,' which takes into consideration the psychological damage incurred due to the use of technology in committing a crime.

VI. LEGAL REFORMS

The concept of CEHT is yet to be included in the Indian legal system. This inclusion should encompass a legal definition, accountability of all stakeholders who act as enablers of the crime, and statutory rights of the victims to access support services. The following recommendations look at the legal reforms necessary to ensure a more robust legal framework to address the problem:

i. Initiate and bring appropriate legal amendments to the Bhartiya Nyaya Sanhita (BNS), the Information Technology Act (IT Act) and the Protection of Children from Sexual Offences Act (POCSO) ensuring clear definitions of CEHT, data protection, data retention, stringent penalties, and robust enforcement mechanisms.

ii. Review and strengthen the data privacy and protection laws to safeguard personal information and prevent its misuse by traffickers, aligning with international standards such as the General Data Protection Regulation (GDPR).

iii. Evolve legal sanctioned protocols and procedures on intelligence gathering, evidence gathering, witness protection, victim protection and procedures for dealing with foreign nationals.

iv. Set up legal safeguards for the ethical use of technology in detecting and prosecuting CEHT, ensuring the protection of civil liberties and privacy.

v. Evolve legally vetted data retention policies that require Internet Service Providers (ISPs) and telecom companies to retain user data for a specified period to aid in the investigation of CEHT crimes.

VII. CAPACITY BUILDING

As new crimes emerge there is a dire need to build the capacities of various stakeholders including those in the criminal justice system to address the crime effectively. The vested interests who manage criminal enterprises involving human trafficking are way ahead in using latest versions of technology to support their nefarious activities. Regretfully, those responsible to prevent, detect, and prosecute the crimes are not adequately prepared to take on these new-age criminals and their

modus operandi. Regular and consistent capacity building is the only option to bridge this gap. This section looks at recommendations to build the capacities of all stakeholders:

i. Develop comprehensive and standardized training resource materials, including SOPs and training manuals to provide capacity building training workshops for law enforcement officers, prosecutors, judicial officers, civil society organizations, legally competent bodies, labor officials, and financial institutions on detection of CEHT cases, identification of victims and perpetrators, investigation and prosecution of CEHT cases, including appreciating digital evidence and providing victim-centered assistance to survivors.

ii. Develop standardized training resource materials to provide capacity building training for frontline workers such as Anganwadi workers, ASHA workers, Village Volunteers, Panchayat Raj Institutions, airport staff, immigration officers, etc., on dangers of CEHT, indicators for identifying potential victims and perpetrators, preserve digital evidence and reporting mechanisms.

iii. Ensure regular training on the latest technologies and investigative techniques is provided to equip officers placed in units meant to deal with CEHT cases; upgrading skills necessary to investigate CEHT; using state-of-the-art tools and technologies, ethical considerations in cyber-crime investigations, procedures to request electronic evidence from private companies and obtaining evidence and cooperation from other states or countries.

iv. Ensure training curriculum in a law schools have all components to prepare next generation lawyers on the complexities of CEHT cases, including digital evidence and cyber laws.

v. Provide specialized training for certified expert witnesses in the field of cyber-crime and human trafficking to provide credible testimony in court.

We live in a world where our lives are intrinsically entwined with technology in the digital space. The concept of private space as we knew it, does not exist anymore. This is a new reality that we need to cope with. Like every new technology that humankind has been exposed to over the past century, the advancement in digital technology too has had its unintended consequences - an unanticipated explosion in cyber-crimes and cyber enabled human trafficking. While criminals using cyber technology continue to evolve newer methods of committing crimes and expand their area of operations, it is critical that each society and country prepare itself to keep its citizens safe and secure. Hopefully, when implemented, these recommendations will be a positive step in that direction.

Annexure I

List of officers who contributed to the research

Andhra Pradesh (03 January 2024)

Sl. No.	Name	Designation and Place of Posting
1.	P. Arjamma	S.I. of Police, Disha P.S., Kakinada
2.	D. Rajya Lakshmi	S.I. of Police, Disha P.S., Konaseema
3.	V. Kanthipriya	S.I. of Police, Disha W.P.S., Eluru
4.	Sk. Ameena Begum	S.I. of Police, Disha P.S.
5.	T. Aruna Kumari	S.I. of Police, Kavali G.R.P., Guntakal Railway District
6.	K. Vasavi	Inspector of Police, Disha P.S., I/C AHTU, Velaya
7.	D. Sakuntala	S.I. of Police, Disha P.S., ASR District
8.	T. Laskshmi	Inspector of Police, Disha P.S., Anakapalli
9.	P. Syamali	S.I. of Police, Disha W.P.S., Vizianagaram
10.	P. Syamala Aparna	S.I., CCPS, CIO
11.	N. Gowri	S.I. of Police, Disha W.P.S.
12.	B. Bhudevi	Women P.C. Disha W.P.S.
13.	T. Mahita	W.S.I., CID RO, Nellore
14.	P. Fathima	S.I. of Police, CID RO, Guntur
15.	D. Chandra Sekhar	Inspector of Police, CID, CCPS, HQPS
16.	Ch. Venkateshwara Rao	Inspector of Police, CID RO, RJY
17.	T. Bhadra Rao	S.I. of Police, CID RO, Vijaywada
18.	S. Subba Raju	S.I. of Police, CID RO, Tirupati
19.	M. Mohan	S.I., Cybercrimes, CID
20.	S. Naseeruddin Peer	P.C., CID RO, Kurnool
21.	B. Balakrishna	S.I., 30, Cybercell Rayachoti
22.	A. Sunny Babu	P.C. 6016, CID RO, Guntur
23.	V. Thulasiram	P.C. 4327, Disha W.P.S., Chittoor
24.	R. Sivake Savulu	P.C. 2405, Disha W.P.S., Tirupati
25.	K. Sarat Chandra	C.I. of Police, Disha P.S., Tirupati
26.	K. Balaiah	Inspector of Police, Disha P.S., Chittoor
27.	T. Ch. Govindu	Inspector of Police, Disha P.S., Anantapuram
28.	D. Mallikagida	Inspector of Police, Disha W.P.S., Ongole
29.	K.Srinu	P.C. 2353, Disha W.P.S., Ongole
30.	K. Kola Venkata Ramana	C.I., Disha W.P.S., Kurnool
31.	G. Iqbal	S.I. of Police
32.	K. Mallikarjuna Rao	P.C.
33.	B.U. Mahesh	Constable
34.	Y.Ch. Alluri Reddy	C.I. of Police

