EMERGING CYBERCRIMES: MEASURES AND CHALLENGES IN CYBERSPACE

GROUP 1

PRESENTERS – ASTHA SHARMA,
ARADHYA GUPTA,
ANANYA MAHANTA,
ALANKRITA MALVIYA

INTRODUCTION

• Cybercrime implies to all criminal occurrences happening through the mode of the internet, computers, worldwide web and cyber space.

Cyber space can be defined as an intricate environment that involves interactions between people, software and services.

• The term 'Cyber Security' means "protecting information, equipment, device, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.'

• Day in and day out we find human rights violations and privacy of an individual is at stake with the recent advancements in the cyber space.

• This paper acts like a litmus test to check the misuse of cyber space, the prominent emerging kinds of crime and to discuss challenges faced in it which is doing wonders in many a field.

OBJECTIVES OF RESEARCH

1. To explain major kinds of cyber crimes and related laws in India.
2. To identify major issues and challenges present in Cyberspace.
3. To analyze relationship between intellectual property and cybercrimes.
4. To recommend measures and reforms necessary for protection of Cyber space.

- The term 'Cyberterrorism' was first coined by Banny C. Collin of the Institute for Security and Intelligence (ISI) in the late 1980s. But, its usage was better understood during the 9/11 attack.

- Use of the Internet to carry out violent activities that result in or threaten the loss of life or substantial physical injury to accomplish political or ideological advantages through threat or intimidation.

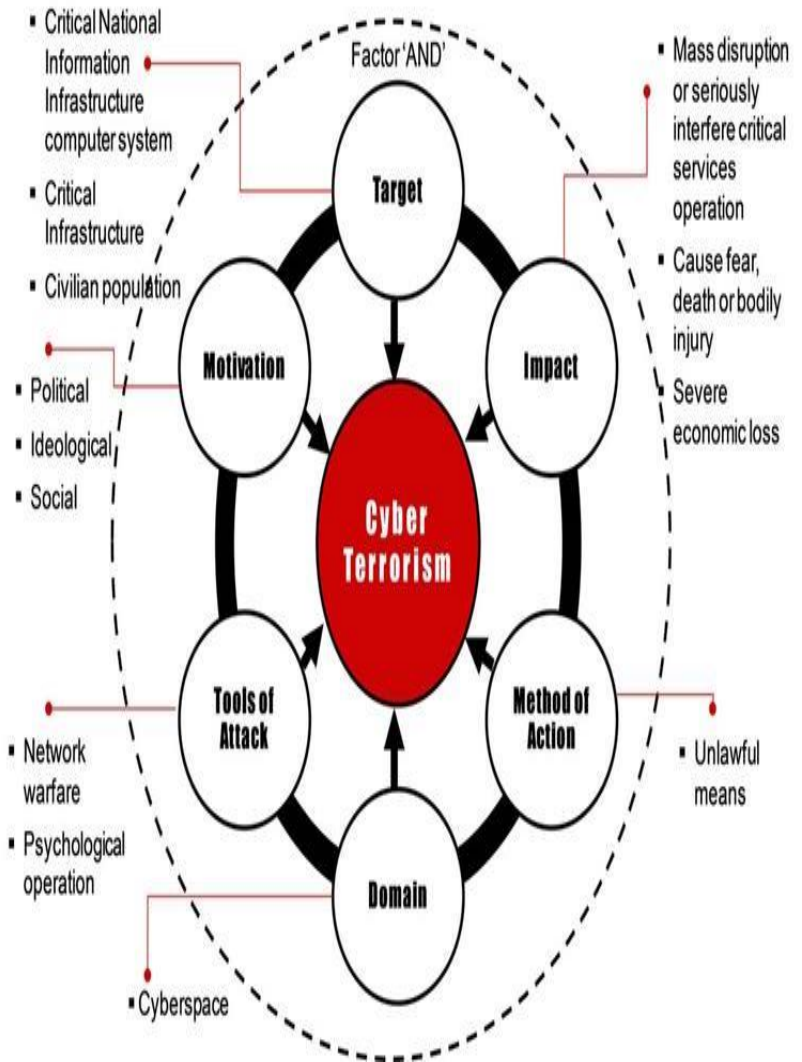
- According to Federal Bureau of Investigation (FBI), new phenomenon recognized as a cyber terrorism is defined by follow: “previously planned, politically motivated attack against information, computer systems, computer programs and data that result with violence against targets that are not military (civilian) by the sub - national groups or secret agents”

- Why should India Worry about Cyber Terrorism?

- Is India prepared to face Cyber Terrorism?

- Steps taken by Indian Government to control Cyber Terrorism:
- Cases related to Cyber Terrorism:

1. 26/11 Attack Case
2. The WannaCry outbreak



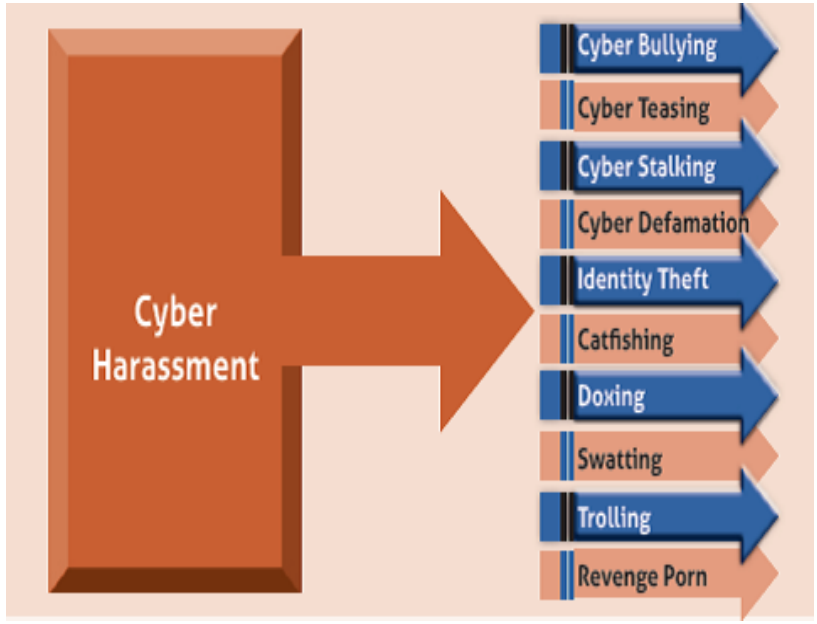
ONLINE SEXUAL EXPLOITATION

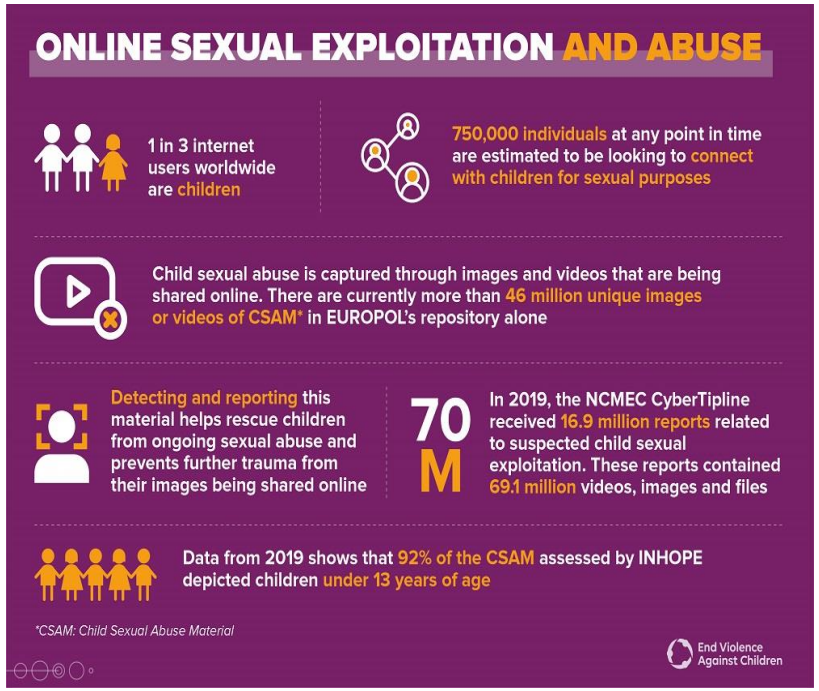
- One of the most witnessed form of exploitation is cyber harassment. Cyber harassement which is defined as unsolicited, repeated, hostile behaviour by a person using cyberspace with the intention of intimidating, harassing, threatening or humiliating a person. Any harassment through the use of electronic devices is considered to have the same impact as traditional forms of harassment.

