“CRIMES IN CYBERSPACE: A THREAT TO HUMAN RIGHTS & NATIONAL SECURITY.”

GROUP 1 TEAM MEMBERS

Aditi Vyas

Aishwarya Motwani

Aniket Grover

Akanksha Rawet

Anjali Yadav

Alayka Aftab

Anmol Gupta

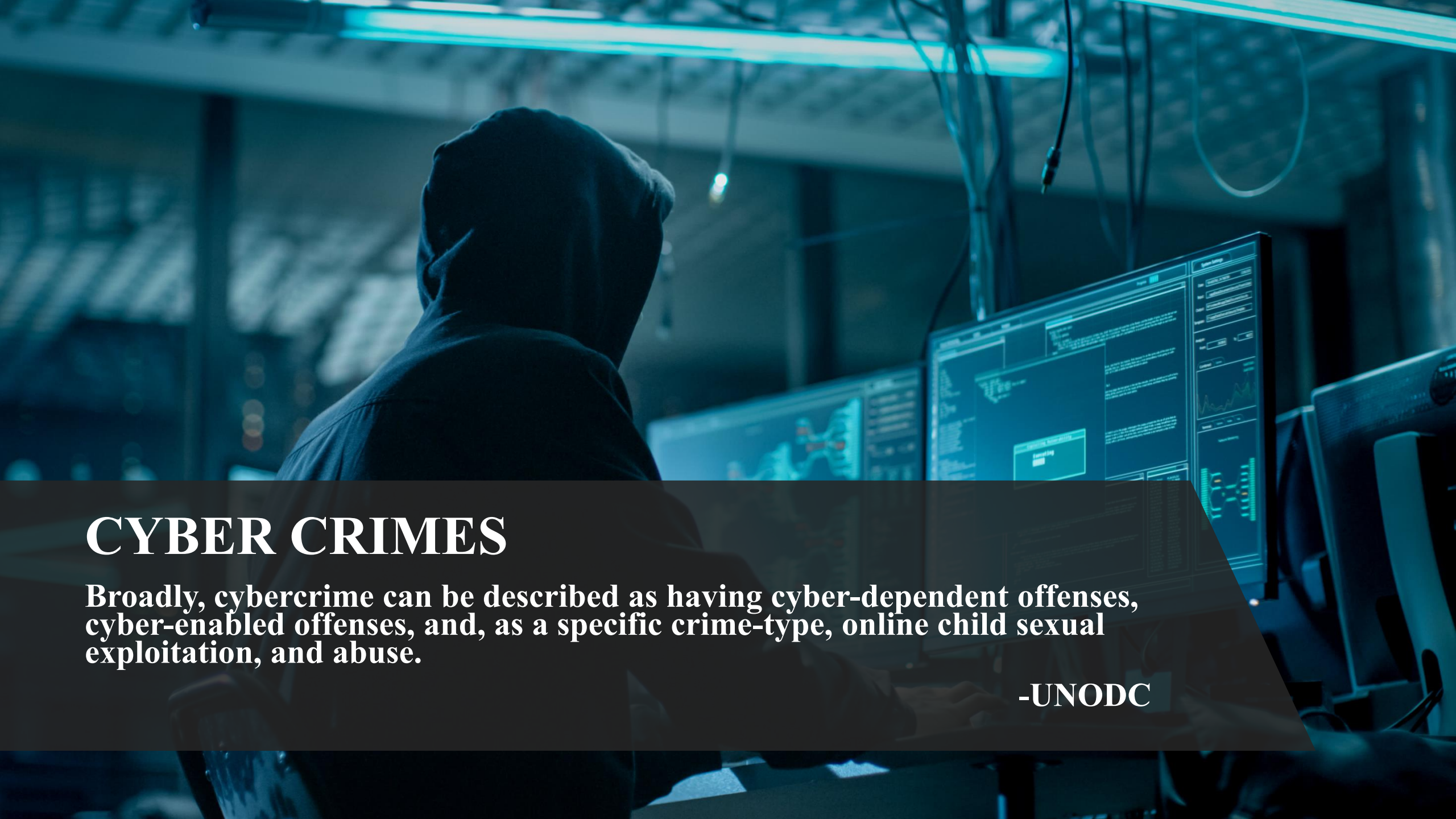
Anushka Kishwar

Akshaya S. Kumar

Anantika Kushwaha

Arista Dalal

TABLE OF CONTENTS



CYBER CRIMES

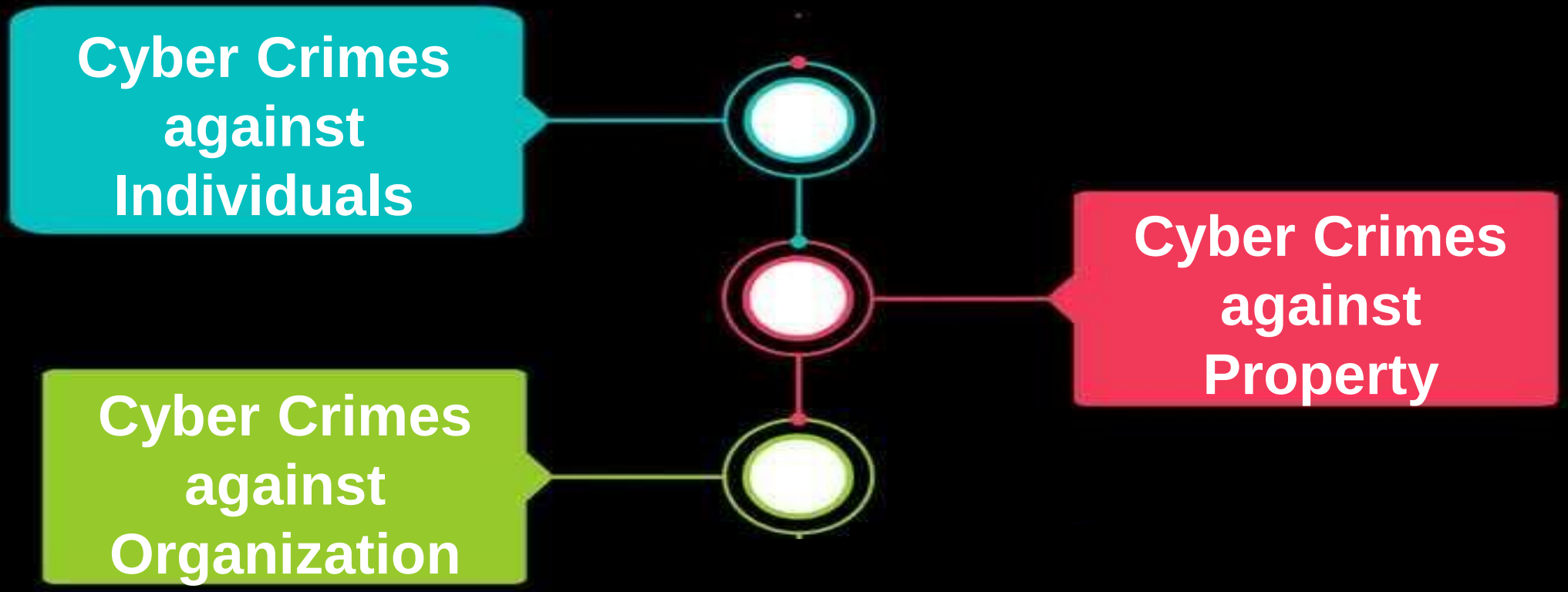
Broadly, cybercrime can be described as having cyber-dependent offenses, cyber-enabled offenses, and, as a specific crime-type, online child sexual exploitation, and abuse.

-UNODC

Cyber Crimes as threat to Human Rights and National Security

Cybercrime violates human rights such as the right to privacy, the right to secrecy, and the right to be free from any kind of blackmailing and torture. It is also a threat to national security in the form of cyber terrorism and espionage.

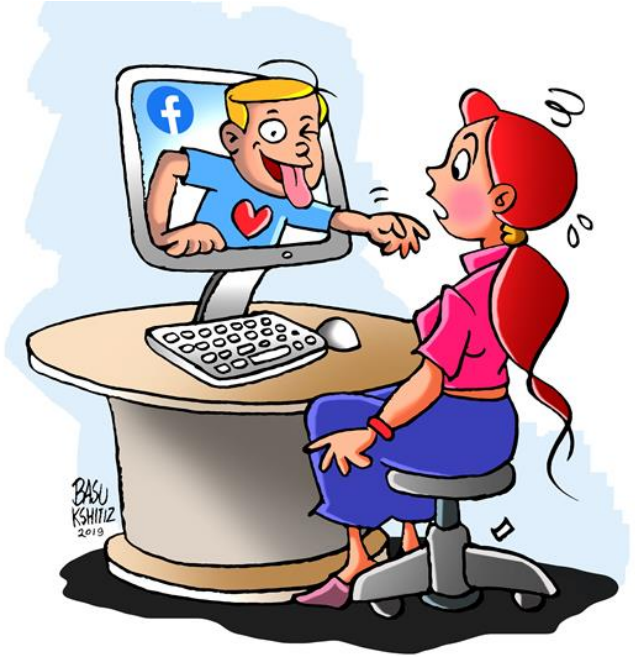
Types of Cyber Crime



Cyber Crimes against Individual

Cyber Sexual Harassment

Cyber sexual harassment involves the actions of a person or persons toward the victim in cyberspace which causes emotional distress, mental harassment, gender harassment, invasion of privacy, etc.



Cyber Bullying

When a person or group of persons, bully, or harass another, with the use of digital technologies, on the internet, or in another digital sphere, is considered cyberbullying.

Child Pornography

Child pornography is defined by the Optional Protocol on the Sale of Children, Child prostitution, and Child pornography as any representation of a child engaged in real or simulated explicit sexual activities or of the sexual parts of a child for primarily sexual purposes.

Cyber Stalking

Cyberstalking is an activity in which a person or abuser or stalker stalks or harass another person or victim by misusing the internet or electronic media.

Cyber Crimes against Property

Phishing

Phishing is an attempt by cybercriminals posing as legitimate institutions, usually via email, to obtain sensitive information from targeted individuals and fraudulent communications that appear to come from a reputable source. It is usually done through email.

ATM Skimming

ATM skimming is a type of payment card fraud. It is a way of stealing PINs and other information off credit cards and debit cards by rigging machines with hidden recording devices.

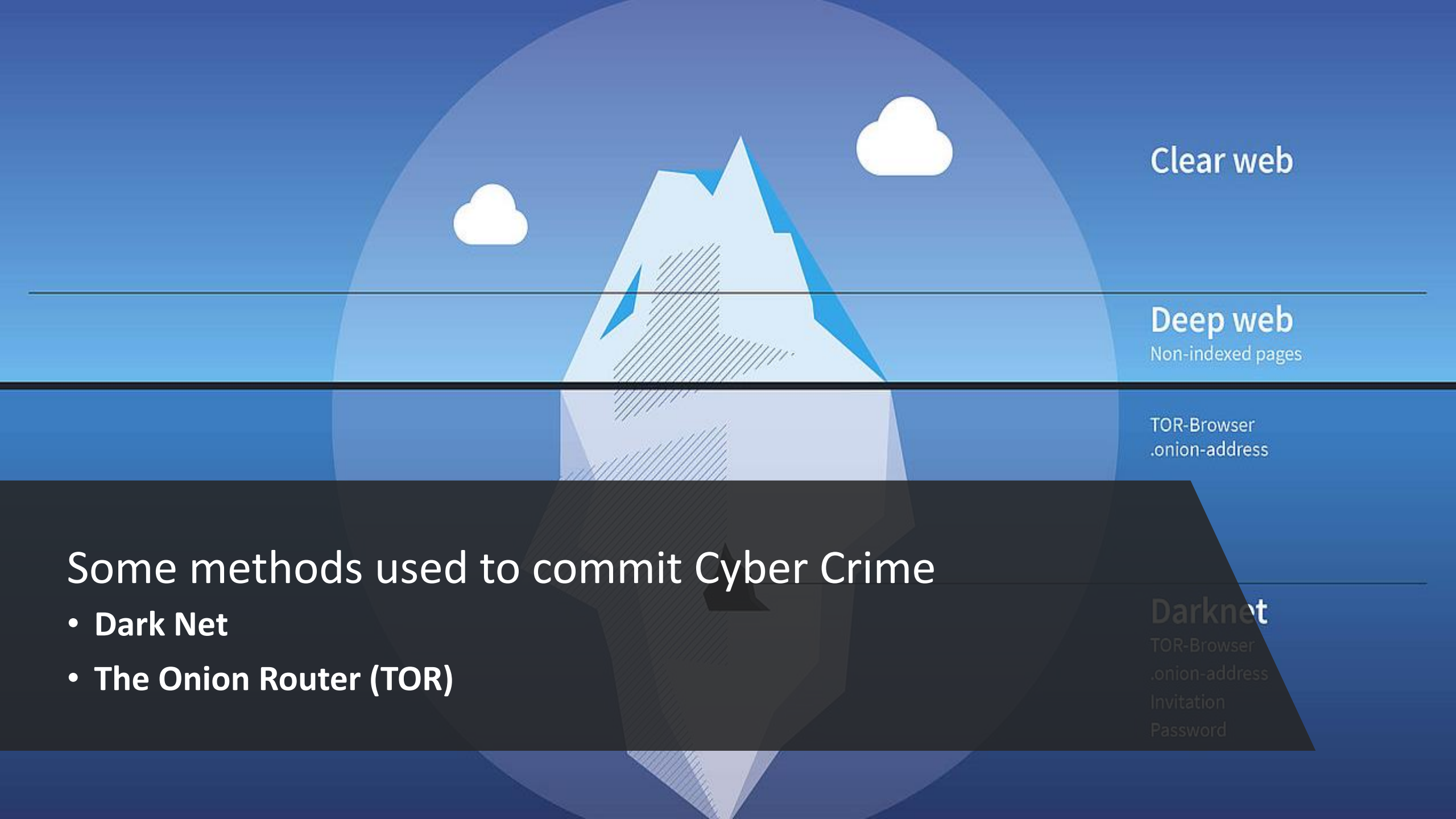
Cyber Crimes against Organization

Cyber Terrorism

Cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

Espionage

It refers to stealing classified, sensitive or intellectual property with the help of digital devices to gain an advantage over a competitive company or government.



Some methods used to commit Cyber Crime

- **Dark Net**
- **The Onion Router (TOR)**

India's ranking in the global security Index 2020

- India has made it to the top 10 in Global Cybersecurity Index (GCI) 2020 by ITU, moving up 37 places to rank as the tenth best country in the world on key cyber safety parameters.

Research Questions

How do Cybercrimes violate the Human rights of the victim?

What are the measures undertaken to tackle cybercrimes?

What are the challenges in countering Cybercrimes in India?

What can be recommended to deal with the challenges?