35.	B. Siva Koteswara Rao	P.C. 6111
36.	V. Subba Rao	S.I. of Police, Disha
37.	S. Satish	P.C. 1422
38.	Mottavi Krishna	P.C. 338, Disha, PVP (M)
39.	B. Mohan Babu	P.C. 3718, Disha W.P.S., Kurnool
40.	P.V. Ramana Murty	S.I., CID
41.	K. Paidapu Naidu	C.I., CID
42.	B. Supriya	C.I., CID RO, VSP
43.	M. Sudhakara Rao	H.C. 106, CID RO, USP
44.	P. Saroja	S.I. 146
45.	K. Srinivasa Rao	S.I. of Police
46.	K. Ravi Kiran	P.C.
47.	R. Murali Mohan	S.I. of Police
48.	D. Sathish Babu	A.S.I., AHTU, SPS Nellore
49.	TVS. Ramababu	P.C. 420
50.	G. Babi Rani	WASI- 699
51.	JJN. Rao	P.C. 3611
52.	M. Bala Krishna	P.C. 2136
53.	M. Ramya	S.I.
54.	K. Lalitha	Women H.C.
55.	I. Ramadevi	W.S.I.
56.	A. Kandaias	S.I., Disha P.S., Nandyal
57.	Y. Sirusha	P.C., Cyber Team
58.	M. Naga Raju	P.C., Disha P.S., Vijaywada
59.	D.N. Subrahyan	Cyber Expert, Disha P.S.,
60.	N. Mahesh	P.C. Disha P.S., AKP
61.	K. Rupakala	W.P.C., Disha W.P.S., ASR

Assam (18 January 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Nayan Jyoti Das	Inspector CID
2.	Tapan Dass	Inspector Anti Trafficking
3.	Paulus Narzary	Inspector Golapara
4.	Uttam KR Deley	Inspector CID
5.	Kaushik Malla Bujar Baruah	Inspector CID
6.	Daisy Nath	Sub-Inspector CID.
7.	Jayanta Kakoti	Panban Chimaug
8.	Ratul Haloi	Inspector PI, Dhubmi
9.	Arup Jyoti Baishya	Inspector Nalbari

10.	Sanjeeb KR Das	Inspector CID
11.	Mukut Kakati	Inspector Mamgo Doi Police Station
12.	Ajit Kumar Rai	Inspector Dibrugarh
13.	Rimjim Mahanta	Inspector CID
14.	Bichitra Hazong	Inspector CID
15.	Jayant Kakoti	Inspector CI Panbari Chimang
16.	Hemanta Halol	Inspector CID
17.	Arbil Hojai	Inspector CID
18.	Tripti Gogoi	Inspector CID
19.	Muktajur Rahman	Inspector CID
20.	Ajay Barman	Inspector CID HQ
21.	Longki terom	Inspector Biswanath DEF
22.	Deep Jyoti Mazumdar	Inspector Tamulpur DEF
23.	Arup Pathak	Inspector Kamrup DEF
24.	Ajoy KR Saha	Inspector Bongaigaon DEF
25.	Rakesh Kahita	Inspector CID
26.	Nadarul Islam	Inspector CID

Bihar (01 February 2024)

Sl. No.	Name	Designation and Place of Posting
1	Vijay Kumar Ojha	Inspector, Economic Offences Unit
2	Ajay Kumar	Inspector, AHTU CID, Bihar, Patna
3	Jawad Akhtar	Inspector EOO
4	Binod Singh	Inspector, EOO
5	Santosh Sharma	Inspector, SSp office, Patna, AHTU
6	Sanjeev Kumar	Inspector of Police, EOU, Bihar, Patna
7	Kapil Deo Prasad	Inspector, Patna
8	Vishwajit	Inspector, Cyber police station, Gaya
9	Krishna Murari	Inspector, Economic Offences Unit
10	Pratibha Kumari	Sub Inspector, CID
11	Faisal Ahmed Ansari	Inspector, Bengusarai
12	Kr. Santosh Rajak	Inspector, Muzaffarpur
13	Amrita Rani	Inspector, EOU
14	Sachindra Yadav	Inspector, Jehanabad
15	Ajay Chaudhary	Inspector SJPO
16	Ramanendra Kumar	Inspector SJPO
17	Chaturvedi Seedhra Kumar	Inspector EOU
18	Deo Narayan Paswan	Inspector, EOU
19	Nagendra Paswan	Inspector, EOU, Patna