- Cases on Online Sexal Harassment:

1. Saurabh Kumar Mallick vs. Comptroller & Auditor General of India

2. Jahid Ali vs. UOI





INTELLECTUAL PROPERTY INFRINGEMENT IN CYBERSPACE

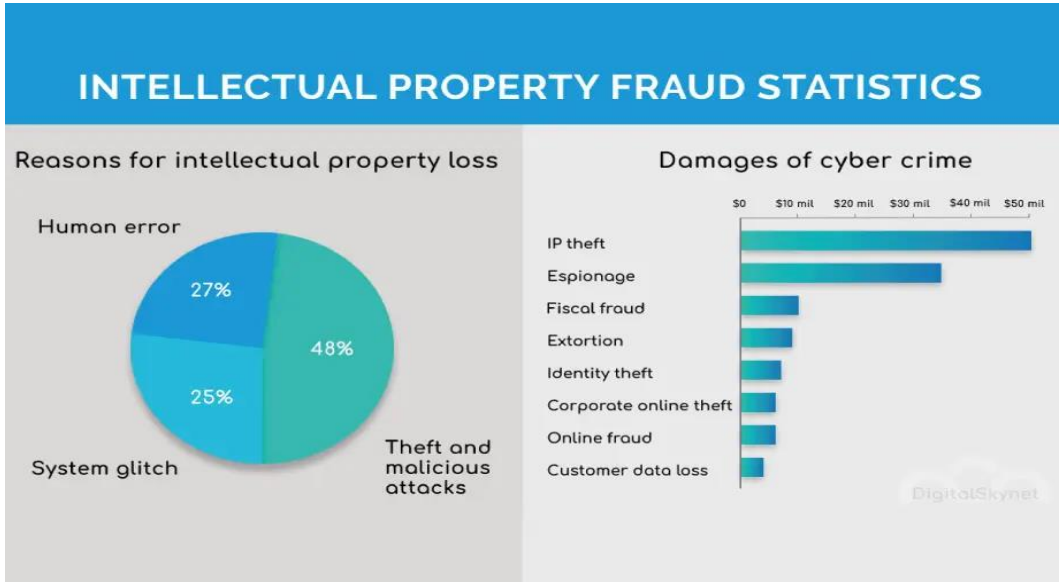
- **WHAT IS INTELLECTUAL PROPERTY (IP) ?**

IP is an intellectual work produced by the intellect of human brain. It is the product of human ingenuity, knowledge and skills besides labour and capital. For example, literary work, musical work, trademarks and design of industrial products, etc.

- **WHY IPR IN CYBERSPACE SHOULD BE PROTECTED ?**

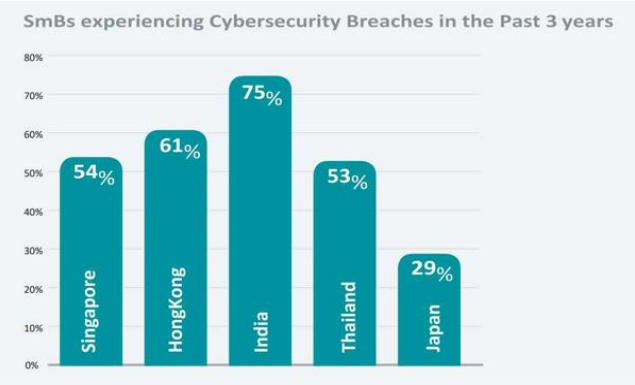
Effective protection of Intellectual property rights is essential since it protects the necessary incentives for creativity, as otherwise could be freely used. The main motivation of its protection is to encourage and reward creativity. An inventor does not have to fear that his/her invention is likely to be imitated or used by others without compensation.

- **WHAT IS COPYRIGHT ?**
- **COPYRIGHT INFRINGEMENT IN CYBERSPACE**
- **CASE – Super Cassettes v. MySpace**
- **WHAT IS TRADEMARK ?**
- **TRADEMARK INFRINGEMENT IN CYBERSPACE**
- **CASE – Christian Louboutin SAS vs. Nakul Bajaj.**



CYBER EXTORTION

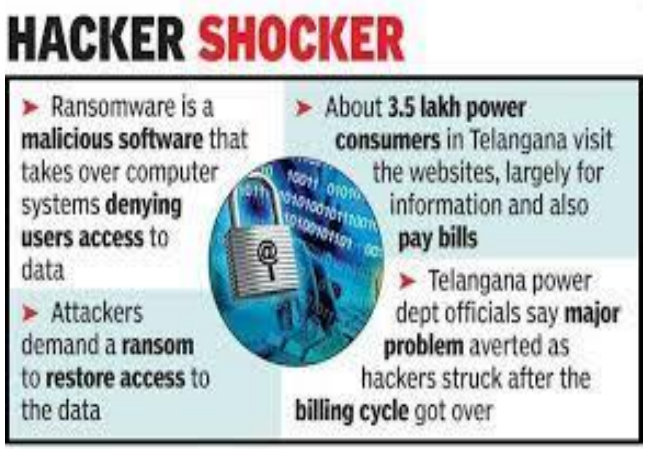
- Cyber extortion is used as an umbrella term for a wide array of cyber-crimes. Cyber extortion occurs when hackers or cyber-criminals try to threaten a targeted business or organization to compromise its confidential data unless they receive a ransom. Ex - Ransomware & DDoS (Distributed Denial of Service) Attacks.
- India ranked fourth among Asian countries in terms of doubling ransomware detection rate to 7.34% in Q3 2021, from 3.65% in Q2 2021.



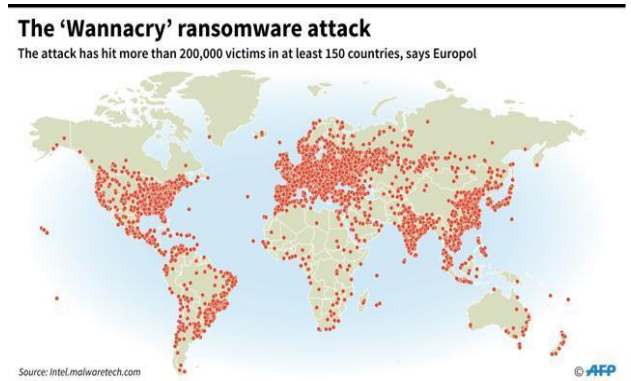
WHAT IS RANSOMEWARE ?

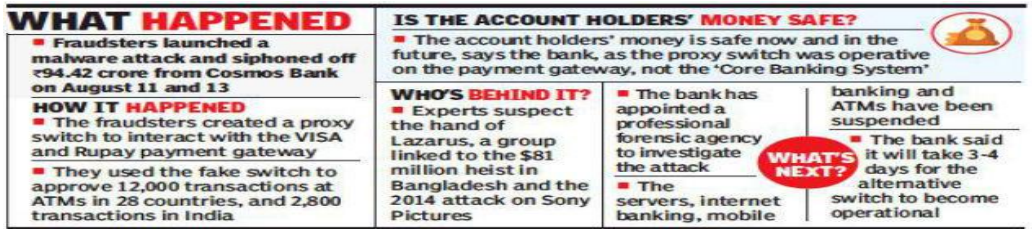
WHAT IS DDoS ?