Data Analysis

Cyber Crime against Individual

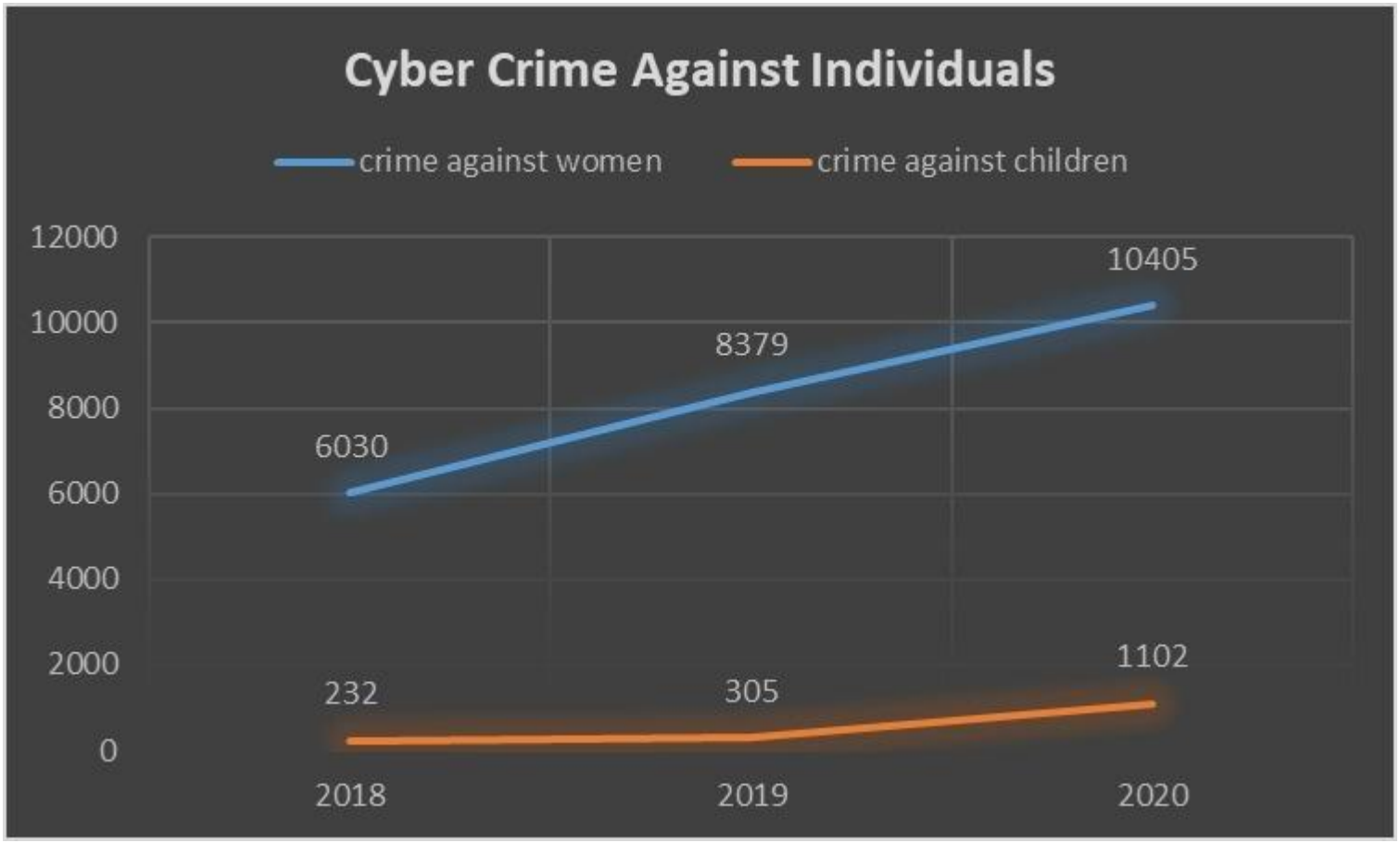


Chart 1 (Source: NCRB)

Cyber Crime against Property

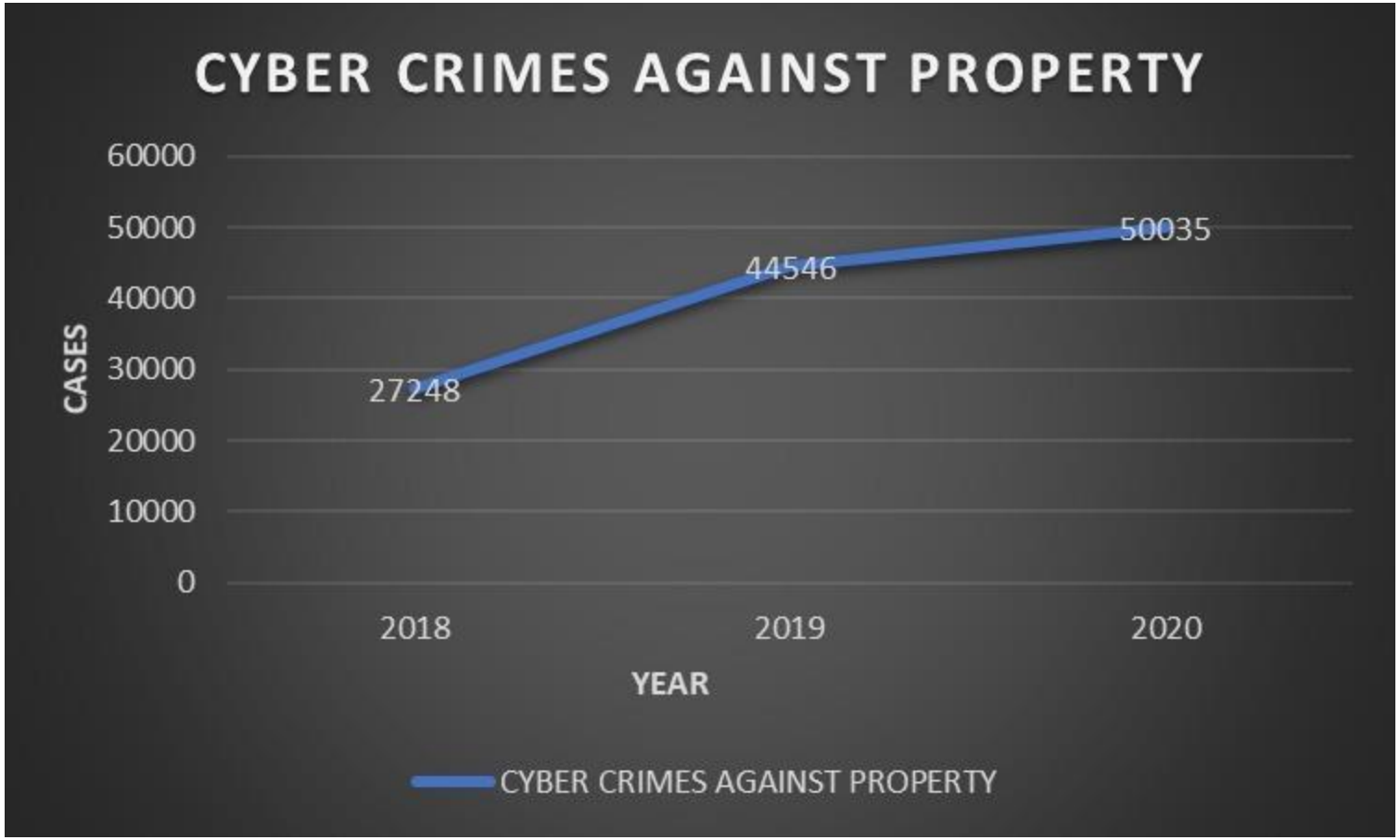


Chart 2 (Source: NCRB)

Cyber Crime against Organization

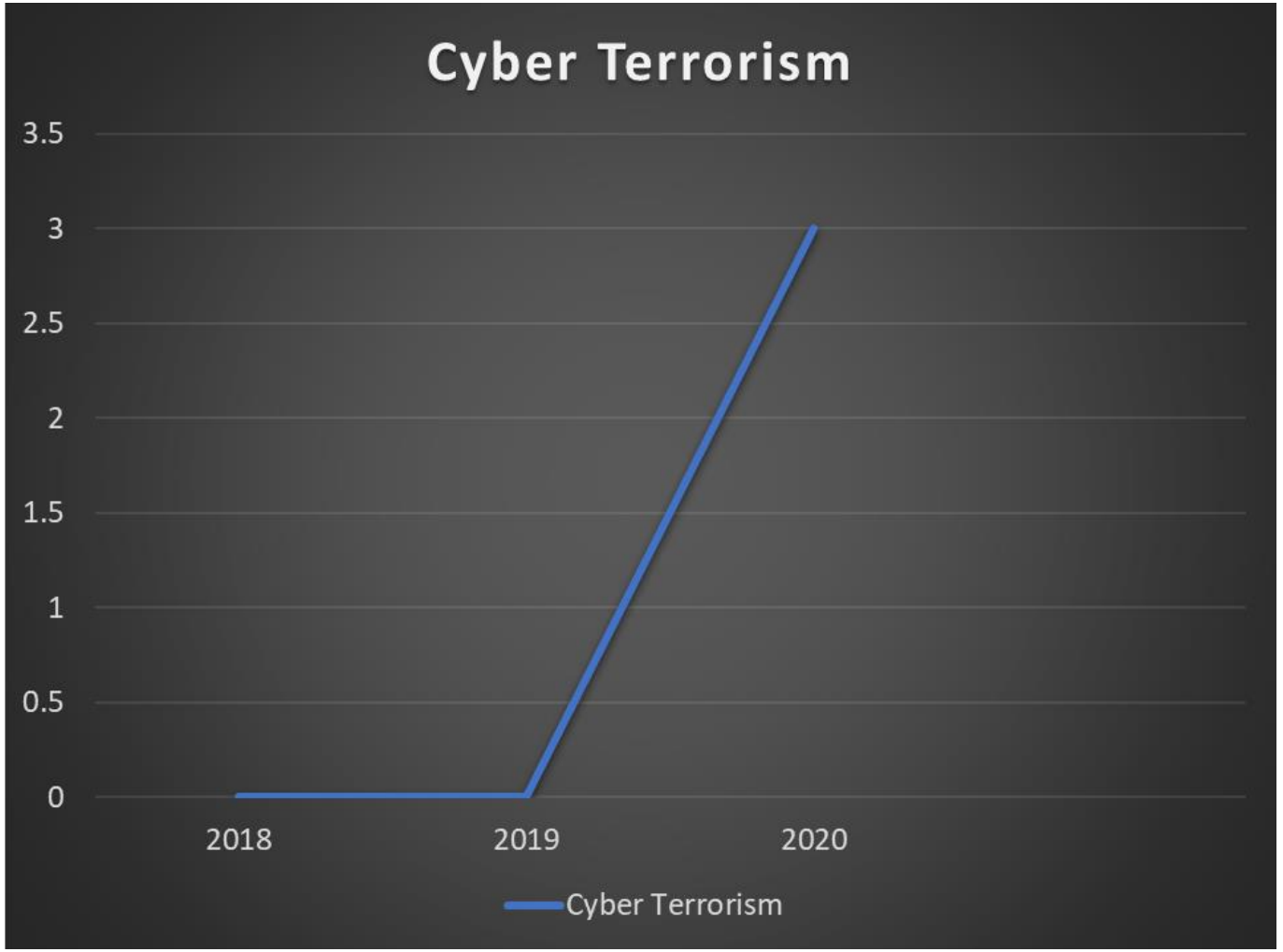


Chart 3 (Source: NCRB)

Laws Concerning Cyber Crime

The Information Technology Act of India, 2000

Indian Penal Code, 1860

Indian Evidence Act, 1872

Protection of Children from Sexual Offences Act, 2012 (POCSO)

National Policy on Information Technology, 2012

Efforts taken by the Government

- Personal data protection bill, 2019
- Blocking malicious apps
- Comprehensive Changes in Criminal laws
- CERT- In
- Initiative programs by govt
- Indian Cyber Crime Coordination Center
- NATGRID
- Creating a post of National Cyber Security Coordinator

Challenges

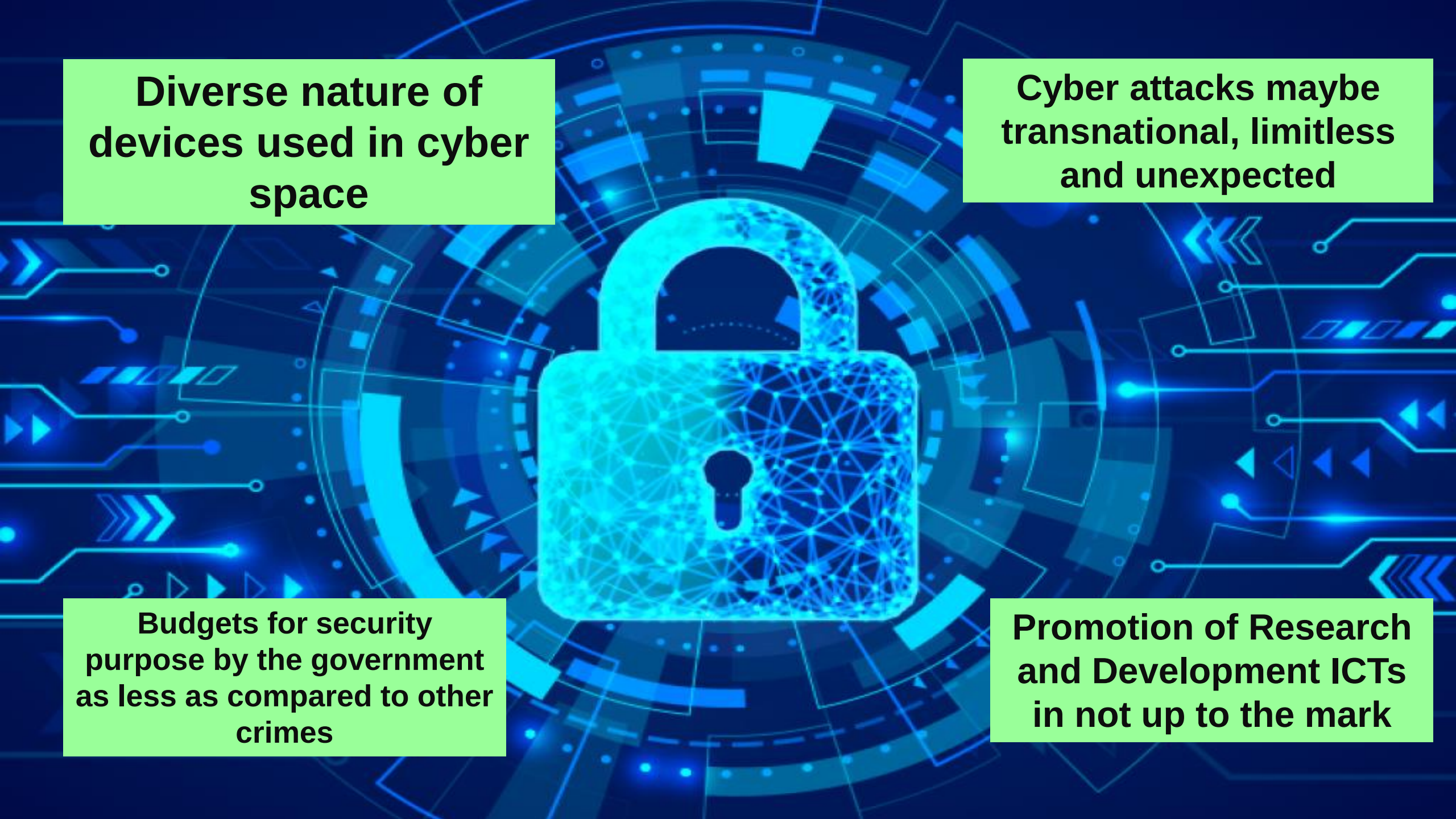
Lack of specific legislation

Dynamic nature of cyber technology

Lack of awareness of cyber security

Lack of self sufficiency of existing protocols

Lack of trained and qualified manpower to implement countermeasures


Diverse nature of devices used in cyber space
Cyber attacks maybe transnational, limitless and unexpected
Budgets for security purpose by the government as less as compared to other crimes
Promotion of Research and Development ICTs in not up to the mark


A
B
C
D
E
RECOMMENDATION

Cyber Crimes against Individuals

- Awareness camps for Elders, women and children
- Reporting suspicious activities
- Parent and Child counselling
- Cyber awareness programs for children
- Avoid disclosing sensitive information
- Increased patrolling on the internet
- 4-tier cyber cell mechanism
- Universal enforcement jurisdiction
- Designing privacy policies for social media platforms
- Monitoring activities
- Application of cyber experts

Cyber Crimes against Property

- Data access using public Wi-Fi
- Upgrading KYC norms
- Premium domain name registration
- Purchase domain directly from a registrar
- Use of encryptions (Curb Cyber Vandalism)
- Staying vigilant on domain names
- Third party insurance
- Installation of anti-spy and firewall settings
- Monitor and report violation under respective acts

Cyber Crimes against Organisation

- Doctrine of Loss Minimization
- Security of use of third-party software systems
- Restrictions of data availability
- Techniques used in cyber-Espionage attacks
- Monitor system for unexpected behaviors
- Bring your own device
- Partnership with Private Industry.
- Support & Train Cyber Dept. in every State
- Establish Cyber Fusion Cell (CFC)
- Establish more Digital Forensic Labs. in India
- Educate employees about security & policies

Technical Preventive measures & recommendations to oppose Cyber crimes

DATA RECOVERY

- Development of new Technology
- Use blocking & filtering programs
- Monitoring controls of money
- Bring your own device
- Use of authentic technologies

CBI now part of Interpol's anti-child abuse database

Interpol's database, which has over 2.7 million images and videos on an average, helps in the identification of at least seven abuse survivors across the globe per day.

THANK YOU!!!

ONLINE SHORT-TERM INTERNSHIP UNDER NATIONAL HUMAN RIGHTS COMMISSION

RESEARCH PAPER PROJECT SUBMISSION

"CRIMES IN CYBERSPACE: A THREAT TO HUMAN RIGHTS & NATIONAL SECURITY."