Goa (30 January 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Pushpalata Borkar	LPI, AHTU, Margaon
2.	Nathan De Almeida	PI, SIT (LG), Cybercrime
3.	Vilas N. Patil	PSI, Cybercrime
4.	Ashok Megeri	ASI, AHTU, Panaji
5.	Datharam C. Gabkar	ASI, AHTU, Panaji
6.	Rupali Govekar	PSI, Women PS, Panaji
7.	Reema A. Naik	PSI, Women PS, Panaji
8.	Suvarna Talgu	PI, GRP (E-Coy)
9.	Manda M. Naik	PSI, GRP (E-Coy)
10.	Adam Skaikh	ASI, GRP (E-Coy)
11.	Vinayak M. Ghogali	ASI, GRP (E-Coy)
12.	Lalan A. Calangutkar	LHC-4567, (BCoy)
13.	Tulshi Das S. Malik	ASI, GRP (B-Coy)
14.	Jitendra N. Kerkar	HC-4761, (D-Coy)
15.	Dilip Harmnkar	PSI, GRP (D-Coy)
16.	Sanjay Gawbnoi	ASI, GRP (D-Coy)
17.	Manoj P. Goltekar	ASI, GRP (E-Coy)
18.	Swati Desai	LASI, Women Cell, Marga
19.	Nutan U. Verenkar	DySP FRRO, WPS & AHTU
20.	Sudiksha S. Naik	PI, AHTU, Margao
21.	Nehanda Tavares	PSI, AHTU, Margao
22.	Deepa D. Desai	PSI, AHTU
23.	Pallavi P. Gawas	LASI, GRP (E-Coy)
24.	Ashok S. Thanekar	PC-6391, GRP (A-Coy)
25.	Olga Fernandes	LHC-3805
26.	Bhikaji Salgaonkar	ASI, (C-Coy)
27.	Prakash D. Patil	ASI, (E-Coy)
28.	Yashwant P. Salgaonkar	ASI, GRP (E-Coy)
29.	Nitin D. Morje	ASI, GRP (C-Coy)
30.	Narsimrao Tikali	PC-6916, GRP (C-Coy)
31.	Amar Konadkar	PC-6098, GRP (A-Coy)
32.	Sripad Gawas	PSI, GRP
33.	Vikas Gawade	PSI, Cybercrime P.S
34.	Sanit Karlekar	PSI, Cybercrime P.S.
35.	Sagar Gawas	PC-7265, Cybercrime P.S.
36.	Santosh Naik	PC-6213, GRP (A-Coy)

Gujarat (14 February 2024)

Sl. No.	Name	Designation and Place of Posting
1.	D.S. Vaghela	Dy SP, AHTU, CID
2.	G.A. Patel	PI, AHTU, Surat City
3.	Dikshit Gamit	PI, Cyber Cell, Surat City
4.	Krupesh P. Patel	PI Cyber Cell, Rakjot City
5.	Mahendrasinh Zankat	PI Cyber Cell, Rakjot City
6.	Kalpesh S. Maniya	PI, AHTU, Jamnagar
7.	P.M. Judal	PI, AHTU, Panchmahal
8.	S.A. Dabhi	PI, AHTU, Gandhinagar
9.	R.S. Damor	PI, Cyber Cell, Gandhinagar
10.	P.U. Rana	PI, Cyber Cell, CID Crime, Gandhinagar
11.	P.P. vaghera	I/C, AHTU
12.	N.W. Rathwa	PI, AHTU, Vodadra (Rural)
13.	P.A. Valvi	PI, AHTU, Valsad
14.	A.P. Bramhbhatt	PI, I/C AHTU Kheda
15.	Dr. B.B. Patel	PI, Baroda City
16.	S.N. Karanjia	PI, Himmatnagar
17.	N.N. Pargi	PI, Ahmedabad (Rural)
18.	M.P. Pathan	PI, AHTU, CID
19.	N.J. Jangle	PSI, AHTU, CID
20.	K.D. Kerdiya	PSI, AHTU, CID

Jharkhand (08 January 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Arjun Oraon	S.I., Jharkhand Police
2.	Bilkan Bage	S.I., Jharkhand Police
3.	Dulhhrmani Tudo	S.I., Jharkhand Police
4.	Sukhendra Yadav	A.S.I., Jharkhand Police
5.	Ram Pravesh Kumar	INS, Bokaro
6.	Bimal Kindu	INS, Jamshedpur
7.	Manendra Pal Roy	S.I., Jharkhand Police
8.	Birendra Kumar Rajabanshi	Police Inspector
9.	Sukant Tripathi	Police Inspector
10.	Edual Gesten Bage	Police Inspector
11.	Rajkapur	Police Inspector
12.	Kundan Kumar Verma	S.I., Jharkhand Police
13.	Akash Kumar Panda	S.I., Jharkhand Police
14.	Subodh Kumar Yadav	Police Inspector, Cyber P.S., Jamtara

15.	Ramdeo Ravidas	S.I., Simdega
16.	Ravi Sanjay Tapo	Police Inspector, Cyber P.S., Palamu
17.	Sony Xalro	S.I., AHTU P.S., Sahibganj
18.	Gajendra Kumar Water	Inspector, Cyber-Crime P.S., CID Jharkhand, Ranchi
19.	Kumar Sumit Yadav	S.I., Jharkhand Police
20.	Salan Paulkerketta	S.I., Jharkhand Police