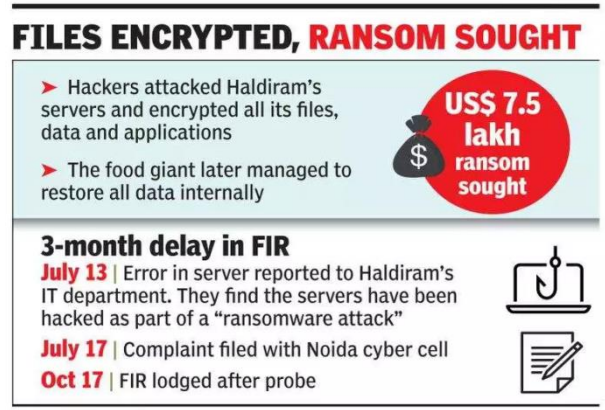
CASES ?



1. Telangana Cyber Extortion case
2. Haldiram Ransomeware Case







CYBERSPACE CRIMES: INTERNATIONAL AGENCIES AND INTERNATIONAL CONVENTIONS:

BUDAPEST CONVENTION

- The first international treaty on crimes committed via the Internet.
- Convention provides the ‘substantive’ and ‘procedural’ provisions
- which are needed to be adopted by State parties in their domestic
- legislations in order to implement the Convention.
- Convention aims principally at setting up a fast and
- effective regime of international co-operation.

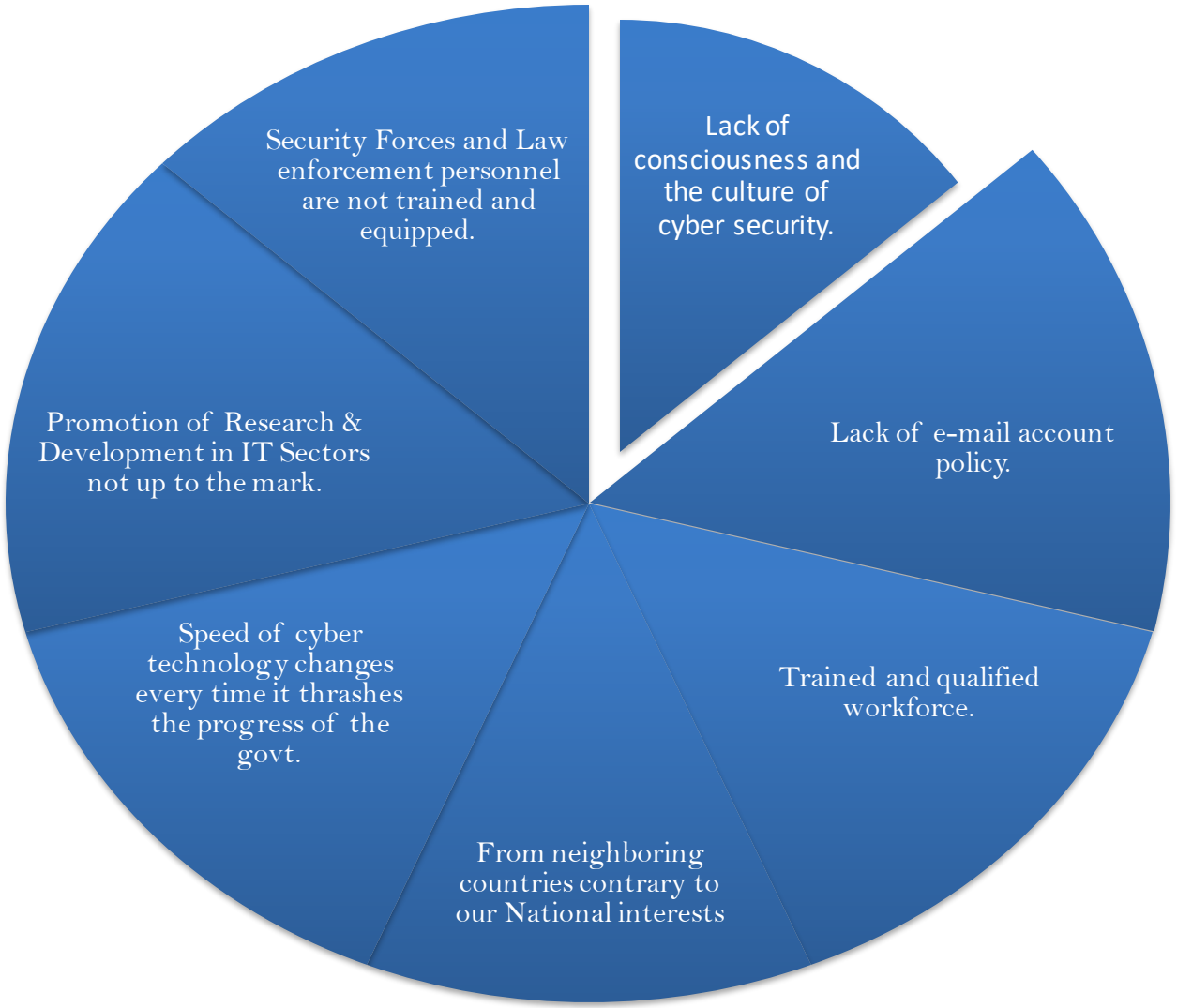
INTERPOL'S RESPONSE

- Criminals are exploiting the fear and uncertainty caused by the unstable social and economic situation around the world due to the COVID-19 pandemic to launch cyberattacks.

- Outlines five action streams, with the common goal of helping member countries to identify cyberattacks and their perpetrators.

- INTERPOL uses 'Purple Notices' to alert member countries to emerging and high-risk cyberthreats, providing technical guidance to victim organizations for their recovery efforts.

CYBER CRIME CHALLENGES



RECOMMENDATIONS

TECHNOLOGICAL ASPECTS

1. Intrusion Management

Process which primarily aims at precluding intrusions in the computer system therefore furnishing effective-security control medium.

2. Self- regulation by computer and net druggies

It's a process of developing a healthy law of conduct by espousing a policy of restraint by both the computer druggies as well as the service providers.

3. Use of voice-recognizer, sludge software and collar-ID for Protection

Computers as a means for carrying out routine life conditioning, should be equipped with some safety and security bias to cover against authorised operation of computer systems.

4. Use of diligent Anti-Virus Softwares

Antivirus software is a computer program which detects, prevents and takes action to protect the system and remove all malicious software programs like viruses etc.

RECOMMENDATIONS

LEGAL ASPECT

1. Use of encryption technology

To appoint well trained Information Security Officers who should be responsible for overall protection of computer coffers and for any lapse in computer security.

2. Use of international treaties & agreements to present a combined front

Ensures that all applicable local legislations in harmony with international laws and conventions

3. Establish progressive capacity building programmers for national law enforcement agencies

4. Symbiotic relationship between firms, government and civil society to strengthen legal frameworks for cyber-security.

RECOMMENDATIONS

RESEARCH ASPECT

1. Improving awareness and competence in information security

2. Formalize coordination and prioritization of cyber security research and development

3. Implement an evaluation or certificate programme for cyber security system

4. Develop foster and maintain national culture of cyber security

5. Efforts to standardize and coordinate cybersecurity awareness and education programme

CONCLUSION

Cybercrime is inflating at an exponential rate in India and the globe alike. Crimes in Cyberspace includes intellectual property infringement, cyber terrorism, cyber extortion, sexual harassment which have been analyzed thoroughly in this paper in the context of Indian jurisprudence.

The paper also provided a comparative analysis with the New challenges faced in cyber security in electronic networks. It is time for Indian legal system to match its pace with the growing cyber crimes and the developing international jurisprudence around it as in the information age, opportunities to grow exist for those who are best able to utilize both technology and information.

With the advent of COVID-19 pandemic the need for this change has become more imminent and necessary. Statutory laws, government policies, specialised investigating agencies will go a long way in securing India's cyber spaces.

The people ought to be equipped with enough knowledge to be able to defend themselves against the threats of cyber crimes through legal awareness programmes.