SUBMITTED BY- GROUP NO.1

ROLL NO. 1-12

SUBMITTED BY- GROUP NO.1

ROLL NO. 1-12

1. **Aditi Vyas**, BBA LLB, 3rd year, BM Law College, Jodhpur.
2. **Aishwarya Motwani**, MBA 1st year(HR), Harcourt Butler Technical University, Kanpur, Uttar Pradesh.
3. **Akanksha Rawet**, MA Political Science (Hons), 1st Year, Patna, Women's College (Autonomous), Bihar.
4. **Akshaya S. Kumar**, 5th year, BBA LLB (Hons), School of Excellence in Law, The Tamil Nadu Dr Ambedkar Law University, Tamil Nadu.
5. **Alayka Aftab**, MA in Sociology, 2nd year, Presidency University.
6. **Anantika Kushwaha**, MBA 1st year, Delhi Technological University, New Delhi.
7. **Aniket Grover**, BA LLB, 4th year Chandigarh University, Mohali (Punjab).
8. **Anjali Yadav**, B.A. prog, 3rd year, Lakshmibai College, University of Delhi, Delhi.
9. **Anmol Gupta**, BA LLB, 3rd year, School of Law, Guru Ghasidas Central University, Chhattisgarh.
11. **Anushka Kishwar**, BBA LLB, 4th year, GGSIPU, New Delhi.
12. **Arista Dalal**, BA LLB (Hons) 3rd year, Maharshi Dayanand University, Rohtak.

SUBMITTED TO-

SHRI. MUKESH KULSHRESHTA

(Consultant (SRO) Training, NHRC)

TABLE OF CONTENTS

ABBREVIATIONS

1.	ATM	Automated Teller Machine
2.	BYOD	Bring Your Own Device
3.	CERT	Computer Emergency Response Team
4.	IIP	Invisible Internet Project
5.	ICTs	Information and Communication Technology
6.	INTERPOL	International Criminal Police Organization
7.	IP	Internet Protocol
8.	IPC	Indian Penal Code
9.	IT	Information Technology
10.	ITES	Information Technology Enabled Services
11.	KYC	Know Your Customer
12.	MHA	Ministry of Home Affairs
13.	NATGRID	National Intelligence Grid
14.	NCB	Narcotics Control Bureau
15.	NCFL	National Cyber Crime Forensic Library
16.	NCIIPC	National Critical Information Infrastructure Protection Centre)
17.	NCRB	National Crime Records Bureau
18.	NIA	National Investigation Agency
19.	OTP	One Time Password
20.	PIN	Personal Identification Number
21.	POCSO	Protection of Children from Sexual Offences
22.	RAW	Research and Analysis Wing
23.	TOR	The Onion Router
24.	UDHR	Universal Declaration of Human Rights
25.	UOI	Union of India
26.	USB	Universal Serial Bus
27.	UTs	Union Territories
28.	VPN	Virtual Private Network
29.	Wi-Fi	Wireless Fidelity
30.	WWW	World Wide Web

ACKNOWLEDGEMENT

Completing this project would not have been possible without the support and guidance of a lot of individuals. We would like to extend our sincere thanks to all of them. We would like to thank National Human Rights Commission (NHRC).

We would like to express our special thanks of gratitude to NHRC who gave us the opportunity to do this wonderful research paper on the topic ***"Crimes in Cyber-Space: Measures and Challenges to control it".*** We are highly indebted to Mr. Mukesh Kulshreshta for his supervision. We would also like to thank Mr. Sam T John for his guidance and providing the necessary information and resources for this project. Lastly, we would like to express our gratitude towards our parents for their kind co-operation and encouragement. Thank you to all the people who have willingly helped us out with their abilities

Date: 28/04/2022

GROUP 1

NHRC Interns

APRIL 2022

ABSTRACT

Cyber Crime is an emerging crime. It is dynamic in nature as Internet is expanding and covering the global space. Hence, Crime is moving to a large scale and each year the categories of cybercrimes are increasing. With the development in cyber-space came various challenges. Cyber security has become a major challenge for this ever-changing society. It can be rightfully said that cyber-space is both a boon and bane at this time. It has two sides, at one end great achievements can be made while using while at another end it can be misused for unethical purposes. The growth of Cybercrimes is rapid. It can be seen that in the past three years there is a significant rise in the cybercrime's cases. This situation is alarming and startling.

This paper focuses on the concept of cybercrimes, the motivations for committing cybercrimes, and different cybercrimes against individuals, property, and society. It also focuses on various legislations and conventions concerning cyberspace. Further, it also focuses on challenges concerning the handling of cybercrimes and the methods and recommendations to curb the same.

Keywords: *Cyber Crime, Cyber Attacks, Cyber Security, Information, Internet, Technology, Cyber Ethics, Social Media*

INTRODUCTION

"Cybercrime poses a real threat to people's human rights and livelihoods and efforts to address it need to protect, not undermine rights. Governments should oppose overbroad and aggressive cybercrime measures that threaten rights."

-Deborah Brown[1], senior digital rights researcher and advocate at Human Rights Watch.

In this era of technology, it is impossible to live without the internet. The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and

[1] Deborah Brown is a senior researcher and advocate on digital rights at Human Rights Watch. Her areas of focus include the role of digital technologies in electoral processes, cybersecurity, and digital exclusion.

communication technologies (ICTs) are omnipresent and the trend toward digitization is growing.

India is the second-largest online market in the world with over 560 million internet users, ranked only behind China.[2] The introduction of the internet has made our life so much easier. It has made us dependent on it for every little thing. However, this Internet is also a "double-edged sword." Along with the convenience, also comes the inconvenience of crime in the virtual world.

The Internet was originally built for research. The rapid evolution of the computer networks that comprise the Internet has provided a gateway for offenders and deviant entrepreneurs. The internet revolution brought in a lot of changes in our world. One of them included how crimes were being committed. The crimes being committed in the physical world changed their shape and shifted towards cyberspace.

Cyber-crimes or the crimes committed in cyberspace is a broad term used to define crimes committed in which computers, mobiles, or any computer networks are used as a tool, or as a platform to commit criminal or illegal activity. The crimes in cyberspace have no limits and boundaries. Cybercrime violates human rights such as the right to privacy, the right to secrecy, and the right to be free from any kind of blackmailing and torture. Hackers usually lock secret data of the user or of any company and demand ransom to unlock them, they also steal data and misuse them. There are several landmark judgments on cybercrime in India. The first cybercrime occurred in 1992 when the first polymorphic virus was released.[3]

The case of **Yahoo v. Akash Arora (1999)** was one of the earliest examples of cybercrime in India. The defendant, Akash Arora, was accused of utilizing the trademark or domain name 'yahooindia.com,' and a permanent injunction was sought in this case.[4]

---

[2] Sakshi Singh, Suresh Kumar, The Times of Cyber Attacks, ACTA TECHNICA CORVINIENSIS – Bulletin of Engineering [e-ISSN: 2067–3809] TOME XIII [2020] | FASCICULE 3 [July – September]

[3] Sehar Qayyum, Samiya Rafiq, Prohibited Activities of Computer, Journal of Information Engineering and Application, Vol.7, No.1, 2017

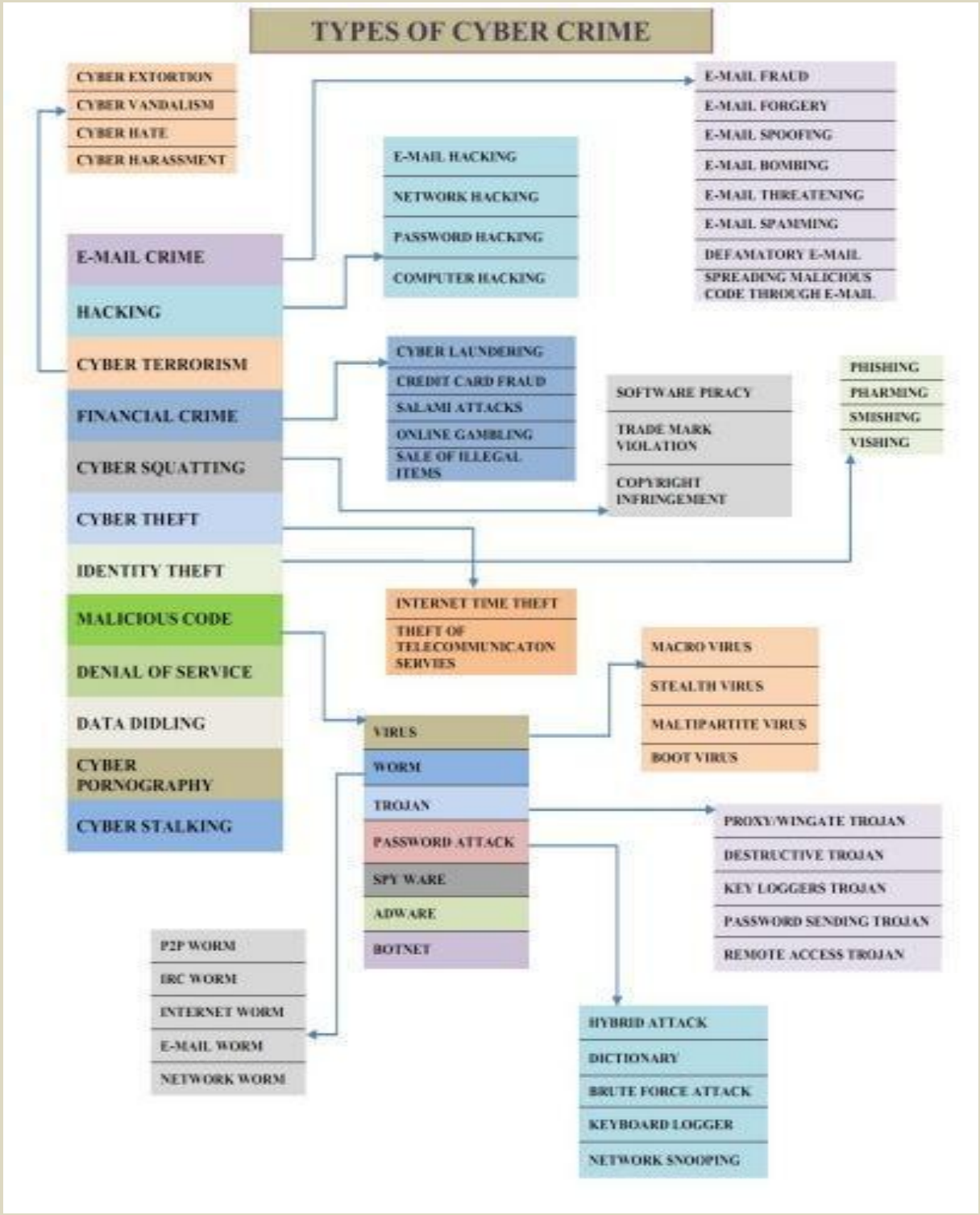
[4] Yahoo! Inc. v. Akash Arora and another, 1999 Arb. L. R. 620 (Delhi High Court).

With the increasing use of computers in society, cybercrime has become a major issue. Crimes in cyberspace range from a variety of activities. These include monetary crimes as well as non-monetary crimes. These crimes in cyberspace result in damage to persons, computers, and governments. They are broadly categorized into three categories, namely crime against Individuals, Property, and the Government. Each category can use a variety of methods and the methods used vary from one. The Crimes in cyberspace against the individual include cyberstalking, harassment, child pornography, and phishing. The crimes against the property include computer vandalism, harmful program transmission, and hacking. Crimes against the government include cyber terrorism and cyber warfare.

The world has united to take a stand against this crime as it cannot be tolerated. The laws and the way of overseeing these crimes vary from country to country since the form of crime also differs. Cybercrime is one of the most prevalent crimes playing a devastating role in modern India. Several measures are being adopted to tackle the situation, but nothing is enough. Governments should oppose overbroad and aggressive cybercrime measures that threaten rights. However, countering cybercrime should not come at the expense of the fundamental rights and dignity of innocent citizens. To achieve such a balance in which both human rights and national security concerns are respected, it is important to have guidelines that could help States develop an online environment that does not hamper individuals' privacy and freedom of expression.[5]

[5] Online privacy and freedom of expression, IPDC, UNESDOC, Page 9, CI-14/CONF.202/Inf.4, 10 October 2014

CLASSIFICATION OF CYBER CRIME



There are many types of cybercrime prevailing in the system; broadly we can classify them in to four major categories as discussed below:

1. **CRIME AGAINST INDIVIDUALS:** Cybercrimes committed against individual persons include such types of crimes like transmission of Child Pornography, Harassment of any one with the use of a computer. such as e-mail, Cyber Defamation, Hacking, Indecent exposure, E-mail spoofing, IRC Crime (Internet Relay Chat), Net Extortion, Malicious code, Trafficking, Distribution, Posting, Phishing, Credit Card Fraud and Dissemination of obscene material including Software Piracy. The potential harm of such a crime to individual person can hardly be bigger.

2. **CRIME AGAINST PROPERTY:** Another classification of Cyber-crimes is that Cybercrimes against all forms of property. These crimes include computer vandalism (obliteration of others' property), Intellectual Property Crimes, Threatening, Salami Attacks, Data Breach, hacking of data of institutions. This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the amendment is so small that it would normally go unobserved.

3. **CRIME AGAINST ORGANIZATION/STATE:** The third type of Cyber-crimes classification relate to Cybercrimes against organization/State. Cyber Terrorism is one discrete kind of crime in this kind. The growth of internet has shown that individuals and groups are using the standard of Cyberspace to pressure the international governments as also to terrorize the citizens of a country. This crime obvious itself into terrorism when a human being "cracks" into a government or military maintained.

4. **OTHER TYPES OF CYBER CRIME :** There are several other types of cyber crime which includes, crime in metaverse (metaverse gangrape case), and cases like bulli bai and sulli deals.

DEFINING VARIOUS CYBERCRIMES

❖ Crimes against Individual

Cyber Sexual Harassment: Cyber sexual harassment involves the actions of a person or persons towards the victim in the cyberspace which causes emotional distress, mental harassment, gender harassment, invasion of privacy etc.

Cyber Bullying: When a person or group of persons, bully, or harass another, with the use of digital technologies, on the internet or other digital sphere, is considered cyberbullying.

Child Pornography: Child pornography is defined by the Optional Protocol on the Sale of Children, Child prostitution and Child pornography as any representation of a child engaged in real or simulated explicit sexual activities or of the sexual parts of a child for primarily sexual purposes.

Cyber Stalking: Cyberstalking is an activity in which a person or abuser or stalker stalks or harass another person or victim by misusing the internet or electronic media.

Cyber Grooming: It is "the process of 'befriending' (often an adult befriends a child) another person online to facilitate

an emotional connection with future online sexual contact and/or a physical meeting with them with the goal of committing sexual abuse, sexual exploitation, or trafficking." The main goals of cyber grooming are to gain trust from the child, to obtain intimate and personal data from the child[6] in order to threaten and blackmail for further inappropriate material.[7]

❖ Cyber Crimes against Property

Phishing: Phishing is an attempt by cybercriminals posing as legitimate institutions, usually via email, to obtain sensitive information from targeted individuals and fraudulent communications that appear to come from a reputable source. It is usually done through email.

Cyber Squatting: Cybersquatting means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example, two similar names i.e., www.yahoo.com and www.yaahoo.com.

Hacking: Hacking is gaining unauthorized access to your system profit, protest, information gathering, or to evaluate system weaknesses. Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity, there will be loss of data as well as computer. Also research especially indicates that those attacks were not intended for financial gain too and to diminish the reputation of particular person or company.

[6] (Often sexual in nature—such as sexual conversations, pictures, or videos)
[7] https://www.childsafenet.org/new-page-15

Transmitting Virus: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays significant role in affecting the computerize system of the individuals.

Cyber Trespass: It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.

Cyber Vandalism: Vandalism means deliberately destroying or damaging property of another. Thus, cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.

ATM Skimming: ATM skimming is a type of payment card fraud. It is a way of stealing PINs and other information off credit cards and debit cards by rigging machines with hidden recording devices.

❖ Cyber Crimes against Organization /Government

Cyber Terrorism: Cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

Cyber Warfare: It refers to politically motivated hacking to damage and spying. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.

Distribution of Pirated Software: It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.

Possession of Unauthorized Information: It means to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

MEANS THAT ARE DEPLOYED TO COMMIT CYBERCRIME

Dark Net - A **dark net** or **darknet** is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization,[1] and often uses a unique customized communication protocol.

Technology such as Tor, I2P, and Freenet was intended to defend digital rights by providing security, anonymity, or censorship resistance and is used for both illegal and legitimate reasons. Anonymous communication between whistle-blowers, activists, journalists and news organizations is also facilitated by darknets through use of applications such as Secure Drop.