Kerala (05 January 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Subeeshmon K.S	SI of Police
2.	M.S Shibu	SI of Police
3.	Jobin George	IP Cyber PS
4.	Saranya S Devan	SI Cyber PS , KTM
5.	Kannan S P	SI, Hi-Tech Cell, PHQ
6.	Prakash K S	JOP,NRI Cell & Addl. Charge of Hi-Tech Cell
7.	Zacharia Mathew	Asst. Commissioner of Police, Dist. Crime Branch, Kollam City
8.	Viju Kumar N	ACP DCB
9.	Sudheesh Kumar V S	IOP Cyber PS
10.	Vinod Kumar P B	IOP Cyber PS
11.	Sajeev Kumar J S	IP Cyber, Palakkad
12.	Arun M J	IP Cyber, Malappuram
13.	K J Thomas	IP Cyber, Kochin City
14.	M B Latheef	IP Cyber-Crime, EKM RL
15.	K Vinukumar	IP Cyber PS, TVM RL
16.	A Jayakumar	SHO Cyber PS, Kollam City
17.	Sivaprakash T S	SHO Cyber-Crime PS, Kollam Rural
18.	P Narayanan	IP SHO Cyber PS, Kasaragod
19.	Premlal S L	IP Cyber PS, KKD RL
20.	Shibu	SI, Cyber Branch, Kollam Rural
21.	Sanil Kumar	Inspector, Cyber PS, Konni City
22.	Shaju Joseph	IP Cyber PS, Wayanad Dist

Madhya Pradesh (05 January 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Mrs. Nilesh Ahirwan	Inspector, Cyber Cell, Jabalpur
2.	Sapna Choure	Inspector, Cyber P.H.Q
3.	Rama Masram	Inspector, Cyber P.H.Q
4.	Anuj Samadhiya	S.I.

5.	Indra Singh	Inspector
6.	Renu Agul	T.I.
7.	Ankita Khatarkar	ACP, Bhopal
8.	Priti Tiwari	T.I., Indore
9.	Varsha Sutavri	S.I. Mahila
10.	Shilpa Kourav	Inspector, W.P.S., Bhopal
11.	Mukesh Haroliya	Inspector, State Cyber Police, Gwalior
12.	Dinesh Gupta	Inspector, State Cyber Police, Gwalior
13.	Ram Sumer Tiwari	Inspector, State Cyber, Indore
14.	Zaheer Khan	T.I., GRP Bhopal
15.	Ramayan Prasad	Inspector, SDL
16.	Shashikala Chouhan	S.I.
17.	Lakhan Lal Vikas	Inspector
18.	Shashikala Maskule	Inspector
19.	Anuradha Girwal	Inspector
20.	Dinesh Verma	Inspector
21.	R.D. Kanwa	Inspector
22.	Dr. Sarita Neeraj Thakur	Inspector (Cyber)
23.	Shashi Dhurve	Inspector, GRP, Jabalpur
24.	Girish	Inspector, Nimach

Maharashtra (15 February 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Sanjay A Pawar	S.I. Sahar PS
2.	Vishal Shravgi	SI Cyber-Crime East Mumbai
3.	Shankar Jadhav	SI Cyber-Crime Thane circle
4.	Manoj R Sutar	PI Mumbai City
5.	K.D. Aher	PI Mumbai City
6.	J.R Kamble	PI Mumbai City
7.	S.B, Khadke	PI Central Cyber-Crime Unit
8.	Surabhi S Pawar	PI AHTU
9.	Hema Chowdhry	PI AHTU
10.	Gajanan kadam	PI Cyber Cell Navi Mumbai
11.	Prithvi Raj Gharpode	PI AHTU Navi Mumbai
12.	Nilam Pawar	API, AHTU Navi Mumbai
13.	S.S. Yadav	PI Unit 7, Crime Branch Mumbai
14.	Rajashri Balaji	PI Unit 7, Crime Branch Mumbai
15.	Nitin Potdar	Spl. PI Enforcement Mumbai
16.	Nilesh Khanade	API Crime Branch Thane

Meghalaya (07 February 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Sunady Manner	Inspector
2.	Swedish R. Marak	Inspector
3.	Melissa M. Momin	Inspector
4.	Sandra Anny mary Nongohar	Dy S.P.
5.	Starday Kharjana	Inspector
6.	Vijoy Udpadhya	Inspector
7.	Kinshewmon Tham	Sub Inspector
8.	Cheryl R. Kharkongor	Sub Inspector
9.	S. Rikseng M. Sangma	Inspector
10.	Fredis K. Marak	Inspector
11.	Handakarhhi P. Lytan	Inspector
12.	Kalpana Kuhari	Sub Inspector
13.	Neena B. Rabha	Dy S.P.
14.	Jessica A. Sangma	Inspector
15.	John Marbaniang	Inspector
16.	Darisha Marbaniang	Constable
17.	Smti Namrata Chhettri	Constable
18.	Brilliansiar Nongsiet	Constable
19.	Opaia Tyngkan	Inspector
20.	Bopphy I. Sangma	WPC Constable
21.	Goalan K. Sangma	Inspector
22.	Animesh Mandal	Inspector
23.	J. Dhar	Sub Inspector

Odisha (26 December 2023)

Sl. No.	Name	Designation and Place of Posting
1.	Sambit Kumar Majhi	DSP, Koraput
2.	Haramani Baskey	Inspector, Sambalpur
3.	Hrusikesh Behera	Inspector, Keonjhar
4.	Niranjan Sethi	Inspector, Rourkela
5.	Anand Dungdung	DSP, Boudh
6.	Manash Kumar Deo	DSP, Balasore
7.	Satya Ranjan Mallick	ACP, CTC UPD
8.	Arati Kumari Parida	SI, CID CB, Cyber Complex
9.	Banita Mharana	Inspector,BBSR UPD
10.	Kiran Mohanty	Inspector, Nabarangpur