Emerging Cyber Crimes: Measures and Challenges to control them

- Group 1

GROUP 1

AARUSHI VERMA (3rd year, B.A Economics (Hons), University of Delhi)

ADITI MEHNDIRATTA (2nd year, M.Sc. Forensic Psychology, National Forensics Science University)

ALANKRITA MALVIYA (5th year, B.A LL.B (Hons), Himachal Pradesh National Law University, Shimla)

AMISHA BANSAL (5th year, B.A LL.B (Hons), University Five Year Law College, Jaipur)

AMIT JAIN (5th year, B.A LL.B (Hons), National Law University and Judicial Academy, Assam)

ANANYA MAHANTA (1st year, LL.M, Assam Rajiv Gandhi University of Cooperative Management)

ANIKET RAJ (4th year, B.A LL.B, O.P. Jindal Global University)

ARADHYA GUPTA (5th year, B.A LL.B (Hons) Teerthanker Mahaveer College of Law & Legal Studies)

ASTHA SHARMA (4th year,B.A LL.B, Guru Ghasidas University, Chhattisgarh)

BHASKER RAWAT (1st year, M.A South Asian Studies, Pondicherry University)

TABLE OF CONTENTS

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 Mr. Bimadhar Pradhan, Secretary General, NHRC who gave us the opportunity to do this wonderful research paper on the topic "Cyber CimesThe Concerns and Measures Surrounding Them". We are highly indebted to Mr. Mukesh Kulshreshtha for his supervision. We would like to thank Mr. Sam T John for his guidance and providing the necessary information and resources for this project. Also, 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: 03/03/2022

GROUP 1

NHRC Interns

February, 2022

ABSTRACT

Cyber Security plays a crucial role in the field of information technology. Securing and protecting the information has become one of the biggest challenges in the present day. Digital technology is circumscribing in all walks of life, all over the world and has put forward the real meaning of globalisation. At one end, the cyber system provides convenience to communicate and at the other end some individuals or communities make unethical use of its power for criminal purposes.

Whenever we think about cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing tremendously day by day. Various Governments and companies are taking many measures and actions in order to prevent these cybercrimes.

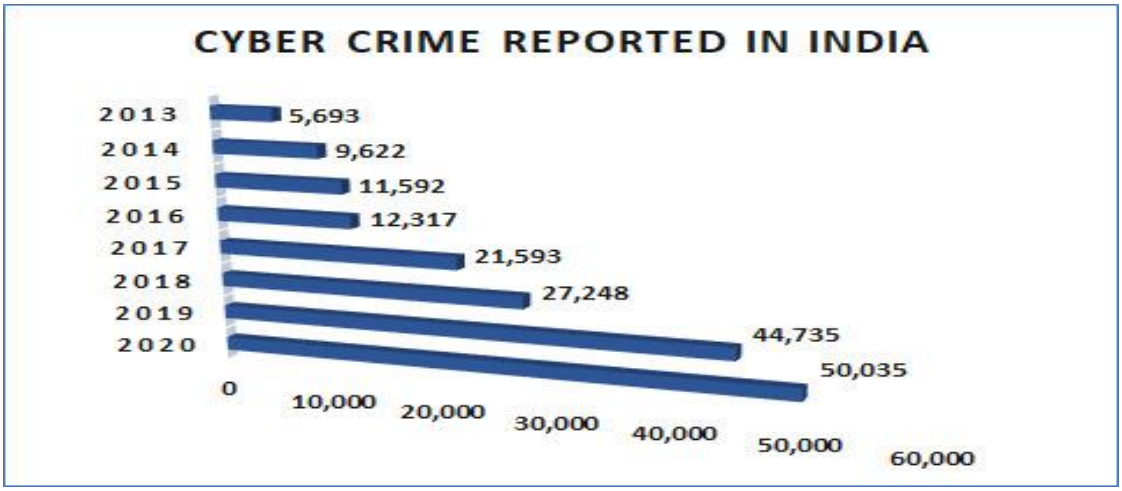
Situation is alarming and startling: Cybercrime is the talk of the town in every field of society and systems. In the last decade they have severely destroyed businesses and compromised individual and as well national security.

This paper mainly focuses on the concept of cybercrime, some particular types of prevalent cybercrimes taking place prominently, challenges faced by cyber security on the latest technologies, looking towards people who are involved and the reasons for their involvement. It also focuses on the trends changing the face of cyber security and proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

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

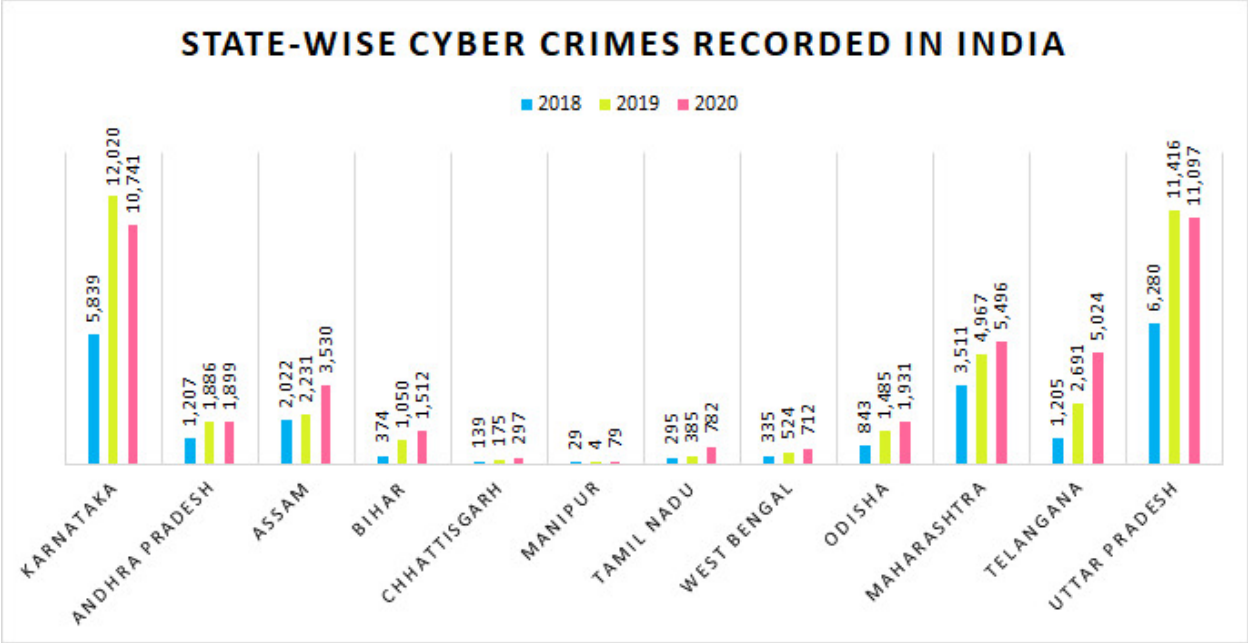
1. INTRODUCTION

Human Rights are interconnected with everything which is happening around us. It gives us the right to live with dignity and liberty. Some of our human rights are mentioned in Fundamental Rights and Directive Principles of State Policy of our Constitutions and also in the UDHR (UNIVERSAL DECLARATION OF HUMAN RIGHTS) 1948. Human rights are not only those which are mentioned in any law in simple terms but it is that which gives you strength to live freely with the fulfilment of basic needs and value. In the present times, we use technology to share our information in various platforms which includes bank records, medical records, job applications and e-commerce websites and the most important among them all is the sharing of information in the social media. Due to the covid-19 pandemic, the usage of internet has increased manifold and people are forced to resume their work from home. At the same time, there is an increase in the use of technology for work, studies, entertainment which includes frequent sharing of data with everyone. Today, we need to share our information in order to access many important provisions such as health care services, monetary transactions, purchase of goods etc. At the same time, technology has helped the security and law enforcement agencies to detect and prevent any incident affecting the national security of the country. Meanwhile, every the cyber criminals try to extract data and hack into systems of government establishments which can lead to great consequences of data being sold on unauthorised servers and internet domains. In all this strong data protection is the need of the hour, which may either prevent the attack or reduce its magnitude.