THE ONION ROUTER(TOR) - Tor, short for **The Onion Router**, is free and open-source software for enabling anonymous communication.] It directs Internet traffic through a free, worldwide, volunteer overlay network, consisting of more than six thousand relays,[8] to conceal a user's location and usage from anyone performing network surveillance or traffic analysis.[9]

Using Tor makes it more difficult to trace a user's Internet activity. Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to communicate confidentially through IP address anonymity using Tor exit nodes.

ATM SKIMMER - A skimmer is a device that is rigged to the card reader of an ATM machine. An unsuspecting user will enter their card into the ATM, not knowing that the device attached to the slot (unnoticed or ignored) has proceeded to record their payment card data.

TROJAN HORSES - The Trojan horse is a program that inserts instructions in the software of the information system to perform unauthorized acts or functions. This type of abuse is exceedingly difficult to identify and much more difficult to fix responsibility.

PIGGYBACKING - Piggybacking is an abuse technique in which the unauthorized access to information is obtained after the authorized user has exchanged the identification and authentication information with the server of information. The unauthorized access may be gained by a parallel connection with the information server remaining untraced.

REASONS BEHIND THE CYBER CRIME

There are many reasons why cyber-criminals are doing cyber-crime; chief among them is mentioned below:

A. For the sake of recognition.

B. For the sake of quick money.

C. To fight a cause one thinks he believes in.

D. Low marginal cost of online activity due to global reach.

E. Catching by law and enforcement agencies is less effective and more expensive.

F. New opportunity to do legal acts using technical architecture.

G. Official investigation and criminal prosecution are rare.

H. No concrete regulatory measure.

I. Lack of reporting and standards

J. Difficulty in identification

K. Limited media coverage.

L. Corporate cybercrimes are done collectively and not by individual persons

CYBER SECURITY, CYBER CRIME AND HUMAN RIGHTS

The internet has been in existence since the 1960s and the World Wide Web (WWW) since the 1990s. The International Telecommunications Union estimates that almost 40% of the world's population and over 76% of people in developed countries are now internet users.[8] Government, business, and organizations in civil society are increasingly using cyberspace platforms in the communication of information and delivery of services. But due to the increase in cybercrime and cyber security, the concerned question that arose is the impact of cyber security and cybercrime on Human rights? Does it infringe Human Rights?

- **CYBER SECURITY AND HUMAN RIGHTS**

Many international or domestic laws apply to cyber security, Article 19 of the UDHR includes protections of freedom of speech, communication, and access to information. Similarly, Article 3 states that everyone has the right to life, liberty, and security of a person, but enforcing these rights is difficult under international law. As a result, many countries like India ignore the rules.

Cyber security breaches the human rights of freedom of speech and expression, right to privacy, freedom of opinion, and free flow of information. The government has created many policies which intend to protect a crime-related computers, but many of these policies are overly broad and ill-defined and lack clear checks and balances or other democratic accountability

[8] Measuring digital development facts and figures (2020), International Telecommunication Union

mechanisms, which can lead to human rights abuses and can stifle innovation. This all reveals that the state defines security as protecting itself from political instability, applies disproportionate measures to ensure its preservation, and itself becomes the source of insecurity.

As we see there were some restrictions on social sites on what we can write, speak, or post. More often cyber security laws can be used to censor dissidents, monitor communications, and criminalize online users for expressing their views. Government officials can at any point in time and track users' communication whenever they felt suspicious about someone, sometime their assumptions result absurd. This all directly violates human rights given by UHDR or countries own law.

For example, the surveillance of Saudi dissident Omar Abdulaziz contributed to the extrajudicial execution of Saudi journalist Jamal Khashoggi. According to a lawsuit, Abdulaziz's cell phone was targeted by the Saudi Arabian government with spyware, compromising the confidentiality of his communications with Khashoggi about opposition projects in the months leading up to Khashoggi's killing.[9]

SHREYA SINGHAL vs. UOI[10]

This is a case of 2012, in which two girls were arrested by Mumbai Police for expressing their displeasure against a strike by the Shivsena for the Shivsena chief's death. The accusation made against the petitioners was that they engaged in posting their comments on Facebook and liking the comment at the same time which resulted in widespread public protest. The issue raised in this case was, Whether Sections 66-A, 69-A, and 79 of the IT Act are constitutionally valid? And Whether Section 66A of the IT Act is violative of the fundamental right of freedom of speech and expression?

The court observed that the expressions used in 66A are completely open-ended and undefined and it is not covered under Article 19(2) of the Indian Constitution. Section 66A had no

[9] David D. Kirkpatrick. (2018, Dec 2). Israeli Software Helped Saudis Spy on Khashoggi, New York Times. Retrieved from https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html
[10] AIR 2015 SC 1523; Writ Petition (Criminal) No. 167 OF 2012

proximate connection or link with causing disturbance to public order or with incitement to commit an offence and hence it was struck down by the court.

The approach adopted by the court was to protect the fundamental right of freedom of speech and expression and in no way the legislation can take away this right by claiming the shield under Article-19(2) of the Constitution.

- **CYBER CRIME AND HUMAN RIGHTS**

Cybercrime violates human rights such as the right to privacy, the right to secrecy and the right to be free from any kind of blackmailing and torture. Hackers usually lock secret data of the user or of any company and demand ransom to unlock them, they also steal data and misuse them. Like in the recent case they hacked the Twitter account of many well-known persons and misuses their accounts to collect money by fraud, some demanded money to give back to their accounts. They blackmail and violates children's rights by using their videos and pictures on different sites.

NASSCOM v AJAY SHOOD & ORS.[11]

It was a landmark judgment by the Delhi High Court, phishing' on the internet was declared to be an illegal act, entailing an injunction and recovery of damages. The Supreme Court stated that phishing is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. The Delhi HC stated that even though there is no specific legislation in India to penalize phishing still the court held the act of phishing as passing off and tarnishing the Nasscom's image.

One of the leading cybercrime cases is the Bank NSP case, the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time, the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the bank's

[11] 119 (2005) DLT 596, 2005 (30) PTC 437 Del

computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

CYBERCRIME AS THREAT TO NATIONAL SECURITY

Today every country is linked to the rest of the world through cyberspace. To fight against hackers, criminals is difficult because the number of attacks has grown. A country's system, which supports the country's critical defense and intelligence, should be secure regardless of their place.

Today the internet is a weapon for political, economic, and military espionage. In the past, many cyber-attacks have been witnessed like: "It is said that Chinese hackers targeted Indian Vaccine makers Serum Institute and Bharat Biotech to gain the information regarding the vaccine made against Coronavirus."

Steps taken: The Indian and the US government have come together to address national security issues as the dependency on network information systems has become involved. In the 2001 summit in Washington DC between President George Bush and Prime Minister Atal Bihari Vajpayee the priority talk was about how to enhance security of shared information.

The work for this began in April2002 by establishment of US-India Cyber Security Forum. It was a group who focused on cooperating on policy, procedural and the technical issues faced by both the nations in cyber security. A joint Indo-US Cyber Security Initiative was formed after both governments committed to enhance the cooperation which will focus on building a good cyber security team by exchange of experts, training, sharing information and strengthening the private-public partnership.

RESEARCH QUESTIONS

The research project addresses the following questions pertaining to cybercrime in India-

(i) How do Cybercrimes violate the Human rights of the victim?

(ii) What are the measures undertaken to tackle cybercrimes?

(iii) What are the challenges in countering Cybercrimes in India?

(iv) What can be recommended to deal with the challenges?

OBJECTIVES

The objectives of our research paper are as follows-

- To understand major cybercrimes and how it violates human rights.
- To analyze cybercrimes by categorizing them into- (i) cybercrime against individual, (ii) cybercrime against property, (iii) cybercrime against organization and (iv) other emerging cybercrimes.
- To delve into motives behind these cybercrimes and suggest some solutions to deal with it.

LITERATURE REVIEW

There is no definite definition of cybercrime. Cybercrimes may be deemed as any crime committed using digital media. The United Nations office on drugs and crime, Vienna in its *"Comprehensive study on cybercrime"* (2013) says 'Definitions' of cybercrime mostly depend upon the purpose of using the term. It was also noted that out of almost 200 items of national legislation cited by countries in response to the Study questionnaire, fewer than five percent used the word 'cybercrime' in the title or scope of legislative provisions. This study also gives us the global picture of cybercrimes and related legislations and frameworks.

In our research paper, we analyze diverse types of cybercrimes regarding violations of human rights. Danielle Keats Citron in her book "Hate crimes in Cyberspace" (2014) makes a compelling case for understanding cyber-harassment as a violation of civil rights law. She provides critical insights into history and jurisprudence to explain how social, political, and legal norms must be employed more productively and fairly to create more civil egalitarian online cultures.

Suzanne Ost in her book "Child Pornography and Sexual Grooming" (2009) explores parallels between child pornography and grooming, the way in which the internet has shaped their contemporary forms to contextualize the problems of child pornography and sexual grooming in the contemporary social and legal arena. She also discusses the harms of creating and distributing child pornography and the harms of sexual grooming. Lastly, she also lays down the repercussions of the current societal and legal response to children.

Debarati Halder and K. Jaishankar in their book, "Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations" say that the cyber victimization of women exists, and it is growing in number (Citron, 2009a; Finn & Banach, 2000). Cybercrimes of general nature, such as hacking, phishing, cybersquatting, identity theft, stalking, online bullying, online defamation, etc., target men and women alike. But certain offences, such as email/profile hacking, morphing, spoofing, obscene publication, cyberstalking, cyber pornography, internet voyeurism, cyber defamation, cyberbullying, e-mail harassment, cyber blackmailing/threatening, emotional cheating by impersonation (Whitty, 2005), intimate partner violence through the internet (Jenson, 1996) and abetment of such offences may happen more to women than their male counterparts.

Lech J. Janczewski and Andrew M. Colarik in their book, *"Cyber Warfare and Cyber Terrorism"* (2008) focus on the Dynamic and human aspects of cyber warfare and cyber terrorism, technical aspects of handling cyber-attacks, and its identification, authorization, and control. They also differentiate hacking from cyber-terrorism laying down that the cyber terrorists are different, operating with a specific political or ideological agenda to support their actions.

The act of spying for national security and the concept of infringement of the right to privacy have always been a matter of debate. Gordon Corera in his book *"Intercept: The Secret History of Computers and spies"* (2016) writes that the computer was born to spy. He further says that sometimes a thorny knot of issues is portrayed as simply a case requiring us to 'balance' security with privacy, but the reality is far more complex and multi-layered.

To facilitate better implementation of policies in this regard in India, a global perspective of espionage especially pertaining to the US and effective measures to curb the same have been discussed in this research paper. The Foreign Intelligence Surveillance Act of 1978[12] lays down certain limitations thereby establishing a fine line between infringement and protection of the right to privacy. Interpretation of the right to privacy by the Indian Judiciary has been done in the case of **K.S. Puttaswamy v. Union of India[13].** Anirudh Rastogi in his book, *"Cyber Law – Law of Information Technology and Internet*" (2014) brings the concept of espionage under the purview of cyber terrorism as discussed in Section 66F of the Information Technology Act, 2008.

[12] Section 50 U.S.C. §1801
[13] (2017) 10 SCC 1

RESEARCH METHODOLOGY

For the purpose of the research paper, the statistics and reports published by National Crime Record Bureau (NCRB) and The International Criminal Police Organization (INTERPOL) are analyzed. Moreover, the legal statute, laws, and provisions available for dealing with cybercrimes in India are critically studied so that shortcomings of such provisions can be highlighted to offer recommendations for the same.

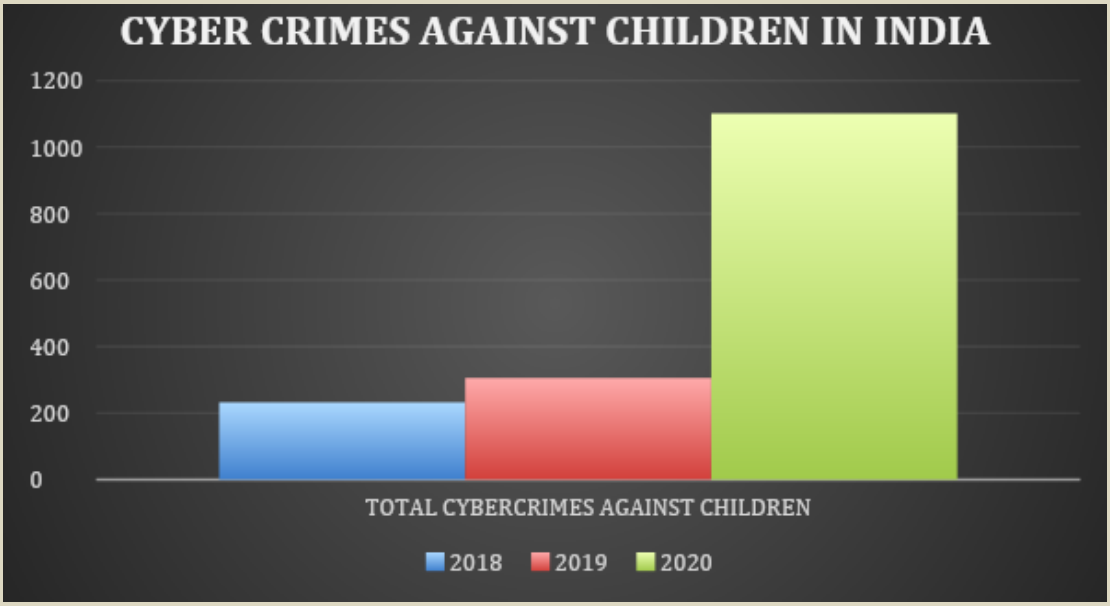
DATA ANALYSIS

Under this Section we have analyzed the data from **National Crime Records Bureau** to provide a systematic analysis of data from 2018-2020 and to observe contemporary trends of different crimes in these three years.

I. **CYBER CRIMES AGAINST INDIVIDUAL**

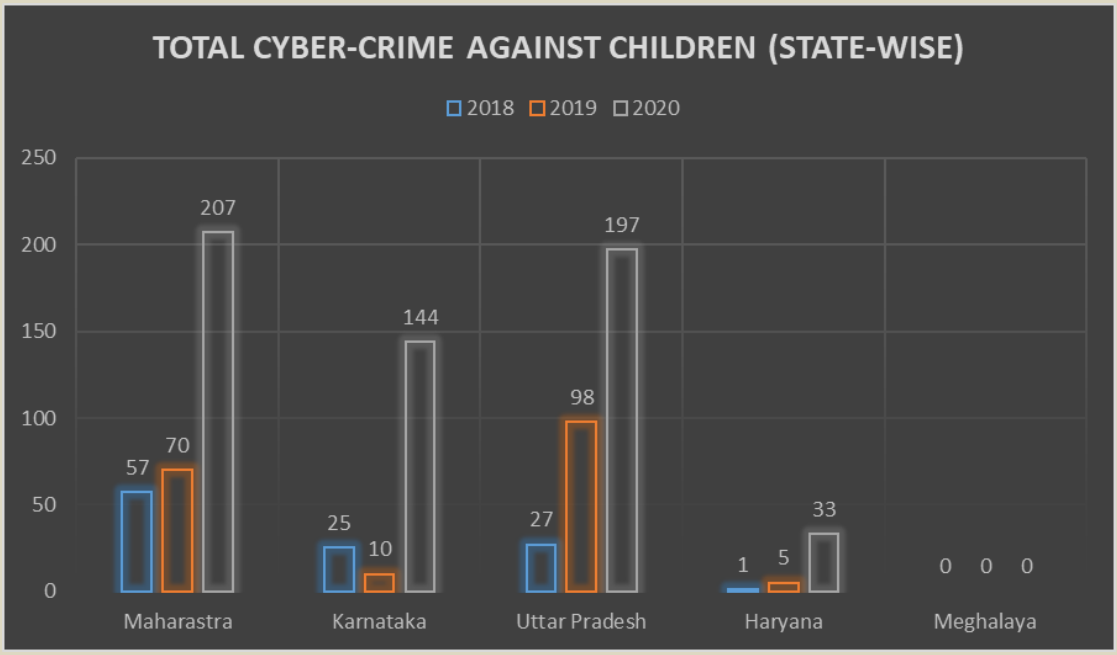
Crimes taken here under the Crimes against individual are Cyber Bullying, Child Pornography, Harassment, Stalking etc. According to the data published by the NCRB the crimes committed against individual has significantly increased from 2018 to 2020. Crimes against Individuals can be further divided based on the victim's profile.

a.) **Cyber Crimes against Children:** While looking below at the Graph (1) data published by NCRB, we see a 375% increase in cyber crimes from 2018 to 2020. Total Crime committed in 2018 against children was 232, while in 2019 the number rise to 305 and the year 2020 showed highest number of cases amounting to 1102.