11.	Budhadev Naik	Inspector,GRP Rourkela
12.	Satish Chandra Nayak	Inspector, Ganjam
13.	Sangram Tudu	DSP,Jajpur
14.	Sarita Mahapatra	DSP, Kendrapada
15.	Prasanta Nisika	Inspector, Gajapati
16.	Saubhangiri Sethy	ASI, CID CB, BBSR
17.	Bimal Kanta Nayak	DSP, Berhampur
18.	Rashmi Rekha Mahalick	Inspector, Mayurbhanj
19.	Priya Ranjan nayak	Inspector, Cuttak

Punjab (05 February 2024)

Sl. No.	Name	Designation and Place of Posting
1.	ASI Satinder Singh	I/C Social Media Cell (Patiala)
2.	LR/ASI Harpal Singh	Cyber-Crime Cell (Patiala)
3.	S/CT Rajinder Singh	CITSU (Faridkot)
4.	ASI Surjit Singh	CITSU (Hoshiarpur)
5.	CT Gourav Kaushal	Social Media Cell (SBS Nagar)
6.	SI Geeta	I/C Social Media Cell (Ferozepur Range)
7.	INSP Rajinderpal Singh	I/C Cyber-Crime Cell (Bathinda)
8.	SI Bajeet Kaur	Cyber-Crime Cell (Fatehgarh Sahib)
9.	INSP Amanjot Kaur	I/C Cyber-Crime Cell (SAS Nagar)
10.	S/CT Jagdeep Singh	I/C Social Media Cell (Tarntaran)
11.	ASI Harjit Singh	I/C Cyber-Crime Cell (Tarntaran)
12.	ASI Jorawar Singh	Computer Cell (Amritsar City)
13.	CT Gourav	Cyber-Crime Cell (SAS Nagar)
14.	CT Harpreet Singh	Cyber Cell (Amritsar Rural)
15.	CT Rohit Verma	Social Media Cell (Khanna)
16.	CT Gurwinder Singh	Cyber-Crime Cell
17.	INSP Pushpinder Kaur	Cyber-Crime Cell (Mansa)
18.	INSP Harjit Kaur	Cyber-Crime Cell (Sangrur)
19.	SI Gurpreet Kaur	Cyber-Crime Cell (Malerkotla)
20.	SI Jyoti	Social Media Cell (Ferozepur)
21.	SI Amarjeet Kaur	I/C Social Media Cell (Fazilka)
22.	INSP Simranjeet Singh	INT HQ
23.	CT Amritpal Singh 488/PTK	Social Media Cell (Pathankot)
24.	LR/ASI Hira Singh 231/GSP	Cyber-Crime Cell Gurdaspur
25.	S/CT/ Kuldeep Singh 1368/SMS	Cyber-Crime Cell (Muktsar Sahib)
26.	ASI Pardeep Singh	Cyber-Crime Cell (Rupnagar)
27.	L/CT Manpreet Kaur	Social Media Cell (Amritsar)

28.	SI Manpreet Kaur	CCPWC
29.	SI Rupinder Kaur	CCPWC
30.	ASI Harminder Singh	Cyber-Crime Cell (Patiala)

Rajasthan (13 February 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Aditya Poonia	Dy SP, Rajasthan Police
2.	Tej Karan	CI
3.	Brij Mohan Deoraj	Inspector
4.	Nitiraj Singh	Dy SP
5.	Umaid Singh	Dy SP
6.	Puram Mal	Inspector
7.	Vinod Kumar	Inspector, Cyber PHQ
8.	Rakesh Rajora	Ad SP, Jaisalmer
9.	Hari Ram Soni	Dy SP, Junjhunu
10.	Ramesh Tiwari	Dy SP, Tonk
11.	Parul Yadav	SI, Cyber Thana, Ajmer
12.	Shimla Devi	ASI, Jaipur (Rural)
13.	Preeti Beniwal	CI, Mahila Thana, Sikar
14.	Hari Ram Meena	CI, CCPS, SOG, Jaipur

Telangana (07 November 2023)

Sl. No.	Name	Designation and Place of Posting
1.	Ch.Gangadhar	Inspector Cyber-Crime
2.	M. Adi Murthy	DSP CoE
3.	P.Sita Reddy	DSP CoE-CID
4.	K.Venkata Lakshmi	SP EoW
5.	Padma Palle	Inspector, CCPS
6.	K.Narsimha Reddy	Inspector. AHTU, Cyberabad
7.	B.Ram reddy	SP CMS
8.	J Anyonya	SP Admin
9.	K.Shravan	Insp. CCPS Cyber
10.	A.Nandeshwar	Inspector CCPS
11.	M.Shyam Prasad Rao	DSP, EoW
12.	S.Chakrapani	DSP CoE
13.	M.Shankar	DSP EoW
14.	B.Raja Ravindra	SI, CID
15.	M.Madhu Kumar	CI, Cyber-crime

16.	Lavanya NJP	SP, Cyber-Crime
17.	P.Salomon Raj	Inspector of Police RO, Cyberabad
18.	S.Ramachnadra Reddy	ACP, Cyberabad
19.	G.Sathish Kumar	Inspector, Cyberabad
20.	N.Chandra Babu	Inspector AHTU Rachakonda
21.	P.Sangameshwar	Sub - Inspector
22.	G.Venkat Reddy	Dy. Superintendent of Police
23.	B.Saroja	Inspector of Police
24.	Ch.Suresh Babu	Inspector of Police