(*Source: Image from News 18*) Figure 1

Cyber Crime is a crime committed by a person using a digital medium. As shown in Figure 1, the incidents of cybercrimes in India have been increasing at a rapid pace and jumped by nearly nine times between 2013 and 2020, official data showed. As per the latest 'Crime in India' report, cybercrimes in India increased to 50,035 during 2020 from 5,693 cases reported in 2013.



(*Source: Image from News 18*) Figure 2

As explained in Figure 2, in the year 2020 alone, Uttar Pradesh recorded the most cases of cyber crime — 11,097 — followed by Karnataka with 10,741 cases. Maharashtra (5,496 cases) and Telangana (5,024 cases) stood next, the data showed. The states that have recorded massive jump in the cases of cyber crimes between 2019 and 2020 were Arunachal Pradesh (from 7 to 30); Assam (2,231 to 3,530); Chhattisgarh (175 to 297); Goa (15 to 40); Gujarat (784 to 1,283); Manipur (4 to 79) and Telangana (2,691 to 5,024).

Also, states, including Bihar, have reported a huge rise in cyber crimes last year when compared to 2018. In Bihar and Telangana, cases of cyber crimes have increased by over four times, while in Uttar Pradesh, there has been an increase of over 75 percent since 2018. In Odisha, West Bengal, Karnataka and Chhattisgarh, the cases have more than doubled since 2018, while that in Tamil Nadu and Manipur have increased by three times.

Many have witnessed new and emerging cybercrimes in the form of Phishing, Extortion, Cyber Exploitation and Cyber terrorism. According to FBIs report, India stands third among top 20 cybercrime victims. The national cybercrime reporting portal started by the central government received 33,152 complaints till now resulting in lodging of 790 FIRs. In fact, according to a 2017 report, Indian consumers had lost over 18 billion US dollars due to cybercrimes. In 2018, there were over 27,000 cases of cybercrimes recorded in the country, marking an increase of over 121% compared to the number of the cases in 2016[1]. The government is making various efforts to control Cyber Crime at both the National and International levels but they are facing challenges too. We have covered some kinds of cybercrime happening in cyberspace and also we have discussed what measures we can take and what challenges we are facing as far as cybercrimes are concerned in this research paper.

Figure 3
Source: Centre for Strategic and International Studies (CSIS)

The above graph shows the data on the number of cyber-attacks in the year 2020 of which India stands at the third place for highest number of such attacks.

[1] NCRB Report, 2018

2. RESEARCH QUESTIONS

a) How human rights are violated by the emergence of cybercrimes?

b) What are the important laws and judicial pronouncements that protect individuals from cybercrimes?

c) How can intellectual property be infringed by cyberspace attackers?

d) What are the measures that can be adopted to control cybercrimes?

3. OBJECTIVES OF THE STUDY

a) The research aims to understand the hidden and emerging cybercrimes like cyber terrorism, cyber extortion, intellectual property infringement and inline sexual exploitation.

b) It tries to identify the major issues and challenges present in cyberspace and its potential to affect human rights.

c) By analysing various statistical data and reports the research tries to analyse the relationship between intellectual property and cyberspace crime.

d) The study proposes to establish that the crimes are serious threat to human rights and national security

e) The study will bring out appropriate suggestions that can assist the stakeholders in policy making decisions.

4. LITERATURE REVIEW

Anirudh Rastogi, "Cyber Law- Law of Information Technology and Internet"

In this book, the author explored different kinds of cybercrime in India. It covered the IT Act together with laws governing jurisdiction, e-contracts, intellectual property rights and E- evidence. He also provided critique of laws relating to Information technology. This book also includes emerging fields and aspects of cyber study and issues such as state observations and supervision, cloud computing, virtual currencies and social media regulation, conditions and terms of the websites and e-governance.

Mohak Rana, "Crimes in Cyberspace: Right to Privacy and Other Issues"

This article discusses the meaning and types of the cybercrime in India as well as US and UK. It also deals with the evolution of cybercrime, their categories, Indian perspective of cyber space legislations and, different types of liabilities under IT Act and cases of cyber crime in India.

Talat Fatima, "Cybercrimes"

In this book Dr. Fatima highlights the key issues that the legal world faces in current cyber-age.

i. identifies online crime offences; and
ii. Analyze the legal problems and
iii. measures need to be taken up against the cyber criminals.

The book broadly analyses and discusses the cyber laws and judicial practices in India along with taking into picture the aspects of systems of the United Kingdom and the United States.

Maskun, Manuputty, Noor, & Sumardi, 2013

This book studies and discusses the concept of Cyber Warfare. “Cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood.” In comparison to Alford's (2001), this definition avoids attempting to define the motivation of the fighting parties. It discusses that a cyber-attack on critical national framework, such as the power grid may result in loss of life. Colarik and Janczewski (2011) agree with this point and argues that cyber warfare cannot be seen as bloodless.

Vakul Sharma, "Information Technology- Law & Practice".

This book has been written in a very clear and comprehensive manner with examples, narratives and diagrams, which the readers may not be found in any other book of this genre. This book discusses the different challenges and aspects of the IT field. It analyses the issues related to the cybercrime, Internet blocking, virtual currency, child pornography, cyber terrorism, cyber security.

This research paper deals with concepts of cyber crime keeping in mind the recent activities that have taken place and offering solutions to protect an individual and/or an organisation. It also elucidate on the state of cyber crimes and cyber security in India and an overview of Indian cyber laws is presented in this paper as well.

5. METHODOLOGY

The Methodology used in this research paper is strictly doctrinal. The report is the descriptive analysis of the different types of cyberspace crimes in India. The most precise secondary data on cybercrimes had been collected from authentic sources. The data used here has been collected from different books, articles, magazines, journals and legislations.

6. STUDY ANALYSIS

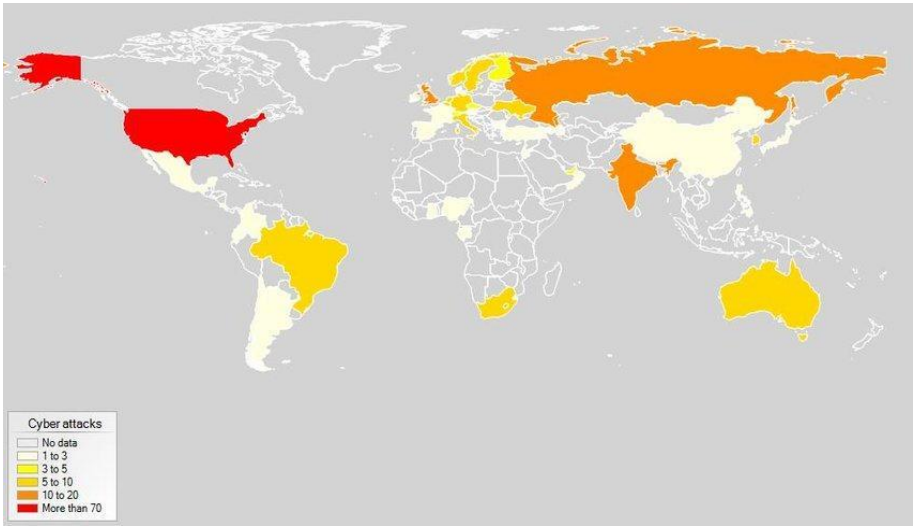
In research, it is found that in every 10 people 7 people are found as a victim of cybercrimes. In the easiest term, we can define cybercrime as the use of computers and other digital mediums to commit a crime is Cyber Crime. Today we can see so many kinds of Cyber Crime in the world such as Phishing, Cyber Extortion, Child Pornography, Cyber Terrorism, Cyber Harassment, Data Theft among others. Some of those types are covered in our research paper. The US Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

❖ TYPES OF CYBERCRIMES

The rapid growth of this information highway has also led to new forms of crime online - also termed as 'cybercrime' (Tandon, 2022). According to a report published by the Indian Computer Emergency Response Team (CERT), which is the national agency responding to computer security

incidents, the number of incidents reported in 2004 were 23. In 2007, the figure went up to 1,237 and in 2010 there was a significant rise to 10,315 incidents.