Graph (1) (indicating 375% increase in cyber crimes from 2018 to 2020)

The reason can be attributed to the pandemic and the majority of the things becoming online. The graph takes an increasing trend.



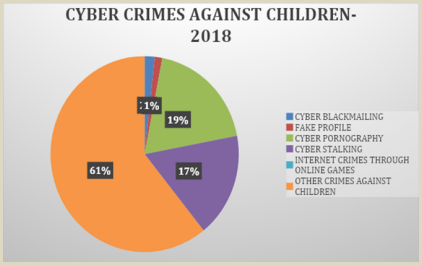
(Bar Graph 1 source **NCRB**)

According to above Bar Graph 1

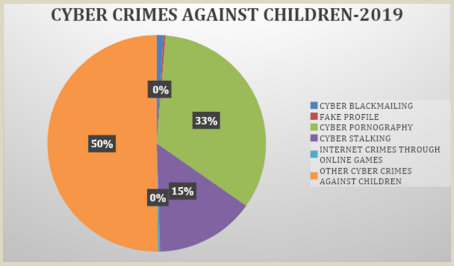
In 2018, Maharashtra recorded the highest number of crimes against children followed by Uttar Pradesh, Karnataka, and the lowest cases was recorded by haryana and meghalaya.

In 2019, Uttar Pradesh recorded the highest number of crimes against children followed by Maharashtra and the lowest cases recorded by the state Meghalaya.

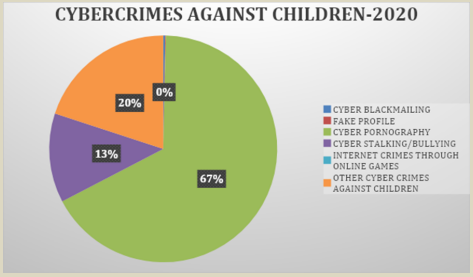
In 2020, Maharashtra recorded the highest number of crimes against children followed by Uttar Pradesh, Karnataka, and the lowest case recorded by the state Meghalaya.



(Fig. 1) (NCRB)



(Fig. 2) (NCRB)



(Fig. 3) (NCRB)

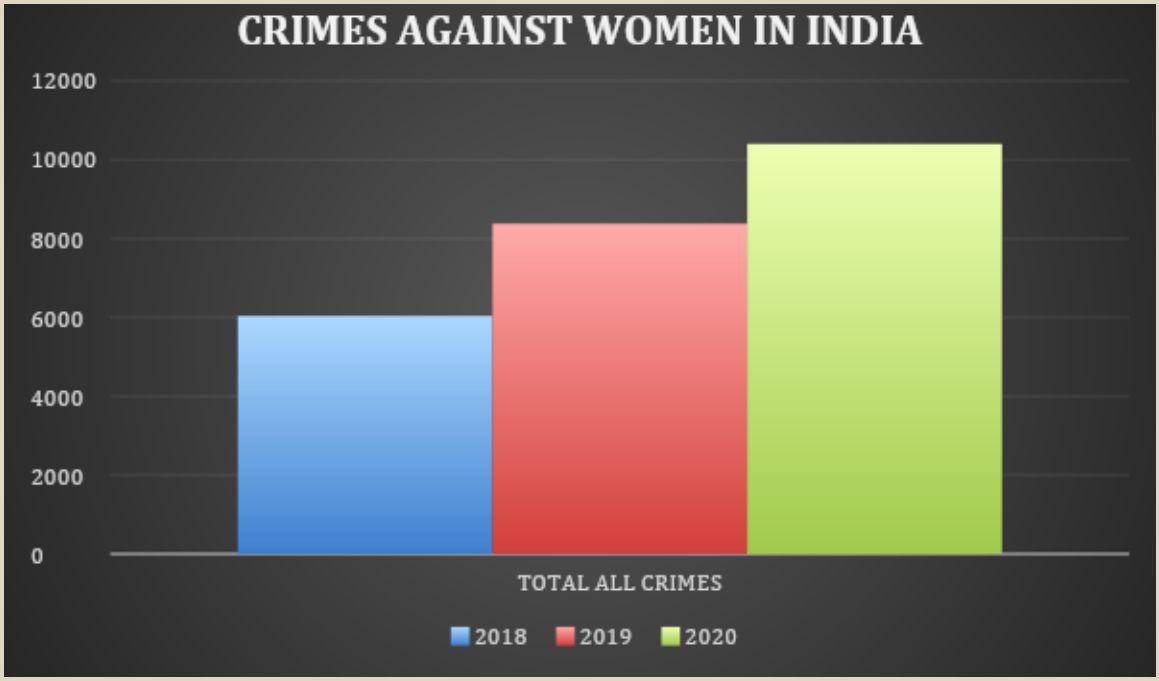
The fig.(1-3) represents the composition of types of cyber crime take place against children in the year 2018, 2019, 2020 respectively.

b.) <u>Cyber Crimes against Women</u>

Crimes against women are a common threat that needs to be tackled strictly. In the cyber state, it includes Cyber sexual exploitation, Cyber Bullying, Fake profiles, Unconsented pornography, etc. According to below Graph (2) Total Crime committed in 2018 against women was 6030,

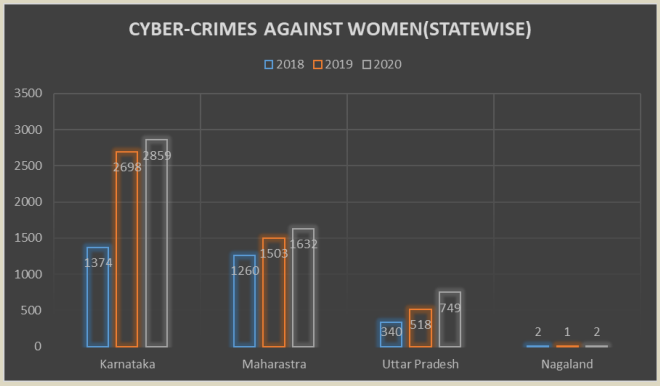
while in 2019 the number rise to 8379 and the year 2020 showed highest number of cases amounting to 10405, crimes committed against women in three consecutive years were-

- **2018-** 6030
- **2019-** 8379
- **2020-** 10405



Graph (2) Source NCRB

The recorded number of cybercrimes against women in India was 6030 in 2018 which increased to 8379 in 2019. This number increased in the same proportion to 10405 in 2020. Figures show that the increase in cybercrimes against women showed a similar trend in the concerned years. The graph takes on an increasing trend.



Graph (3) Source NCRB

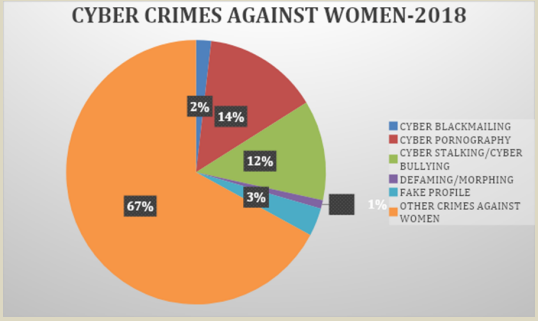
According to the above **Graph (3)**

In 2018, cyber-crimes committed against women were the highest in Karnataka 1374 cases followed by the state of Maharashtra 1260 cases and the lowest crimes reported by the state is Nagaland 2 cases. Although the difference in numbers varies quite much.

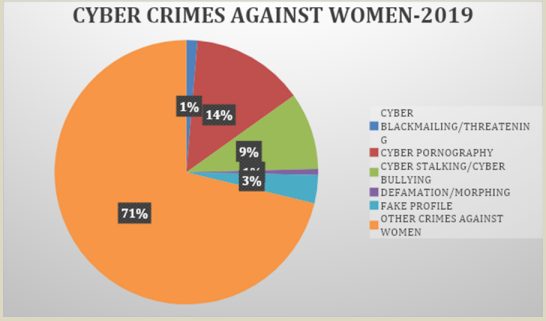
In 2019, cyber-crimes committed against women were the highest in the state of Karnataka 2698 cases followed by the states of Maharashtra 1503 cases, and the lowest crimes reported by the state is Nagaland 1 case. Although the difference in numbers varies quite much.

In 2020, cyber-crimes committed against women were the highest in the state of Karnataka 2859 cases followed by the states of Maharashtra 1632 cases, Nagaland recorded 2 cases and the lowest crimes reported by the state is sikkim 0 case. Although the difference in numbers varies quite much.

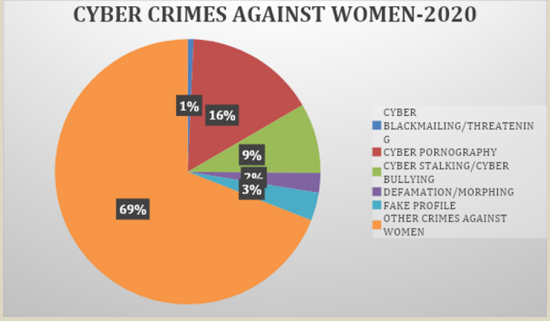
With the expansion of internet and majority of Indians coming online, the incidents of cybercrimes against women and children are also increasing. And **Cyber Grooming** is one of cybercrime against women and children which rapidly increased in last few years.



(Fig. 4) (NCRB)



(Fig. 5) (NCRB)



(Fig. 6) (NCRB)

The fig.(4-6) represents the composition of types of cyber crime take place against women in the year 2018, 2019, 2020 respectively.

b.) <u>Cyber crimes against elderly</u>

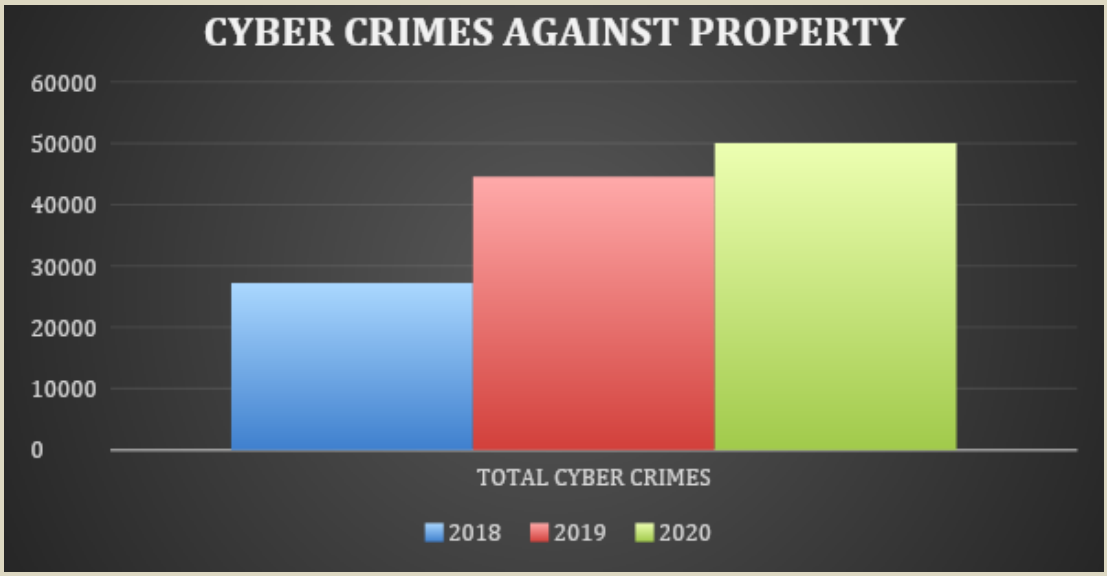
Unlike their younger counterparts, seniors are less aware of cyberthreats and, in many cases, lack the tools and experience to identify attacks and fraudulent attempts. Even elderly people with no access to computers or smartphones can fall victim to cybercrimes such as in the case where their personal details have been leaked from a database and sold to criminals who can then exploit. Identity theft cases comprise 33% of the total number and cheating by virtual impersonation contributes 62% of the total cases. Lack of awareness is one of the biggest reasons for the extent of crime.[14]

---

14 https://www.deccanherald.com/metrolife/cybercriminals-target-seniors-and-new-users-of-technology-1032882.html#:~:text=Elderly%20victims,Centre%20of%20Internet%20and%20Society.

II. **CYBER CRIMES AGAINST PROPERTY**

Crimes taken here under the Crimes against individual are Identity theft, Hacking, Ransomware, etc. According to the data published by the NCRB the crimes committed against individual has a significant increase of 83.6 % from 2018 to 2020.



(Fig.7)- NCRB Data on Cyber-crimes against Property

According to NCRB, the offenses committed under the IT Act in three consecutive years are-

- **2018-** 27,248
- **2019-** 44,546
- **2020-** 50,035

Looking at the data, the offenses doubled (approximately) from 2018 to 2019, while they increased only a little in 2020. Offenses committed in 2020 were almost equal to that of 2019, just a little higher. The graph takes a sharp upward and then a little downward trend. Karnataka and Uttar Pradesh were the top two states where the majority of the offenses were committed.

In 2018, the total cybercrimes committed were the highest for the state of Uttar Pradesh followed by Karnataka, Maharashtra, Assam, and Andhra Pradesh.

In 2019, the total cybercrimes committed were the highest for the state of Karnataka followed by Uttar Pradesh, Maharashtra, and Assam.

In 2019, the total cybercrimes committed were the highest for the state of Uttar Pradesh followed by Karnataka, Maharashtra, Telangana, and Assam.

ATM Skimming

Skimming occurs is a type of payment card fraud when devices illegally installed on ATMs, point-of-sale (POS) terminals, or fuel pumps capture data or record cardholders' PINs. Criminals use the data to create fake debit or credit cards and then steal from victims' accounts. It is estimated that skimming costs financial institutions and consumers more than $1 billion each year.[15]

Skimming devices store data to be downloaded or wirelessly transferred later. Like ATM skimmer devices usually fit over the original card reader. It is inserted in the card reader, placed in the terminal, or situated along exposed cables. Pinhole cameras installed on ATMs record a customer entering their PIN. Pinhole camera placement varies widely. In some cases, keypad overlays are used instead of pinhole cameras to records PINs. Keypad overlays record a customer's keystrokes.

When you slide your card into the card reader, it proceeds to read and store all data embedded on the card. This data is either used (for fraudulent transactions, for example), sold on the dark web, or used to create fake cards.

[15] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/skimming

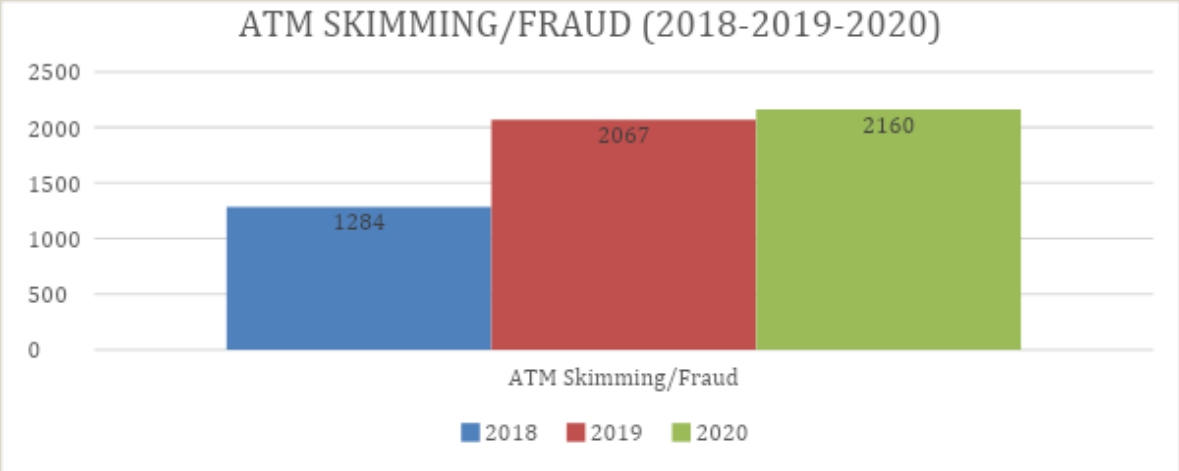


Fig. 8 (NCRB)- The Increasing Cyber-crimes related to ATMs can be easily observed.