West Bengal (24 January 2024)

Sl. No.	Name	Designation and Place of Posting
1.	Pranab Kanti Sahoo	Inspector, Diamond Harbour P.D.
2.	Progati Ranjan Biswas	Inspector (I/C Cyber -Crime), Baruipur P.D.
3.	Sudarshan Debnath	S.I. of Police (I/C AHTU), Baruipur P.D.
4.	Tirtha Sarathi Halder	Inspector of Police (I/C Cyber-Crime P.S.), Diamond Harbour P.D.
5.	Jyotirmoy Biswas	O/C Cyber-Crime P.S., CID, WB
6.	Gautam Saha	O/C AHTU, CID, WB
7.	Ajeet Kumar Jha	O/C Cyber-Crime, Barrackpore
8.	Liton Halder	Inspector of Police
9.	Anjana Bhowmick Ray	Addl O/C AHTU, CID, WB
10.	Mousumi	S.I. of Police, O/C AHTU, Barrackpore
11.	Md. Abdun Noor Chaudhury	S.I. of Police, Cyber-Crime PS, Bidhannagar P.C.

Annexure II

International Experts: Global Consultations

Sl. No.	Name	Country	Association	Date
1.	Mr. John Carr	UK	Order of British Empire, Member, Executive Board, UK Council on Child Internet Safety Secretary, UK Children's Charities' Coalition on Internet Safety	30 Nov 2023
2.	Lori L. Cohen	United States	Chief Executive Officer, Protecting at Risk Children and Youth (PACT)	05 Nov 2023
3.	Special Agent Mark Niegelsky	United States	Diplomatic Security Service	16 Nov 2023
4.	Special Agent David Paik	United States	Human Trafficking Investigations Coordinator, Diplomatic Security Service	16 Nov 2023
5.	Robert C. Bartolo	United States	Senior Advisor, DHS Centre for Countering Human Trafficking	28 Nov 2023
6.	Special Agent Albert Ordonez	United States	National Program Manager, DHS Centre for Countering Human Trafficking	28 Nov 2023
7.	Special Agent Raymond Abruzzese	United States	Program Manager, HSI Cyber-Crimes Centre, Child Exploitation Investigations Unit	28 Nov 2023
8.	Bethany Eberle	United States	Acting Director, DHS Office of Strategy, Policy and Plans/Counter Transnational Organized Crime/ Crimes of Exploitation Policy Group	28 Nov 2023
9.	Ms. Konstantina Stavrou LLM	Austria	University Assistant, Fellow of the Austrian Academy of Sciences, Department of Constitutional and Administrative Law Faculty of Law, University of Vienna	12 Dec 2023

10.	Dr. Wolfgang Spadinger	Austria	Director, Deputy National Anti-Trafficking Coordinator Federal Ministry, European and International Affairs	20 Dec 2023
11.	Brig Gerald	Austria	Law Enforcement Agency	23 Jan 2024
12.	Mr. Thapana Bhasathiti Sanyabutra	Thailand	Special Case Officer and Head of the Centre for International Cooperation, Bureau of Human Trafficking Crime Department of Special Investigation	02 Feb 2024
13.	Mr. Andrey	Philippines	Member of Regional Forced Labor Team	08 Feb 2024
14.	Mr. Gideon C	Philippines	Member of Regional Forced Labor Team, Tech Expert	08 Feb 2024
15.	Mr. Benjamin Lawrence Patrick Aritao	Philippines	Member of Regional Forced Labor Team, Tech specialist, OSEC (Online Sexual Exploitation of Children) Team	08 Feb 2024
16.	Ms. Maria Jose Costano	Spain	Jurist and Lead Researcher for Data Culture in Human Trafficking Project	29 Jan 2024

Annexure III

Consultation with CSOs

S.No	Name and Designation	Name of Organisation
1.	Ms. Surabhi Shivpuri, Director, Programmes and Projects	Shakti Vahini, New Delhi
2.	Mr. Gorakh Jadhav, Lead-ILED and Police Relations	International Justice Mission, Mumbai
3.	Ms. Bariphylla Lyttan, Case Manager /Team Lead	Impulse NGO Network, Shillong
4.	Mr. Abhishek Kashyap, Project Coordinator	Jan Jagran Sansthan, Patna
5.	Ms. Shivani Priya, Program Manager	Bal Kalyan Sangh, Ranchi

Annexure IV

Questionnaire for National Action Research on Countering Cyber Enabled Human Trafficking (CEHT)

State:
Rank:
Unit/Department:
Date:

SECTION 1: NATURE OF CASES - HUMAN TRAFFICKING

1.1. Did you encounter any cases of human trafficking in your jurisdiction where cyber technology was used in the last 2 years?

a. Yes
b. No
If, yes how many? _____

1.2. What is the major purpose of trafficking in these cases?

a. Commercial Sexual exploitation
b. Child Sexual Abuse Material (CSAM)
c. Labor exploitation
d. Forced marriage.
e. Adoption
f. Surrogacy
g. Organ Trafficking
h. Cyber-Crime
i. Other (please specify):

1.3. What is the source of information you receive regarding CEHT cases?

a. Complaint by victim
b. Tip off
c. Portal/Cyber Tipline
d. Suo Moto

1.4. What is the modus operandi / means being adopted in carrying out the crimes of CEHT?

a. False promises for employment
b. False promises for marriage
c. Financial gain
d. Cheating
e. Threats and intimidation / Blackmailing
f. Abduction / Kidnapping
g. Grooming
h. Sextortion
i. Other (please specify):