India is the second largest online market in the world with over 560 million internet users, ranked only behind China. It is estimated that by 2023, there would be over 650 million internet users in the country. According to the recent National Crime Records Bureau data, a total of 27,248 cases of cybercrime were registered in India in 2018. And according to the Global Security Index, 2020 as shown in the figure below, India ranked 10th all over the world in facing cyber attacks every year. On average India face 10-20 cyber attacks every year, which is a concerning number from the cyber security perspective.



Source 2: Global Cybersecurity Index, 2020

I. CYBER TERRORISM

The cyber space has provided an advantageous platform for cybercriminals for executing their malicious activities, spreading hate propaganda, etc. over the internet. This was possible because of minimum online regulations, anonymity, large audience, fast circulation of information, and many other benefits", says Cyber Expert, Anuraag Singh. Just the word terrorism was enough to give some chills to the bones, and when it gets combined with the word Cyber i.e., digital, it becomes even more terrifying.

The term 'Cyber terrorism' was first coined by Banny C. Collin of the Institute for Security and Intelligence (ISI) in the late 1980s. But its usage was better understood during the 9/11 attack.

Cyber terrorism is a controversial term with no clear definition yet. However, it can be understood as the use of the Internet to carry out violent activities that result in or threaten the loss of life or substantial physical injury to accomplish political or ideological advantages through threat or intimidation. Under Cyber terrorism attack, there will be large-scale disruption of computer networks that are connected to the Internet. This is accomplished using tools such as computer viruses, computer worms, phishing, malicious software, hardware methods, programming scripts, and much more.

- *Why Should India Worry about Cyber Terrorism?*

The World Economic Forum's Global Risk Report for 2021 highlighted cyber security failure as one of the most serious challenges to humankind over the next decade.

After China, India has the second-largest online market in the world with a population of 749 million. Along with the perks of technology India has enjoyed in the last few years, it has also faced the brunt of many terrorist activities that were successful only because of the availability of technology.

Some of the deadliest terrorist operations to which India fell prey because of the misuse of digital technology include the URI attack, the Pulwama assault, and the horrific 26/11 Mumbai incident.

In the investigation of the Mumbai Attack, the extensive use of digital telecommunication by the terrorists was revealed. It was only through the internet that the terrorists were able to get India’s map, population infrastructure, place, etc. They even used “Google Earth” to execute their plan, a mobile network for command and control, and social media to track the movement of Indian Rescue and Defense Forces. In the year 2020, CERT-In handled 11,58,208 cyber terrorism-related threats. These included Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware attacks, Data Breach and Vulnerable Services.

- *Is India prepared to face Cyber Terrorism?*

"Today, the enemy no longer needs to enter the border. He can also target our security apparatus from outside the border. Alignment and realignment of global powers have added to the already changing security challenges," said the Defense Minister, Rajnath Singh said on 77th Staff Course at the Defense Services Staff College (DSSC), Wellington.

To make India ready to fight cyber terrorism, certain steps are taken by the Government itself:

i. A Defense Cyber Agency under the Ministry of Defense is established. This agency seeks to reduce cybercrimes in the Indian Army, Navy, and Air Force.
ii. Cyber Emergency Response Teams (CERT) are established.
iii. The Government of India took a major leap with the establishment of the National Cyber Coordination Centre (NCCC). It deals with cyber threats and cyber-terrorism. All CERTs and ISACs would subsequently be linked with NCCC to provide a speedy and seamless flow of cyber threat information across the board for all stakeholders.
iv. The Indian Cyber Crime Coordination Centre (I4C) is also launched under the Ministry of Home Affairs (MHA) to combat cybercrime and cyberterrorism.
v. Adequate protections are implemented in the form of Cyber Audits, Physical Checks, and Policy Guidelines to guarantee the Armed Forces of the nation are strong in cyberspace.
vi. Mock drills and exercises in cyber security are conducted regularly.
vii. To reduce the susceptibility of internet traffic to cyber-attacks, efforts are taken to guarantee that traffic originating and ending within India is routed within India's geographical borders. The mechanisms will be developed in collaboration with the relevant government ministries, Internet Service Providers (ISPs), and NIXI.
viii. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been established to identify dangerous programs and provide free tools to remove them.

According to US law, the state secretary has an obligation to get the report on Congress each year, which is put into the Annual report. Terrorism is defined in a follow way: "premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents". "The term "terrorist group" means any group practicing, or which has significant subgroups which practice, international terrorism". According to Federal Bureau of

Investigation (FBI), new phenomenon recognized as a cyber terrorism is defined by follow: "previously planned, politically motivated attack against information, computer systems, computer programs and data that result with violence against targets that are not military (civilian) by the sub - national groups or secret agents". Another definition according to US Commission for Protecting Critical Infrastructure is that terrorist attacks are created in order to cause physical violence or extreme financial damage. The cyber-terrorist is assumed to be professional, creative, and very clever. They will seek unorthodox and original methods to accomplish their goals. Individuals who are well schooled in traditional information security techniques are not well suited to being a cyber-terrorist, simply because they have been exposed to or trained in classic security techniques and doctrine. The cyber terrorist will seek to accomplish their mission by techniques not mitigated by classic security mechanisms (Petrović R. S., 1999). Terrorists leave traditional way of fighting with classical weapon and other weapon but also they introduce the use of sophisticated high technology which shows that they become can use digital medium for committing terrorist activities.

II. CYBER EXTORTION

Cyber extortion is used as an umbrella term for a wide array of cyber-crimes. Cyber extortion occurs when hackers or cyber-criminals try to threaten a targeted business or organisation to compromise its confidential data unless they receive a ransom. Therefore the two most common types of Cyber extortion are ransomware and DDoS (Distributed Denial of Service) Attacks.

- **Ransomware**

The world first came across the term ransomware, in the true sense, after crypto currency like Bitcoin came in 2013. It came with the advent of malevolent 'Cryptolocker' RWA, which utilised 'game-over zeus' botnet and extorted over $3 million. Russian hacker Evgeny Bogachevave, father of Zeus botnet and originator of first sophisticated Ransomware attack (RWA), is still at large and carries a reward of more than USD 5 million.

It is typically a malware (or a malicious software) that enables cyber extortion for financial gain. Ransomware can easily be hidden inside a mail or seemingly normal webpage. It can prevent you

from accessing your computer files, networks, and demands you to pay a ransom in return. Usually in anonymous currency like Bitcoin. What makes Ransomware exponentially dangerous is that it is next to impossible to decrypt data by experts, as current techniques of decryption, like RSA would require billions or even trillions of years to decrypt data.

India ranked fourth among Asian countries in terms of doubling ransomware detection rate to 7.34% in Q3 2021, from 3.65% in Q2 2021[2].

Apart from data loss by encryption, sometimes the cyber-criminal also makes money by selling the sensitive data. In 2020, India's housing loan company was hit by ransomware, which led to loss of data. The organisation was in deep trouble, as it lost the data of how much they need to recover from their clients. It had to pay over Rs. 50 crore in Bitcoins as ransom to procure the decryption key. The case was never reported to law enforcement, as per an article by Times of India.

Virtual currencies have given a huge flip to ransomware. As it gives relative anonymity to the owner, in order to trace the IP address of the cyber-criminal, it can take a forensic expert tremendous amount of effort.

Forbes in its recent edition has stated that in 2021, ransomware extortions have exceeded USD 250 billion. The attacks are launched almost every 10 seconds affecting 2.5 million internet of things (IoT). Some of the best cyber-criminal earn USD million every month, which has led to the industrialization of this crime. The revenues from it exceed 6 trillion USD in 2021, it is almost about 2.5 times the economy size of India.

Though RWA has appeared to be a robust evil. With the majority of cases being undetected and cyber-criminals are not brought to justice. There is a silver lining. It can be thwarted or prevented making RWA ineffective.