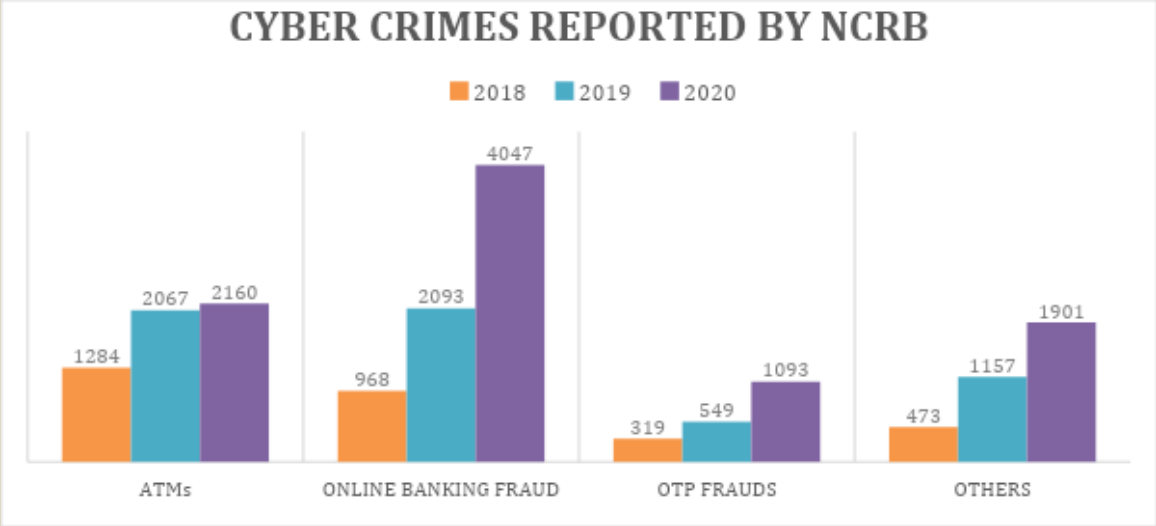


Fig. 9 (NCRB)- Cyber-crimes related to ATMs, Online Banking Fraud, OTPs and others.

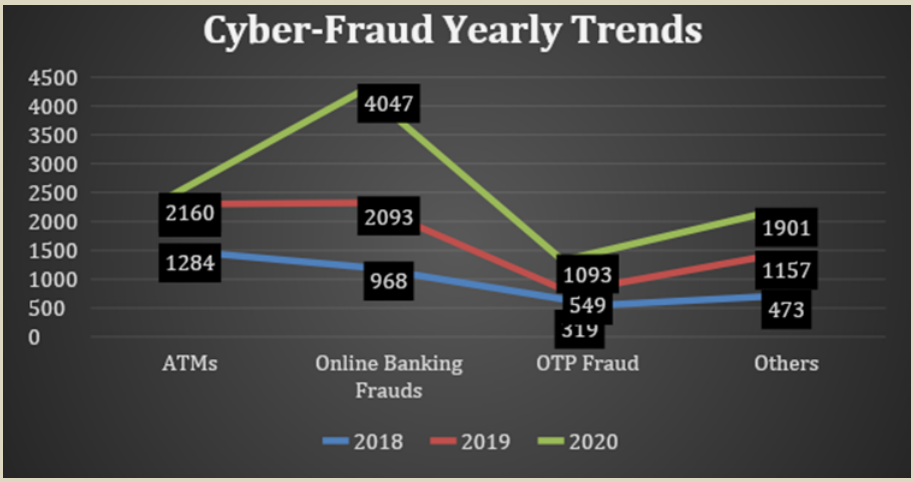
CYBER FRAUD

Cyber-Fraud includes ATMs Fraud, OTP Frauds, Online banking frauds and others.

While looking at the below Graph (3), we see a 200% increase in cyber-Frauds crimes from 2018 to 2020. Total Crime committed in 2018 was 3044, while in 2019 the number rise up to 5866 and the year 2020 showed highest number of cases amounting to 9201.

According to NCRB, total cyber-frauds in

- **2018-** 3044
- **2019-** 5866
- **2020-** 9201



Graph (3) Source NCRB

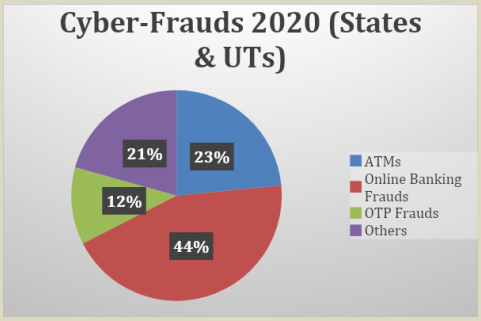


Fig.(10) (NCRB)

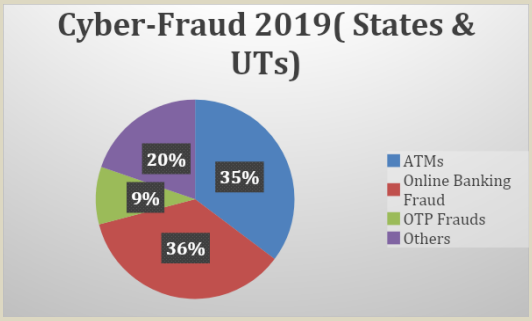


Fig.(11) (NCRB)

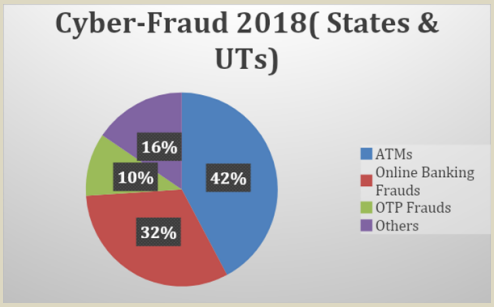
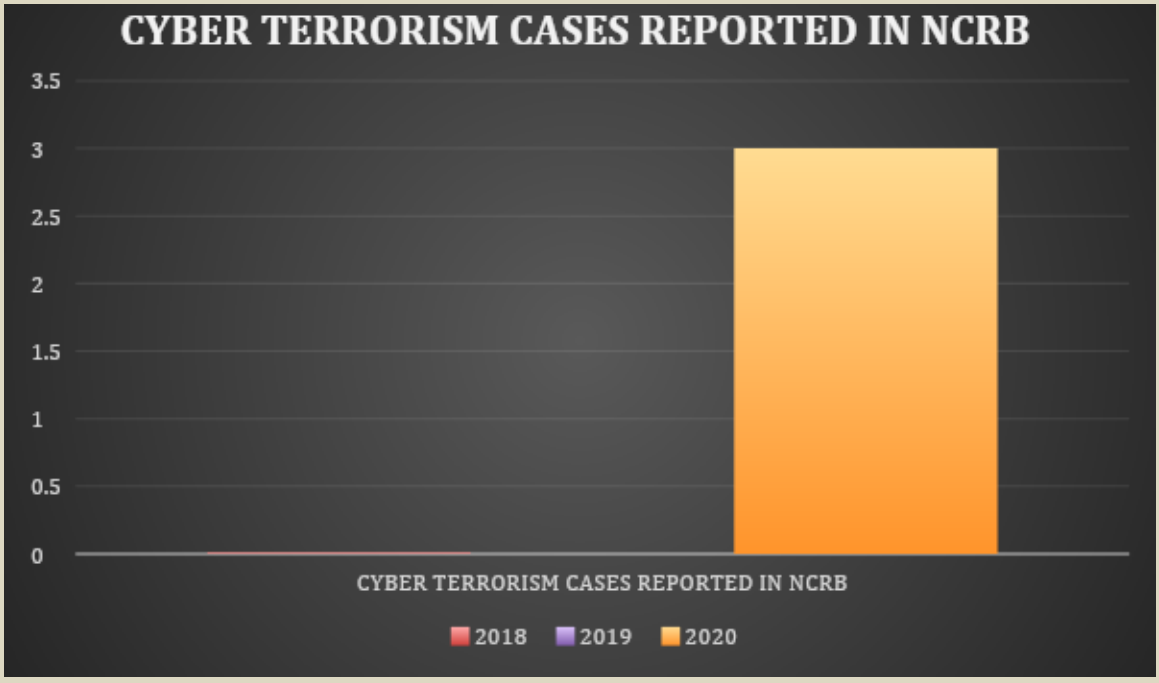


Fig.(12) (NCRB)

The above Fig.(10-12) shows the composition of different Cyber Frauds take place in states & UT

III CYBER CRIMES AGAINST ORGANIZATION/ STATE

The Cybercrimes taken under this section are Cyber Terrorism and Espionage. While looking at below Graph 4. we see that no cases of Cyber Terrorism were reported in 2018 and 2019 however, in 2020 three cases emerged. This shows an increase in Cyber Terrorism.



IV OTHER CYBER CRIMES

Some other important cyber-crimes include, Sulli Deals, Bulli Bai Case and Metaverse Gangrape Case.

Sulli Deals

"*Sulli Deals*" was an open-source app which contained photographs and personal information of some 100 Muslim women online. In July 2021, the app was discovered by Twitter users. The app

had the tagline ‘Sulli deal of the day’ and published photographs of Muslim women without their consent. It encourages users to participate in an ‘auction’ of the women. The case has revealed that around 30 Twitter handles were misused for uploading the morphed pictures of Muslim women for their purported "auction”[16]. On 9 March 2022, the Delhi Police filed a charge sheet, charging the accused persons with offenses including Section 153A (Promoting enmity between groups), Section 153B (causing disharmony), 354A(3) (Sexual harassment), and 509 (insulting the modesty of a woman) of the Indian Penal Code[17].

Bulli Bai Case

The Bulli Bai case is related to an online mock auction of Muslim women. On 4th of July, 2021 several Muslim women pictures were posted on twitter as "deal of the day". Photos of prominent Muslim journalists and activists were uploaded on the Bulli Bai app without their permission where they were auctioned virtually. Like Sulli Deals, the app did not actually sell anyone, but harassed and humiliated these women. The app has been removed from the Internet platform.

GANGRAPE IN METAVERSE

A metaverse in an online world where people exist in shared virtual spaces through what are known as avatars. On its official website, ***Facebook says, “3D spaces in the metaverse will let you socialize, learn, collaborate and play in ways that go beyond what we can imagine***.”

In Feb 2022, a 43-year-old British woman has alleged that she was verbally and sexually harassed in Facebook’s metaverse, Horizon Venues. She said that within 60 seconds of her joining the virtual world, three or four male avatars “virtually gang raped” her avatar and took photos of the same.

---

[16] https://www.indiatoday.in/india/story/creators-bulli-bai-sulli-deals-apps-bail-delhi-court-humanitarian-grounds-1930817-2022-03-29

[17] https://www.thehindu.com/news/national/bulli-bai-app-niraj-bishnoi-a-radicalised-lone-wolf/article38243558.ece

Patel, co-founder, and vice-president of metaverse research Kabuni Ventures, wrote in a post on Medium.com that within 60 seconds of joining Meta's (Facebook) metaverse platform Horizon Venues, London-based **Nina Jane Patel** said a gang of three-four avatars sexually harassed her. "They essentially, but virtually, gang-raped my avatar and took photos as I tried to get away."

The woman is vice president of Metaverse Research for Kabuni Ventures, an immersive technology company. After her initial blog post about the incident, Nina Jane Patel recounts receiving comments calling it "a pathetic cry for attention" and urging her not to pick a female avatar next time.

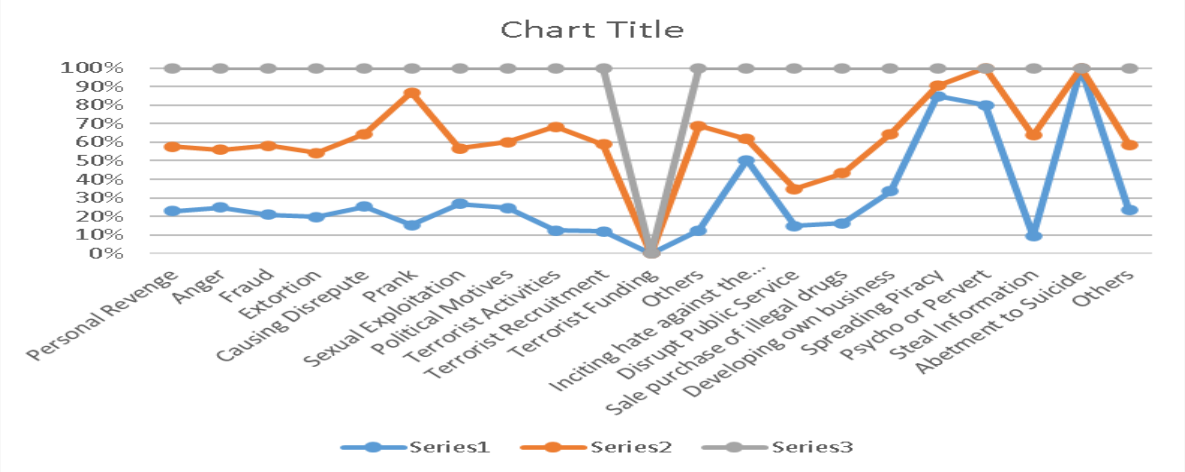
How to Protect Data in Metaverse: The best way to secure and protect your data, always be aware of what information you are sharing, and with whom.

- **CYBERCRIMES AND THEIR MOTIVES**

Total no. of Cyber Crimes with their Motives (States and UT) – 2018, 2019 and 2020

	Series 1	Series 2	Series 3
MOTIVE	**2018**	**2019**	**2020**
Personal Revenge	**794**	**1207**	**1470**
Anger	**461**	**581**	**822**
Fraud	**15051**	**26891**	**30142**
Extortion	**1050**	**1842**	**2440**
Causing Disrepute	**1212**	**1874**	**1706**
Prank	**296**	**1385**	**254**
Sexual Exploitation	**2030**	**2266**	**3293**
Political Motives	**218**	**316**	**356**
Terrorist Activities	**44**	**199**	**113**
Terrorist Recruitment	**2**	**8**	**7**
Terrorist Funding	**0**	**0**	**0**

Others	**42**	**191**	**106**
Inciting hate against the country	**218**	**49**	**165**
Disrupt Public Service	**21**	**28**	**92**
Sale purchase of illegal drugs	**6**	**10**	**21**
Developing own business	**198**	**181**	**210**
Spreading Piracy	**671**	**45**	**75**
Psycho or Pervert	**4**	**1**	**0**
Steal Information	**16**	**93**	**62**
Abetment to Suicide	**2**	**0**	**0**
Others	**4956**	**7578**	**8814**
TOTAL NO. OF CASES	**27248**	**44546**	**50035**



Graph 5 (NCRB-2018 as Series 1, 2019 as Series 2 & 2020 as Series 3)

The above Graph 5 represents the motives of crime (in %) in cyber crime in the year 2018, 2019, 2020, respectively.

As from the above graph and table, we can clearly observe that the among all the motives of cyber-crime, Fraud is one of the most leading one in 2018, 2019, 2020 as well. In 2018, 15051 cases of cyber-crimes with fraud was recorded, while in 2019 the figure increased to 26891 and in 2020, it was recorded as 30142. Among all the cyber-motives, terrorist funding is the least one with 0 count in the years 2018, 2019, 2020 respectively.