1.5. In the cases observed, what is the nature / medium of exploitation?

a. Starting physical, but exploitation mostly virtual
b. Starting Virtual, and exploitation is also virtual.
c. Mixed, both physical and virtual
d. Other (please specify):

1.6. What is the gender profile of the victims of CEHT?

a. Mostly female
b. Mostly male
c. Mixed
d. Other (please specify):

1.7. What is the average Age of the Victims in most of the cases?

a. Below 10
b. 11-15
c. 16-18
d. 19-24
e. Above 25

1.8. What are the key vulnerability factors for the victim / family?

a. Poverty
b. Illiteracy
c. Low social and caste status
d. Violence/ Abuse in home setting
e. Emotional vulnerability
f. Separation/Divorce
g. Other (please specify):

1.9. What is the average age of traffickers identified /arrested in cases of CEHT?

a. Below 18
b. 18-24
c. 25-30
d. 30-40
e. Other (please specify):

1.10. In the cases of CEHT, where are the traffickers located?

a. Within state
b. Within India, but in other states
c. Out of the country
d. Unable to locate.
e. Other (please specify):

SECTION 2: APPLICATION OF THE LAW

2.1. Which of the following Acts or Sections were used in most of the cases?

a. IPC 370
b. IPC 366A, 366B
c. IPC 372, 373
d. The Immoral Traffic (Prevention) Act, 1956 (ITPA)
e. Information Technology (IT) Act, 2000
f. POCSO, 2012
g. The Telangana Preventive Detention Act, 1970
h. Other (please specify):

2.2. Have you used the Information Technology Act 2000 in cases of human trafficking? If yes, how?

a. Use of technology in communicating with the victim
b. Use of technology in facilitating the movement of the victim
c. Use of technology in making payment of HT
d. Exploitation found on the cyber space e.g., Pornography
e. Not used any parameter
f. Other (please specify):

SECTION 3: TECH USAGE

3.1. Are you using any kind of Technologies for Detecting human Trafficking?

a. Yes
b. No

3.2. In your experience, what are the technologies used by the recruiter to spot, communicate and lure a victim?

a. Social media
b. Messaging apps
c. SMS
d. Online classified ads
e. Photo editing apps
f. Encryption tools like VPN, TOR etc.
g. Other (please specify):

Elaborate on how these technologies were used:

_____
_____
_____

3.3. Which are the websites used for Labor Exploitation?

a. Naukri
b. LaborNEt
c. eShram
d. NSDC
e. Other (please specify):

3.4. Do you know any apps or platforms that are enabling other forms of human trafficking such as Organ Trade, Adoption, Fertility, Surrogacy etc.?

_____

3.5. In your experience, what are the main payment modes used for facilitation of crimes?

a. UPI
b. NEFT/RGTS
c. Money Transfer/Western Union
d. Cheque
e. Cryptocurrency
f. Other (please specify):

3.6. Why do criminals use certain apps? What are the loopholes provided by the apps?

a. Ease of use
b. Anonymity
c. Fake Profiles
d. No payment for apps
e. Lack of screening of user profile
f. Other

3.7. Are you aware of any specialized software or services that can be used for dealing with the cases of CEHT?

a. Yes
b. No

If yes, please specify:

_____

_____

3.8. What are these software or services generally used for?

- Detection
- Investigation
- Tracking
- Evidence collection
- Other (please specify):

3.9. Can you discuss a case where technology has been used successfully in cracking a case?

_____

_____

_____

SECTION 4: REVENUE AND TRANSACTIONS

4.1. What are the primary payment methods used by traffickers in CEHT cases? (Select all that apply)

a. Cash
b. Online Bank Transfers
c. International Money Transfer
d. Digital Gift Cards – Google Gift cards, Amazon Gift Cards etc.
e. Online payments for services – UPI, GPay, PayTM, PhonePay etc.
f. Cryptocurrencies
g. Other (please specify):

4.2. In cases, has the money trail helped in identifying the traffickers? If yes, please elaborate.

a. Yes
b. No

_____

_____

SECTION 5: DIFFICULTIES IN GATHERING DIGITAL EVIDENCE

5.1. How do you collect digital evidence?

a. Collect under the seizure report
b. Call in the digital forensic expert
c. Other (please specify):

5.2 Do you have any provision to keep the custody of the digital evidence without breaking chain of custody?

a. Yes
b. No

5.3. What are the main challenges you face in gathering digital evidence in CEHT cases? (Select all that apply)

a. Lack of cooperation from tech companies
b. Servers being outside of jurisdiction/country
c. Difficulty in tracing transactions
d. Encrypted communication
e. Victims' reluctance to cooperate

f. Jurisdiction restrictions
g. Other (please specify):

5.4. What are the legal challenges that you face in admissibility of digital forensics and evidence?

a. Lack of clarity and SoP
b. Encryption in data storage
c. Inadequate digital forensic labs

5.5. When you investigate a human trafficking case, do you look for technological elements?

a. Yes, if they are present at crime scene
b. Yes, if the victim statement mentions usage of technology
c. No, if the ingredients of S370 have been met
d. Any other

5.6. When a crime of CEHT takes place, what challenges do you face during investigation?

a. Difficulty in tracing the use of technology
b. Difficulty in seizure of digital evidences
c. Difficulties in storage of digital evidence
d. Under reporting of facts by victims
e. Threat to tampering of evidence
f. Any other

5.7. What are the key challenges faced in accessing and preserving digital evidence?

_____

_____

_____

SECTION 6: DIFFICULTY WITH TECH FIRMS/INTERMEDIARIES

6.1. What support do you expect or seek from the Tech Firms/Intermediaries??

a. Provide meta data and other details in a timely manner
b. Removal of sensitive/abusive content
c. Assistance in tracking the victims
d. Assistance in tracking the accused
e. Other (please specify):

6.2. Do you encounter challenges when seeking cooperation or information from tech companies and online intermediaries?

a. Yes
b. No

6.3. If yes, what kind of issues do you face in cooperation from intermediaries?

a. They don't respond to notices
b. They don't provide information of victim/ trafficker
c. They don't have mechanisms in place to screen such activities
d. They don't conform to the IT guidelines
e. No nodal person in India

SECTION 7: CHALLENGES IN PROSECUTION

7.1. What are the main challenges in prosecuting CEHT cases, particularly in collaboration with prosecutors and the judiciary?