- **DDoS (Distributed Denial of Services):**

It is a type of cyber- crime in which an internet site is made unavailable. This is typically done by using multiple computers to repeatedly make requests that tie up the site and prevent it from

[2] Acronis Cyber-threats report 2022

responding to requests from legitimate users. The major goal is to deny someone with a particular service. Depending upon the target business, the downtime can sometimes create major financial losses.

The first known DDoS style attack happened in Feb 2000. When a 15 year old Canadian hacker “mafiaboy " orchestrated a series of DDoS attacks against several e-commerce websites, including Amazon and ebay. These attacks used multiple computers at different locations to overwhelm the vendor’s computer and shut down their www (World Wide Web) sites to legitimate commercial traffic. The FBI estimated the damages to be around $1.7 billion, it crippled the internet of commerce.

DDoS is a special kind of hacking. A criminal sets an array of multiple computers with programs that can be triggered externally from another system. These programs are known as “Trojan Horses”, since they enter the computer system as something benign. Like a photo or an e-mail. At the pre allotted time the Trojan Horse program starts to send messages at a predetermined site. If enough computers have been compromised, it is likely that the selected site can be tied up so effectively that little if any legitimate traffic can reach it.

One thing is that much of the software in devices is insecure making it very easy for even amateurs hackers to compromise your data. Although some software companies do patch their vulnerable data from time to time and update their systems.

In August 2020, the DDoS attacks in India hit a record high. In terms of DDoS packets they were well above 10 billion, as per a study conducted by global cyber security firm Radware.

The two main statutes that prescribes punishment for cyber extortion are the Indian Penal Code and the Information Technology Act. Extortion is defined under Section 383 of the Indian Penal Code, 1860 which provides that whoever intentionally puts any person in fear of any injury to themselves or someone else and thereby dishonestly induces such person to create fear to deliver any property, or any valuable security or anything signed or sealed which may be converted into valuable security commits the crime of extortion. Therefore, this provision under the Indian Penal Code provides punishment for situations where the blackmailer has asked for monetary or valuable security.

Forgery has been defined under Section 463 of the IPC to mean the making of a false document or false electronic document or false electronic record or part thereof with the intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed. Section 465 stipulates punishment for the offence of forgery. Further, Section 66 of the Information Technology Act provides punishment for computer related offences. Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resources or communication device. The punishment for this offence under the Act is imprisonment of up to three years or a fine up to Rs. 1,00,000 or both. (The Information and Technology Act, 2000.)

Section 66C prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1,00,000.[3]

Section 66D stipulates punishment for 'cheating by personation by using computer resource' and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1,00,000.

III. INTELLECTUAL PROPERTY INFRINGEMENT

The advancement in e-commerce and e-business has led to an important concern to the companies and organisations to protect their intellectual property rights online. Nowadays, cyber-crimes do not only confine itself to fraud, cyber bullying, identity thefts but also infringement of copyrights and trademarks of various business and other organisations. Intellectual Property Rights (IPR) and Cyber Laws cannot be separated, and online content must be protected.

[3] Section 66C, The Information and Technology Act, 2000

Cyberspace is the non-physical domain over which the communication between computers takes place through computer networks. With the growth of technology every individual has a right of accessing cyberspace and sharing information.

In cyberspace, sometimes private information is shared by a person who is not the owner. Hence, privacy is violated. One makes profit from another person's creation (Abirami, 2020)

Intellectual Property is an intellectual work produced by the intellect of the human brain. It is the product of human ingenuity, knowledge and skills besides labour and capital. Intellectual property rights allow people to assert ownership rights on the outcomes of their creativity and innovative activity in the same way that they own physical property. Effective protection of Intellectual property rights is essential since it protects the necessary incentives for creativity, as otherwise could be freely used. Such incentives help in promoting knowledge based growth and socio economic development. Nations give statutory expression to the economic rights of creators in their creations, and to the rights of the public in accessing those creations. The main motivation of its protection is to encourage and reward creativity.

The intellectual property systems must maintain an equitable balance of interest between public good and private interests and should help promote socio economic improvement, the general prosperity of society through the advancement and worldwide application of beneficial technology, the promotion of competitive trade and encouragement of innovators and creators. An inventor does not have to fear that his/her invention is likely to be imitated or used by others without compensation.

The utility of computers and the internet is well understood and in fact embedded in modern business and commerce as well as in society in general. The advantages of the use of the computers and internet are immense in modern business and our society can’t function smoothly without computers and information technology. But the use of the internet and computers has brought along many unavoidable misuses of computers and the internet. This has been possible more so because, in the use of the computers, there is no any territorial limit and can be used from any jurisdiction. E-commerce nowadays has become very popular especially in the corporate sector. The advantages and scope of publicity of business through e-commerce or business on the World

Wide Web can reach the surfers very fast in any part of the world. But this has paved the way for the emergence of cyber-crime. (Ahmad, 2011)

The meteoric rise of cyber-crimes in the world is undeniable. But it wasn't until much later that this quandary was even acknowledged by the general population or legislation. The fact of the matter is that with the breakneck speed of new digital technology build-out—which patently highlights the nifty uses—sadly, ends up shrouding the major drawbacks. Nevertheless, there has been much-needed awareness in the past few years regarding cyber offences; it's not treated as a trifling matter anymore.

To deal with the cyber-crimes, the parliament of India has enacted the Information Technology Act, an act based on UNCITRAL (United Nations Commission on International Trade Law.) (which adopted model law on e-commerce advocating a shift from paper based environment to a computer based environment) (Sharma, 2013)

The IT Act, 2000 provides legal recognition to digital signatures and electronic records. It is a legal framework to facilitate and safeguard electronic transactions in the electronic medium.

While the digital age has its multiple advantages, the flipside is that the ease of availability of information online and ease of duplicating it along with anonymity pose a continuous threat to the protection of Intellectual property rights including copyrights on the internet.

There are two main ways by which computers can be involved in crime (Schudel, Gregg, and Wood, Bradley, 2000)

• Old crimes conducted using computers as a tool: for example storage of illegal images on a hard disk instead of in print; harassment using mobile telephones or illegal downloads of music and other forms of piracy. Another example is 'phishing': confidence tricks involving spoof emails and fraudulent websites to acquire sensitive information. (Freeh, J.L., 1998)

• New types of crime made possible by specific technology. An example is a denial of service attack or DoS which prevents computer resources from being available to intended users, for example by flooding web servers with more data than they can process, thus forcing websites offline. Other crimes involve attacking a computer (often by 'hacking' or gaining unauthorized

access to a computer system) or writing a virus (a type of malicious software or 'malware') to delete stored data. (Freeh. 1998)

In India, Copyright exists in source code of a computer program. Computer software is protected as literary work and so are computer databases as per Section 2(o) of Copyright Act, 1957. Thus, an original database is also protected by copyright.

According to Section 14 of the Copyright Act, 1957 an author of a work has the sole and exclusive right to enjoy and exploit several rights conferred by the Act for literary , dramatic, musical or artistic work, cinematographic film and sound recording. Rights mentioned under Section 14 include the right to reproduce the work, to issue its copies, perform or communicate work in public , make adaptations, translations, selling or rental rights in respect of different categories of work. Term of copyright in published literary, dramatic, musical and artistic works is the lifetime of the author and sixty years from the beginning of the calendar year the following year in which the author dies. Same is the case with cinematographic film and sound recording.

Where copyright is infringed, the owner of copyright is entitled to sue for remedies including injunction, damages, profit of accounts and delivery of infringing goods.[4]. Section 51 states copyright in a work is considered to be infringed when a person without a license from owner or registrar of copyrights or contravening conditions of a license does anything the exclusive right to do which is the right of the owner as per the Act or permits for profit a place to be used for communication of work to public where such communication constitutes infringement of copyright in the work unless he was not aware and had no reasonable ground to believe such communication will be infringement of copyright.