CYBER LAWS IN INDIA

The following Act, Rules and Regulations are covered under cyber laws:

1. The Information Technology Act of India, 2000
2. Indian Penal Code, 1860
3. Indian Evidence Act, 1872
4. Protection of Children from Sexual Offences Act, 2012 (POCSO)
5. National Policy on Information Technology, 2012

I. THE INFORMATION TECHNOLOGY ACT OF INDIA, 2000

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. It is the most important law in India that deals with the digital crimes or cybercrimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

Following are the sections under IT Act, 2000:

1. Trying to tamper with computer resources- **Section 65**
2. Trying to hack into the data stored in the computer – **Section 66**
3. Provision of penalties for misappropriation of information stolen from computer or any other electronic gadget – **Section 66B**
4. Provision of penalties for stealing someone's identity-**Section 66C**
5. Provision of penalties for access to personal data of someone with the help of computer by concealing their identity- **Section 66D**
6. Provision of penalties for breach of privacy- **Section 66E**
7. Provision of penalties for cyber terrorism- **Section 66F**

8. Provisions related to the publication of offensive information-**Section 67**

9. Provision of penalties for publishing or circulating sex or pornographic information through electronic means- **Section 67A**

10. Publication or broadcast of such objectionable material from electronic means, in which children are shown in obscene mode – **Section 67B**

11. Provision of penalties for disrupting or blocking information by mediators- **Section 67C**

12. Provision for making objectionable access to a secured computer-**Section 70**

13. Delivering data or data incorrectly – **Section 71**

14. Provisions related to mutual trust and privacy – **Section 72**

15. The provisions relating to making public the information violation of the terms of the Protocol-**Section 72**

16. Publication of Ezra Digital Signature-**Section 73**

Rules notified under the Information Technology Act, 2000:

a) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
b) The Information Technology (Electronic Service Delivery) Rules, 2011
c) The Information Technology (Electronic Service Delivery) Rules, 2011
d) The Information Technology (Intermediaries guidelines) Rules, 2011
e) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011
f) The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009
g) The Cyber Appellate Tribunal (Procedure for investigation of Misbehavior or Incapacity of Chairperson and Members) Rules, 2009
h) The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public), 2009
i) The Information Technology (Procedure and Safeguards for interception, monitoring, and decryption of information) Rules, 2009
j) The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

k) The Information Technology (Use of electronic records and digital signatures) Rules, 2004
l) The Information Technology (Security Procedure) Rules, 2004
m) The Information Technology (Other Standards) Rules, 2003
n) The Information Technology (Certifying Authority) Regulations, 2001
o) Information Technology (Certifying Authorities) Rules, 2000

II. INDIAN PENAL CODE, 1860

1. **Section 292:** Although this Section was drafted to deal with the sale of obscene material, it has evolved in the current digital era to be concerned with various cybercrimes. The publication and transmission of obscene material or sexually explicit act or exploit acts containing children, etc., which are in electronic form are also governed by this section. Though the crimes mentioned above seem to be alike, they are recognized as different crimes by the IT Act and IPC. The punishment imposed upon the commission of such acts is imprisonment and fine up to 2 years and Rs. 2000. If any of the crimes are committed for the second time, the imprisonment could be up to 5 years and the fine could be imposed up to Rs. 5000.

2. **Section 354 C:** The cybercrime dealt with under this provision is capturing or publication of a picture of private parts or acts of a woman without such person's consent. This section exclusively deals with the crime of 'voyeurism' which also recognizes watching such acts of a woman as a crime. If the essentials of this Section (such as gender) are not satisfied, Section 292 of IPC and Section 66E of IT Act,2000 is broad enough to take the offenses of a similar kind into consideration. The punishment includes 1 to 3 years of imprisonment for first-time offenders and 3 to 7 years for second-time offenders.

3. **Section 354D:** This section describes and punishes 'stalking' including both physical and cyberstalking. If the woman is being monitored through electronic communication, internet, or email or is being bothered by a person to interact or contact despite her

disinterest, it amounts to cyber-stalking. The latter part of the Section states the punishment for this offense as imprisonment extending up to 3 years for the first time and 5 years for the second time along with a fine imposed in both the instances.

4. **Section 379:** If a mobile phone, the data from that mobile or the computer hardware is stolen, Section 379 comes into the picture and the punishment for such crime can go up to 3 years of imprisonment or fine or both. But the attention must be given to the fact that these provisions cannot be applied in case the special law i.e., IT Act, 2000 provisions are attracted.

5. **Section 411:** This deals with a crime that follows the offenses committed and punished under Section 379. If anyone receives a stolen mobile phone, computer, or data from the same, they will be punished in accordance with Section 411 of IPC. It is not necessary that the thief must possess the material. Even if it is held by a third party knowing it to be others, this provision will be attracted. The punishment can be imposed in the form of imprisonment which can be extended up to 3 years or fine or both.

6. **Section 419 and 420:** These are related provisions as they deal with frauds. The crimes of password theft for the purpose of meeting fraudulent objectives or the creation of bogus websites and commission of cyber frauds are certain crimes that are extensively dealt with by these two sections of IPC. On the other hand, email phishing by assuming someone's identity demanding password is exclusively concerned with Section 419 of IPC. The punishments under these provisions are different based upon the gravity of the committed cybercrime. Section 419 carries a punishment up to 3 years of imprisonment or fine and Section 420 carries up to 7 years of imprisonment or fine.

7. **Section 465:** In the usual scenario, the punishment for forgery is dealt with in this provision. In cyberspace, the offenses like email spoofing and preparation of false documents are dealt with and punished under this Section which imbibes the imprisonment reaching up to 2 years or fine or both.

8. **Section 468:** If the offenses of email spoofing or the online forgery are committed for the purpose of committing other serious offenses i.e., cheating, Section 468 comes into the picture which contains the punishment of seven years of imprisonment or fine or both.

9. **Section 469:** If the forgery is committed by anyone solely for the purpose of disrupting a particular person or knowing that such forgery harms the reputation of a person, either in the form of a physical document or through online, electronic forms, he/she can be imposed with the imprisonment up to three years as well as fine.

10. **Section 500:** This provision penalizes the defamation of any person. With respect to cybercrimes, sending any modes of defamatory content or abusive messages through email will be attracted by Section 500 of IPC. The imprisonment carried with this Section extends up to 2 years along with fine.

11. **Section 504:** If anyone threatens, insults, or tries to provoke another person with the intention of effecting peace through email or any other electronic form, it amounts to an offense under Section 504 of IPC. The punishment for this offense extends up to 2 years of imprisonment or fine or both.

12. **Section 506:** If a person tries to criminally intimidate another person either physically or through electronic means with respect to the life of a person, property destruction through fire or chastity of a woman, it will amount to an offense under Section 506 of IPC and punishment of imprisonment where the maximum period is extended up to seven years or fine or both.

13. **Section 509:** This Section deals with the offense of uttering a word, showing a gesture, and committing an act that has the potential to harm the modesty of a woman. It also includes the sounds made and the acts committed infringing the privacy of a woman. If this offense is committed either physically or through electronic modes, Section 509 gets attracted and the punishment would be imprisonment of a maximum period of one year or fine or both.

III. INDIAN EVIDENCE ACT, 1872

Amendments related to the evidence Act were contained in Sec.92 and the Second Schedule of the IT Act, 2000. Pursuant to the enactment of the Information Technology (amendment) Act, 2008, Sec.92 was deleted and the provisions regarding the Indian Evidence Act were mentioned in Part IV of the amendment Act.

1)Amendment of Sec.3 –In section 3 relating to interpretation clause, in the paragraph appearing at the end, for the words "digital signature" and "Digital Signature Certificate", the words "Electronic signature" and "Electronic Signature Certificate" shall be respectively substituted.

2) Insertion of new Sec.45A – Opinion of Examiner of Electronic evidence –

45A: When in a proceeding, the Court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000, is a relevant fact. Explanation: For the purposes of this section, an Examiner of Electronic Evidence shall be an expert

3) Amendment of Sec.47A –In section 47A, - (i) for the words "digital signature", the words "electronic signature" shall be substituted; (ii) for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted.

4) Amendment of Sec.67A –In section 67 A, - for the words "digital signature", the words "electronic signature" shall be substituted.

5) Amendment of Sec.85A –In section 85A, for the words "digital signature", wherever they occur, the words "electronic signature" shall be substituted.

6) Amendment of Sec.85B –In section 85B, - for the words "digital signature", wherever they occur, the words "electronic signature" shall be substituted.

7) Amendment of Sec.85C –In section 85C, for the words "Digital Signature Certificate", the words "Electronic Signature Certificate" shall be substituted.

8) Amendment of Sec.90A –In section 90A, the words "digital signature", at both places where they occur, the words "electronic signature" shall be substituted.

IV. NATIONAL POLICY ON INFORMATION TECHNOLOGY, 2012

The Union Cabinet has recently in September 2012, approved the National Policy on Information Technology 2012. The Policy aims to leverage Information & Communication Technology (ICT) to address the country's economic and developmental challenges.

The vision of the Policy is "To strengthen and enhance India's position as the Global IT hub and to use IT and cyber space as an engine for rapid, inclusive and substantial growth in the national economy." The Policy envisages among other objectives, to increase revenues of IT and ITES Industry from 100 billion USD at present to 300 billion USD by 2020 and expand exports from 69 billion USD at present to 200 billion USD by 2020. It also aims to create a pool of 10 million additional skilled workforce in ICT.

The thrust areas of the policy include:

1. To increase revenues of IT and ITES (Information Technology Enabled Services) Industry from 100 billion USD currently to 300 billion USD by 2020 and expand exports from 69 billion USD currently to 200 billion USD by 2020.

2. To gain significant global market-share in emerging technologies and Services.

3. To promote innovation and R&D in innovative technologies and development of applications and solutions in areas like localization, location-based services, mobile value-added services, Cloud Computing, social media, and Utility models.

4. To encourage adoption of ICTs in key economic and strategic sectors to improve their competitiveness and productivity.

5. To provide fiscal benefits to SMEs and Start-ups for adoption of IT in value creation

6. To create a pool of 10 million additional skilled workforce in ICT. 7. To make at least one individual in every household e-literate.

8. To provide for mandatory delivery of and affordable access to all public services in electronic mode.

9. To enhance transparency, accountability, efficiency, reliability, and decentralization in Government and in particular, in delivery of public services.

10. To leverage ICT for key Social Sector initiatives like Education, Health, Rural Development and Financial Services to promote equity and quality.

11. To make India the global hub for development of language technologies, to encourage and facilitate development of content accessible in all Indian languages and thereby help bridge the digital divide.

12. To enable access of content and ICT applications by differently abled people to foster inclusive development.

13. To leverage ICT for expanding the workforce and enabling life-long learning.

14. To strengthen the Regulatory and Security Framework for ensuring a Secure and legally compliant Cyberspace ecosystem.

15. To adopt Open standards, promote open source, and open technologies The Policy has however not yet been notified in the Official Gazette.

V. PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT, 2012 (POSCO)

In addition, the POCSO Act was enacted in year 2012 to provide legal protection against sexual assault, sexual harassment, and child pornography. POCSO is a key legislation governing sexual harassment of children and their protection thereof. Under the provisions of the Act, sexual assault, harassment, and pornography - where the victim of the same are children, are made punishable offences as is the abetment of any of the offences mentioned under the Act.

1. Under **Section 11** of the POCSO Act, a person is said to commit sexual harassment upon a child when such person:

- 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 and does so with sexual intent or
- makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or
- shows any object to a child in any form or media for pornographic purposes; or
- repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or
- threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or
- entices a child for pornographic purposes or gives gratification. 'Sexual intent' in such circumstances, is to be determined on the facts of the case

2. **Section 12** further provides for punishment for the said offences and the acts are punishable for imprisonment for a term which may extend to three years with a fine.
3. **Section 13**: The use of a child or the involvement of a child through any medium like print, electronic, computer or any other technology for preparation, production, offering, transmitting, publishing, facilitation, and distribution of the pornographic material, irrespective of it being for personal use or distribution, when done with the purpose of sexual gratification amounts to use of the Child for pornographic purposes under Section 13 of the Act. Sexual gratification under this provision includes:

- representation of the sexual organs of a child.
- usage of a child engaged in real or simulated sexual acts (with or without penetration).
- the indecent or obscene representation of a child, shall be guilty of the offence of using a child for pornographic purposes.

4. Under **Section 15**, the storage of pornographic material involving child for commercial purposes in any form is also punishable with imprisonment which may extend to three years or with fine or with both.
5. Under **Section 20**, The POCSO Act further imposes an obligation on personnel of the media or hotel or lodge or hospital or club or studio or photographic facilities, irrespective of the number of persons employed to provide to the Special Juvenile Police Unit, or to the local police on coming across any material or object which is sexually exploitative of the child including pornographic, sexually-related or making obscene representation of a child or children) through the use of any medium.
6. Under **Section 19**, the Act also enumerates the procedure for reporting cases of child sexual harassment to the Special Juvenile Police Unit or the local police and states that the complaint is to be recorded in simple language to enable the child to understand the contents of the complaint.

CHALLENGES IN HANDLING CYBER CRIME

Cyber Crime is a crime committed through online mode. Thus, to prevent these such offensive crimes implementation of effective cyber laws is important. However, implementation of these laws is an arduous process. Some people are still not aware of the extent of cybercrimes. The number of the incidents is increasing day by day and the periphery of cybercrime is also increasing rapidly. Effective measures need to be taken for the prevention of such crimes. The various challenges which involve in handling of cybercrimes are:

1. Lack of efficient, proper & specific legislation to prevent Cyber-attacks.

2. The speed of cyber technology changes always beats the progress of the government. sector so that they are not able to identify the origin of these cyber-crimes. (Problems in deciding Jurisdiction).

3. Present protocols are not self-sufficient, which identifies the investigative responsibility for crimes that stretch internationally.

4. Lack of awareness and the culture of cyber security, at individual as well as organizational level. The lack of awareness among the people is the major reason for the ineffectiveness of the act.

5. Lack of trained and qualified manpower to implement the counter measures.

6. Cyber-attacks have come not only from terrorists but also from neighbouring countries contrary to our National interests.

7. Promotion of Research & Development in ICTs (Information and Communication Technology) is not up to the mark.

8. Security forces and Law enforcement personnel are not equipped to address high-tech crimes.

9. Budgets for security purposes by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compared to other crimes and proper utilization of that Budget fund.

10. Certain laws and statutes have not mentioned various offenses like cyber stalking, cyber harassment, cyber defamation which are on rise recently. The definitions of crimes are not clear, different laws have different definitions of the same crime which can be misleading in many cases.

11. Diverse nature of devices used in cyber space are owned by various people of India. Out of these devices, only a few provide high security and the others are more vulnerable to cyber-crimes.

EFFORTS OF GOVERNMENT

Apart from engaging our minds to the problems, we should also focus on the remedies and measures that should be adopted in order to curb or minimize the offense of Cyber-Crime. The Data of NCRB (National Crime Records Bureau) clearly shows that there is a significant rise in Cyber-crime cases. Some of the Steps taken by the government to reduce the Cyber-crime cases that should be praised are as follows:

1. On 11 Dec 2019, the Ministry of Electronics, and Information Technology (MEITY) introduced the draft Personal Data Protection Bill, 2019 before the parliament. Which was referred to a joint parliamentary Committee for further consideration. After carrying out a series of consultations with stakeholders, on 16 Dec 2021, the JPC published its report along with the finalized Data Protection Bill, 2021.

2. Since June 2020, the government has banned a total of around 224 apps, which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order. The Ministry of Electronics and Information Technology, Government of India invoking its power under section 69A of the Information Technology Act read with the relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009. The Indian Cyber Crime Coordination Centre, Ministry of Home Affairs has also sent an exhaustive recommendation for blocking these malicious apps. Likewise, there have been similar bipartisan concerns, flagged by various public representatives, both outside and inside the Parliament of India. There has been a strong chorus in the public space to take strict action against Apps that harm India's sovereignty as well as the privacy of our citizens.

3. Seeking to make comprehensive changes in criminal laws to provide affordable and speedy justice and create a people-centric legal structure, the Government has initiated the process to amend the Indian Penal Code, the Code of Criminal Procedure and the Indian Evidence Act in consultation with stakeholders, the Rajya Sabha was

informed on April 7, 2022. The Ministry of Home Affairs (MHA) has also sought suggestions from Governors, Chief Ministers, Lt. Governors and administrators of Union Territories, Chief Justice of India, Chief Justices of various High Courts, Bar Council of India, bar council of various States and members of Parliament regarding comprehensive amendments in criminal laws, Law Minister Kiren Rijiju said in a written reply. We can aspect from the govt. to strict the laws related to cyber-crimes and also, if necessary, insert certain strict provisions in order to minimize the cyber-crime.

4. CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

    a) Collection, analysis, and dissemination of information on cyber incidents.
    b) Forecast and alerts of cyber security incidents
    c) Emergency measures for handling cyber security incidents.
    d) Coordination of cyber incident response activities.
    e) Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response, and reporting of cyber incidents.
    f) Such other functions relating to cyber security as may be prescribed.

5. Initiative like Cyber Surakshit Bharat by Ministry of Electronics and Information Technology, NCIIPC (National Critical Information Infrastructure Protection Centre), Website Audit, crisis management plan by all the government departments, Malware Protection & Cyber Swachhta Kendra, etc.

6. There is also the Indian Cyber Crime Coordination Centre which is a government initiative to deal with cybercrime in India, in a coordinated and effective manner. It is

affiliated to the Ministry of Home Affairs, Government of India. The Indian Cyber Crime Coordination Centre has 7 components which are-

-National Cyber Crime Threat Analytics Unit (TAU)

-National Cyber Crime Reporting Portal

-National Cyber Crime Training Centre

-Cyber Crime Ecosystem Management Unit

-National Cyber Crime Research and Innovation Centre

-National Cyber Crime Forensic Laboratory (NCFL) Ecosystem

-Platform for Joint Cyber Crime Investigation Team

7. There is a framework like NATGRID or the National Intelligence Grid which is a part of the radical revamp of the intelligence and security framework of India and was proposed to be established in the aftermath of the 26/11 Mumbai attack in 2008 which had exposed vulnerabilities in Indian Intelligence gathering and action networks. NATGRID will integrate 21 categories of data from agencies like:
    - Banks,
    - Railways and airlines,
    - Income tax department,
    - Credit card companies,
    - Visa and immigration etc.