(Select all that apply)
a. Lack of expertise among legal professionals
b. Lengthy legal processes
c. Difficulty in presenting digital evidence
d. Lack of specific laws addressing cyber-enabled human trafficking
e. Other (please specify):

7.2. Which of the following software are used by you for investigation?

a. Oxygen Forensic
b. E Discovery
c. FTK
d. Encase
e. Password tool kit
f. Write Blocker
g. Xray mobile data extraction tool
h. IEF
i. X1 Social Discovery
j. C-5
k. Elcomsoft
l. Amped 5
m. Any other

SECTION 8: SUPPORT FOR LAW ENFORCEMENT MECHANISMS

8.1. Are the State Institutes/ Police Academy giving trainings to handle/tackle CEHT cases? If yes, describe.

_____

_____

8.2. What kind of support / cooperation do you need from other departments within your state? interdisciplinary/ intrastate / interstate / International for case management?

_____

_____

8.3. What kind of support / cooperation do you need from other states?

_____

_____

8.4. What kind of support / cooperation do you need from other countries?

_____

_____

_____

8.5. What kind of support do you need to efficiently deal with CEHT cases? Describe under each of the following:

a. Training on application of laws
b. Training on Detection and investigation of crimes
c. Training on usage of technology
d. Access to up-to-date Technology Infrastructure
e. Dedicated budget – for investigation, logistics
f. Any other

SECTION 9: VICTIM PROTECTION AND CHALLENGES FACED

9.1. What challenges do victims face in CEHT cases when it comes to reaching out for help or escaping their situation? (Select all that apply)

a. Fear of retaliation
b. Lack of awareness about available support
c. Limited internet access
d. Coercion and control through technology
e. Other (please specify):

9.2. Are there victim service provisions available for victims of CEHT?

a. Yes
b. No

9.3. If yes, what support do you extend to the victims of CEHT?

a. Victims are provided legal aid.
b. Victims are taken in protection.
c. Content removal
d. Any other

9.4. How can victim protection services be improved? Give suggestions.

_____
_____
_____

SECTION 10: RECOMMENDATIONS

10.1. What recommendations do you have for state governments to improve the legal and operational framework for addressing CEHT?

_____
_____
_____
_____

10.2. Do you have any suggestions for the improvements of investigation process?

_____
_____
_____
_____

10.3. What recommendations do you have for technology companies to assist law enforcement in addressing CEHT effectively?

_____
_____
_____
_____

10.4. What form of improvement do you suggest tackling with CEHT? (Select as many)

a. Separate law on CEHT
b. Inclusion of cyber and technology as means under S370.
c. Trainings on existing laws of technology
d. Campaigns on spreading awareness on CEHT.
e. Any other

Annexure V

Framework for Focused Group Discussion

FORMAT FOR FGD CASE STUDY

1. Suggested Title:
2. Status of Case:
3. Police Station:
4. Details of Complainant:
5. Profile of Victim:
6. Details of the alleged accused:
7. Details of the Case:
8. Usage of Technology / Cyber:
9. Suspected purpose of Trafficking / Exploitation:
10. Inferences drawn from the Researcher:

FORMAT FOR OTHER INFORMATION

1. Trends and Patterns
2. Main Technology Enablers:
    a) Spotting
    b) Recruiting
    c) Transporting / Harbouring
    d) Payment/Revenue
    e) Exploitation
3. Case detection methods, challenges
4. Reasons in reporting and challenges
5. Challenges in investigation
6. Loopholes in technology (used by perpetrator)
7. Capacity Building

Annexure VI

Framework for Inter-nation Consultation

1. General Understanding

a) Patterns of trafficking
b) Purposes of trafficking
c) Nature of exploitation (Physical, Physical-virtual, Only Virtual)
d) Profiles of victims- age, background (family, relations, economic strata), personality, region, socio-cultural conditions etc.
e) Revenue Model
f) Role of Tech Enabler
g) International Mutual Cooperation and International Statutes

2. Legal Framework

a) Specific laws
b) Challenges in application
c) Strengths-used/not used
d) Provisions for victims, challenges
e) Accountability of the Tech Enablers

3. Law Enforcement

a) Challenges in fixing tech enablers
b) Collection and storage of digital evidences
c) Status of digital forensics
d) Preparedness of criminal justice system-police, prosecutor, judges to deal with cyber enabled trafficking-training/upgradation
e) Challenges faced with Tech Firms to share info/leads
f) Victim dependence for prosecution

4. Technology

a) Various technologies present in the country which is being exploited for HT
b) Tech solutions to address the problem
c) Tech solutions to improve safe-guarding within the existing systems
d) Challenges in technology on surface web

PRAJWALA

AN ETERNAL FLAME

PRAJWALA

www.prajwalaindia.com