This combined data will be made available to 11 central agencies including the R&AW, the National Investigation Agency (NIA), the CBI, the Directorate of Revenue Intelligence, the Intelligence Bureau (IB), the Narcotics Control Bureau (NCB) and the Enforcement Directorate (ED) to help them prevent terrorist attacks and criminal activities.

Although there are some legislations, initiative, and Policies, but the NCRB data clearly shows that the cyber-crime reports are nowhere decreasing. Conflicting to it, there is 11% rise in cyber-crime cases in 2020 in respect to 2019. It indicates that the policies and regulations are just like tiger on paper and fails to implement on ground realities.

RECOMMENDATIONS

I. CYBERCRIME AGAINST INDIVIDUALS:

- Cybercrimes involving children like child pornography, cyberbullying, cyber grooming etc. counselling of not only the children but also their parents are essential. This can help parents understand what their child is going through and support them better.
- Updating the software of the devices on a regular basis to avoid cyber fraud.
- Restricting access to devices by setting up PINs and strong passwords to protect them from the hands of children.
- Initiating cyber awareness programs for children in educational institutes in order to prevent them from being the victims of crimes like child pornography since they would be aware and alert.
- Monitor their internet activity, but as a friend - If you put too many restrictions on your children, their curiosity will drive them to that activity. You cannot tell them not to use social media as it's harmful at a young age. Instead, let them use it but ask them to have you added as a friend. This way, you can see whom all are interacting with them and how they are using the medium.
- Avoid clicking spam emails or untrusted websites.
- Implementation of Data Protection Bill, 2021 - As the JPC published its report along with the finalized Data Protection Bill, 2021, the govt. shall pass the bill from the parliament with the suitable amendments and also including the provisions for e-frauds.
- Adding psychological counselling as a part of the school curriculum for both students and their parents so that they can open up to each other and parents can understand and advise their children which in turn will decrease their chances of committing crimes in cyberspace.
- Formation of 4 Tier Cyber Cell Mechanism - As in India, still many districts are not having cyber cells. Govt. of India and different states should work in coordination and should develop 3 tier Cyber cell mechanism i.e., National level, State level, Zonal level, and district level. It will help in registering the complaint and even in the quick disposal of the cases.

- Universal Enforcement Jurisdiction- The extradition of child pornographers should become specifically less stringent and be followed with a vigorous approach. The foreign countries should cooperate by taking whatever measures could be taken.
- Increased patrolling on the internet - The investigation ambit to grow there must be a mechanism more skilful than the perpetrators to follow them up. Keeping in mind the privacy aspect there has to be a sophisticated and effective manner to increase the oversight of the internet.
- Avoid Disclosing Sensitive Information - Surprisingly, many people constantly share personal information about themselves, even outside of social media platforms. By filling out questionnaires or submitting applications for coupons, you are increasing the likelihood of someone getting their hand on your personal data and possibly making cyberstalking more accessible.
- Conducting surveys on general awareness about cybercrimes and their types and in response organizing awareness camps for sections of the society like elders, women and children who have very little knowledge of cyberspace and the crimes committed in it.
- Avoid disclosing personal and sensitive information on every site to stay safe from cyberstalking, cyberbullying, and cyber sexual harassment.
- Reporting and blocking anything suspicious and potentially harmful in cyberspace immediately.
- Children sometimes start feeling an emotional bond with strangers on social media and become victims of cyber grooming at their hands. To prevent this from happening, parents should monitor their children and keep a track of their activities on social media platforms.
- Like in the Noida cases where a married women's pictures were being circulated across 4 crore WhatsApp Nos. & all those belong to prostitute groups. So, in order to such incident doesn't happen with anyone in future, the social media especially WhatsApp, Instagram, Twitter, FB etc. should design a privacy policy and transmission of the same without the content along with penalties.
- Nowadays, Cyber grooming, cyber morphing and revenge porn are one of the emerging crimes which shown visible rise in these crimes in India and across the world in 2020 and 2021. So, GOI along with cyber expert to have cutting edge tools and upgrading the skills

of cyber dept. experts and digital forensic labs., so that we can detect the criminal and solve the case as soon as possible. And also, there is need for legal framework for these crimes.

II. **CYBER CRIMES AGAINST PROPERTY:**

- Installation of anti-spy and firewall settings in the devices to protect themselves from cybercrimes like Phishing, Identity Theft, and hacking.
- UPGRADING KYC norms

Cybersquatting:

- Register domain names before someone else does which is referred to as "Premium Domain Name Registration".
- Keep an eye on domain names containing misspellings or variations of brand name, as well as.com/.org/net versions.
- Contact those who have registered similar names to yours, especially if they contain common misspellings or typos of your mark.
- Purchase your domain name directly from a registrar, which will ensure you are the true owner of it and give you more control over its use.
- Contact the current domain owner if they violate the Anti - cybersquatting Consumer Protection Act or any other rights that may be protected by IP laws.
- Purchase domain ownership protection insurance from a third party to make sure you are covered against cyber squatters.
- Be the owner of the record for your domain name.

Measures to curb Cyber Vandalism:

- Don't access personal or financial data with public Wi-Fi
- Use a password, lock code or encryption
- Encrypt your hard drive
- Be sceptical about links and attachments.

III. **CYBER CRIME AGAINST THE STATE:**

- Identify the techniques used in cyber espionage attacks. This can give an organization a good baseline in what to protect.
- Monitor systems for unexpected behaviours. The use of security monitoring tools can help pick up on or prevent any suspicious activity from occurring.
- Enact data policies, including who has access to what information. This will help ensure only those who need access to critical information can gain access.
- Make sure there are no vulnerabilities in a system and that any used third-party software systems are secured and well protected against cyberattacks.
- Create a cybersecurity policy that addresses security procedures and risks.
- Establish an incident response if an attack is detected, an organization should be able to quickly respond to minimize damage.
- Educate employees about security policies, including how to avoid opening suspicious-looking emails with links or document attachments.
- Ensure passwords are changed periodically.
- Monitor what data can be stored on individual mobile devices for organizations that make use of bringing your own device (BYOD).

TECHNICAL PREVENTIVE MEASURES AND RECOMMENDATIONS TO OPPOSE CYBERCRIME

- **Use of Authentication Technologies**: The difficulty of gaining unwanted access to information systems is considerably increased when password biometric devices, fingerprint or voice recognition technologies, and retinal imaging are used. Biometric technology deserves special attention because it recognizes a certain user's authentication for using a specific computer.

- **Development of new Technologies:** Development of encryption and anonymity technology, and also infrastructure protection, because hackers or cyber terrorists can attack any nation's infrastructure, causing significant damages. Powerful firewalls can

stop by disrupting the foreign invasion of hackers in the country by creating data that is hard to decipher. Personal use of anti-viruses that offer internet security of sites and cookies and VPNs which decrease the extent and impact of damage in case of any cyberattack.

- **Data Recovery**: At the time of any cyberattack or invasion make sure that your data is secure through cloud computing services from authorized software. One can also back up the data/software to USBs or hard drives for minimizing the damage or loss to your personal files and data.

- **Monitoring controls of Money:**

Monitoring controls of the financial transactions and recording the data of monetary transactions or business information is important. Avoid using sites that are not authorized or safe for the transaction and ask for personal and bank details.

- **Use Blocking and Filtering Programs:**

viruses can detect and stop dangerous computer code; they are useful for virus detection. Anti-spyware software assists in preventing criminals from gaining access to one's computer and in cleaning it up if it has been infected.

CONCLUSION

"Security used to be an inconvenience sometimes, but now it’s a necessity all the time"

~Martina Navratilova

The research paper undertaken intends to study different types of cybercrimes and the motives attached to them in detail to provide quality recommendations to overcome the challenges. It also lays down certain preventive measures to avoid crimes in cyberspace. Emphasis has been laid on the division of power and the existence of cooperation between different wings to ensure desirable results. Other recommendations include but are not restricted to the organization of awareness camps for people of society who lack basic technological knowledge, installation of strong software systems with firewall protections and encryption mechanisms by the organizations and regular monitoring of children’s activities by parents. Adopting these measures will provide an upper hand to not only the individuals but also the government to sanitise the cyber space and prevent misuse of the same.

Cybercrime is a social problem as well as a legal one. To successfully fight it, we must engage people in the IT community and those in the general population who are affected, directly or indirectly, by the criminal activity that is being done via cyberspace. Some Measures To Tackle Cybercrime are needed for Massive Cybersecurity Awareness Campaign like there is a Need for Data Protection Law as In the 21st century, Data is referred to as the new currency. Thus, there is a requirement for a stringent data protection regime.The Collaborative Trigger Mechanism is also a need of the time for developing countries like India where the citizenry is more vulnerable to cybercrime, there is an urgent need for a collaborative trigger mechanism.

As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture.

Bibliography

1. Akhalill Zanab and Hewage Chaminda Nawaf Liqaa, frontier In Computer Science, 2021(https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full#F5)
2. Basuroy Tanushree, published 15 March 2022, Statista https://www.statista.com/statistics/1098571/india-incidents-of-fake-news-propagation-by-leading-state/
3. Basuroy Tanushree, Statista published 15 March 2022 https://www.statista.com/statistics/309435/india-cyber-crime-it-act
4. By HT correspondent, Hindustan Times Lakhnow, published 9 August 2020 https://www.thehindubusinessline.com/info-tech/social-media/hate-speech-one-of-the-top-risks-for-indias-online-users-microsoft-report/article33800069.ece
5. By Kevin Rectorstaff May21 2020, The Loss Angles Times, https://www.latimes.com/california/story/2020-05-21/child-sex-abuse-and-exploitation-surge-online-amid-pandemic-overwhelming-police)
6. By Shekhar Shashank, published 05 Sep 2017 (Daily mail Online), (https://www.dailymail.co.uk/indiahome/indianews/article-4855694/India-world-s-worse-rates-online-child-pornography.html)
7. By Thorn February 21, 2014 https://www.thorn.org/blog/child-trafficking-exploitation-in-the-united-states/)
8. Canadian Centre For Child Protection, (http://s3.documentcloud.org/documents/2699673/Cybertip-ca-CSAResearchReport-2016-En.pdf)
9. Convention On Child Right, adopted 20 Nov 1989, United Nation Human Rights, (https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child)
10. Convention On Cybercrime Budapest, 23.XI.2001, (https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)
11. Corera Gordonin “Intercept: The Secret History of Computers and spies” (2016)
12. D Cruze Cyril Danny, MINT, published 12 August 2021, https://www.livemint.com/technology/tech-news/net-banking-users-alert-govt-agency-warns-of-phishing-attack-that-can-steal-money-from-account-11628677018829.html
13. Danielle Keats Citron “Hate crimes in Cyberspace” (2014)
14. Debarati Halder and K. Jaishankar “Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations” (Citron, 2009a; Finn & Banach, 2000).
15. Directorate General for Internal Policies of the Union PE 604.979 – September 2018 https://ec.europa.eu/info/sites/default/files/information-provided-by-the-it-companies-about-measures-taken-to-counter-hatespeech_october2021_en.pdf

16. Hindustan Times, Laknow, published 9 August 2020 https://www.hindustantimes.com/india-news/no-internet-in-10-up-districts-including-lucknow-after-violent-caa-protests/story-KR2GoHodCTbgbqLAdLqaGJ.html
17. https://www.ijlmh.com/wp-content/uploads/Online-Hate-Speech-in-India-Issues-and-Regulatory-Challenges.pdf
18. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf
19. India Code Report. (https://www.indiacode.nic.in/handle/123456789/2079?locale=en)
20. Indian Penal Code,1860 (https://legislative.gov.in/sites/default/files/A1860-45.pdf)
21. Insurance Information Institute, Published 2022 (https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime)
22. International Journal Of Law, Management & Humanities, [Issn 2581-5369] Volume 3 | Issue 5 2020 https://www.ijlmh.com/wp-content/uploads/Online-Hate-Speech-in-India-Issues-and-Regulatory-Challenges.pdf
23. INTERPOL report shows alarming rate of cyberattacks during COVID-19, published August 2020. (https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19)
24. IWF, The Annual Report 2020, (https://annualreport2020.iwf.org.uk/trends)
25. K.S. Puttaswamy v. Union of India, Anirudh Rastogi, "Cyber Law – Law of Information Technology and Internet" (2014).
26. Kannan Saikiran India Today Published 11 April 2020, (https://www.indiatoday.in/news-analysis/story/pornography-gets-a-pandemic-boost-india-reports-95-per-cent-rise-in-viewing-1665940-2020-04-11)
27. Klein Berkman Centre Research Publication No 2016-19 https://deliverypdf.ssrn.com/delivery.php?ID=756021072024123106112080090001030069015032009051054004022004113025030125094098074078007052003023030014055090125098102090070114056022088032093124081121089079090030071033004090089081103010074084093096018075083094099112122093094004073017078095107122095&EXT=pdf&INDEX=TRUE
28. Klein Berkman, Centre Research, Publication No 2016-19 https://deliverypdf.ssrn.com/delivery.php?ID=756021072024123106112080090001030069015032009051054004022004113025030125094098074078007052003023030014055090125098102090070114056022088032093124081121089079090030071033004090089081103010074084093096018075083094099112122093094004073017078095107122095&EXT=pdf&INDEX=TRUE
29. Lech J. Janczewski and Andrew M. Colarik,"Cyber Warfare and Cyber Terrorism" (2008)
30. May 20, 2020. By Harshil Vaishnav | Cyber Law, Indialaw https://www.indialaw.in/blog/blog/cyber-law/cyber-law-and-fake-news-during-covid-19/

31. May 20, 2020. Byvaishnav Harshil | Cyber Crime. LA://www.law.cornell.edu/wex/espionage
32. National Crime Record Bureau (NCRB) and The International Criminal Police Organization (INTERPOL).
33. National Crime Record Bureau, (Volume III 2020) (https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf)
34. National Crime Record Bureau, report "Cybercrime against Children, 2020 (https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.11.pdf)
35. National Crime Records Bureau, (Ministry of Home Affairs), Government of India (Volume I 2018) (https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%202.pdf)
36. National Crime Records Bureau, (Ministry of Home Affairs), Government of India (Volume II 2019) (https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%202.pdf)
37. Panday Munish Chandra, India Today, published Nov 18 2021, https://www.indiatoday.in/india/story/24-lakh-online-child-sexual-abuse-cases-girls-under-14-india-2017-2020-1877928-2021-11-18)
38. Paul Bischoff Tech Writer, Privacy Advocate And Vpn Expert (January11, 2022) Camparitect. (https://www.comparitech.com/blog/vpn-privacy/child-abuse-online-statistics/)
39. Pawar Pal Ram, Director NCRB report" Crime in India 2020 https://cisomag.eccouncil.org/cybercrime-in-india-surges-by-11-8-in-2020-ncrb/
40. Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union PE 604.979 – September 2018 https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdfPolicy Department for Citizens' Rights and Constitutional Affairs
41. Sartak Dogra India Today, Published 19 April 2021 (https://www.indiatoday.in/amp/technology/news/story/over-27-million-indian-adults-experienced-identity-theft-in-the-past-12-months-says-norton-report-1792553-2021-04-19#referrer=https://www.google.com&csi=1)
42. Statatic Research Department, published March 2021, https://www.statista.com/statistics/1013804/facebook-hate-speech-content-deletion-quarter/
43. Statistics Research Department , published 3 March 2022. (https://rm.coe.int/1680084822)
44. Suzanne Ost “Child Pornography and Sexual Grooming” (2009)

45. The Economic Times, published 2021.diatimes.com/tech/internet/india-ranks-fifth-most-targeted-country-for-phishing-attacks-report/articleshow/21977766.cms
46. The United Nations office on drugs and crime, Vienna “Comprehensive study on cybercrime” (2013).
47. United Nation Human Rights , 25 May 2020 resolution General Assembly of the United Nations. (https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-rights-child-sale-children-child)
48. Verma Aditya- Report On Right To Privacy, https://cic.gov.in/sites/default/files/Right%20to%20Privacy%20and%20RTI%20by%20Aditya%20Verma%20%20%281%29%20%281%29.pdf
49. World Health Organization Privacy Legal Nation 2022 https://www.who.int/about/cyber-security