It also amounts to an infringement where a person makes for sale or hire or displays or offers for sale, or distributes for trade or to prejudicially affect the owner of copyright or by way of trade exhibit in public or import into India infringing copies of work (excluding one copy for personal use of importer). As registration is not compulsory, suits for infringement can be filed even if the plaintiff has secured no registration of the work.[5]

[4] Section 55(1) of copyright Act, 1957
[5] JN Bagga v Air ltd, AIR 1969 Bom 302

The relationship between the Internet and Copyright law is complicated. The internet is an international system for the transmission and reproduction of material, much of which is protected by Copyright. It therefore presents previously unimaginable possibilities for copyright infringement and many challenges for copyright law.

When these copyrights are used by anybody without the permission of the owner, it amounts to infringement of such copyright. When copies are made of software which are distributed on the internet and sold by any person other than the owner, it amounts to copyright infringement. Copying from a website or content from the blog also amounts to a copyright violation.

The following features of the internet pose particular difficulties for copyright law:

i. Information may be easily reproduced and distributed. Once the information is in digital form on a computer connected, uploaded, downloaded and distributed.
ii. Internet users expect free access to copyright material. Much of the copyright material published on the internet has been made available free of charge. This has created resistance among users to pay for the Internet material.
iii. Internet users may act anonymously. It is difficult to identify an industrial Internet user. Users may therefore infringe copyright with little risk of detection, especially if the infringements are relatively small-scale and non-persistent.

Taken together, the above features of the Internet have raised new kinds of internet cases:

i. Linking and framing
ii. Uploading of copyright material
iii. Downloading of copyright material

- Trademark And Cyberspace

In India chief legislation which deals with the concept of trademark is Trade Marks Act, 1940 this Act was brought on the statute book laying down specific law on the subject which was repealed by the Trade and Merchandise marks Act, 1958 that served its purpose for four decades. However the act of 1958 did not contain any provision for registration of trademark service and definition of the term ‚registration'. Besides this in view of developments in trading and commercial

practices, increasing globalisation of trade and industry, the need to encourage investment flows and transfer of technology, need for simplification and harmonisation of trade and to fulfil obligations of GATT and TRIPS. Trademarks are names and symbols that a company uses to identify its product or service in the marketplace. Trademarks are the law's recognition of the psychological function of symbols. Trademark rights consist of a particular logo, a company name, a unique packaging style etc. Trademarks serve several useful functions. The development of the Internet has brought a new set of challenges of the trademark law of most importance is the interface between trademarks and domain names. Domain name very simply is the address of a particular site on the internet not much different from a telephone number. On the web to communicate with or access a simple specific site, each site must have an address. Internet protocol addresses act as such addresses (Chaubey, 2008). Machines communicating over the Internet however do not actually 'talk' in terms of domain names. Instead domain name is a proxy for the I.P. address, which is like a telephone number, although there is no logical correspondence between the IP number and the domain name.

Domain name disputes tend to fall into four categories –

i. Cyber squatter
ii. Cyber parasite
iii. Cyber twins
iv. Reverse domain name hijacking

i. **Cyber Squatter** - The term, cyber squatter, refers to someone who has speculatively registered or has acquired the domain name primarily for the purpose of selling, renting or otherwise transferring the domain name registration to the complainant who is the owner of the mark or service mark. Sometimes parties register names expecting to auction them off to the highest bidder. As long as a cyber squatter owns the domain name, the trademark owner cannot register his own trademark as a domain name. Thereby, a cyber squatter breaches the right of the trademark owner to utilize his own trademark. It is relevant to note that there is nothing wrong with the practice of reserving a domain name. Often, cyber squatters register words or phrases they hope will someday be sought after by new companies or new businesses. (Muragendra, 2012)

In *Mark & Spencer v. One in a million Ltd.* the defendants had registered as domain names, a number of well-known trade names, associated with large corporations with which they had no connection. Then they offered them to the companies associated with each name for an amount. The English Court held that when a person deliberately registers a domain name in an account of its similarity to the name, brand name or trademark of an unconnected commercial organisation he must expect to find himself at the receiving end of injunction to restrain the threat of passing off.

ii. **Cyber Parasite -** Like cyber squatters, cyber parasites also expect to gain financially, however, unlike squatters such gain is expected through the use of the domain name. In some cases a famous name will be registered by another, in other cases, a mark that is similar to or a commonly mistyped version of a famous name will be used. The dispute might arise between direct competitors between those in similar lines of business or between those who simply wish to indulge in 'passing off' of the name's fame.

In *Yahoo! Inc. v. Akash Arora & Anothers* the Delhi High Court for the first time successfully protected domain name in India involving passing off remedy. In this case the plaintiff is the owner of the trademark, ``yahoo and the domain name yahoo.com". The defendant adopted the domain name , 'yahooindia.com' for similar service. The plaintiff filed a passing off action. (Muragendra, 2012)

iii. **Cyber Twins -** When both the domain name holder and the challenger have a legitimate claim to the domain name then they are known as parties. In *Indian Farmers Fertilizer Corporation ltd. v. International Foodstuffs Co.* the dispute was relating to the domain name 'iffco.com'. The defendants had registered the domain name iffco.com and had been using it with good faith. The complainant had domain names related to iffco.com and had a legitimate interest in the domain name. The complainant had alleged the defendant of diverting the net surfaces to its own web site. However, the Arbitration Centre dismissed the case, as both the parties had legitimate interest in the domain name and the complainant had failed to prove bad faith on the part of the defendant. (Muragendra, 2012)

iv. **Reverse Domain Name Hijacking -** It is also known as reserve cyber squatting. Where a trademark owner attempts to secure a domain name by making false cybersquatting claims against a domain name's rightful owner. This often intimidates domain name owners into transferring ownership of their own domain names to trademark owners to avoid legal action, particularly when the domain name belongs to smaller organisations or individuals. It is preferred by larger corporations and famous individuals. (Muragendra, 2012)

The advent of the Internet is a serious concern in the field of intellectual property rights. The infringement of IP rights over the internet is common nowadays. The present Indian Legislation on cyber-Law does not have sufficient provision to tackle problems relating to IPR and cyberspace. So, there is a need for specific provisions which regulate IP rights in Cyberspace.

IV. ONLINE SEXUAL EXPLOITATION

One of the most witnessed form of exploitation is cyber harassment. **Cyber harassement** which is defined as unsolicited, repeated, hostile behaviour by a person using cyberspace with the intention of intimidating, harassing, threatening or humiliating a person. Any harassment through the use of electronic devices is considered to have the same impact as traditional forms of harassment.

There are different types of harassment some of them have been discussed below. They are prohibited under the Information Technology Act 2000.

Stalking means, to follow a person, to harass or to embarrass that person. **Cyber stalking** is committed using a computer or email. Sometimes it is also done using spoofing, defamation, identity theft or extortions. Stalkers could create fake email accounts or any other online profiles and can send harassing mail, messages or images to stalk another person. In India, it is strictly prohibited under Section 66A of the IT Act. In one case, the accused promised to marry a woman, cheated and exploited her and harassed her. Complaint was filed under Section 66A of the IT Act along with some other provisions of the IPC.

Section 66E of IT Act also provides punishment for those people who intentionally or with due knowledge captures any image or publishes any image of a private area of a person without the consent of that person. It violates the privacy of that person. This illegal act is punishable with imprisonment of up to three years or fine up to 2 lacs or both. Publishing obscene material is also one of the form of crime under sexual exploitation. Section 67 provides punishment for transmitting or publishing obscene content electronically. This act is punishable with imprisonment of term that may extend to three years or fine upto 5 lacs or both.

Similarly, Section 67A provides punishment against acts directed at publishing or transmitting sexually explicit content online. Imprisonment of upto 5 years and fine upto 10 lacs is provided as punishment for this offence.

Child Pornography is also explicitly prohibited under Section 67B of the IT Act. Publishing and transmitting child pornography is an offence and imprisonment of upto 5 years and fine of upto 10 lacs rupees is prescribed under this section. According to IT (Guidelines to Cybercafe) Rules, 2011 cybercafes are required to put up sign board to bring users to notice that viewing child pornography, downloading or copying illegal information is prohibited.

❖ LANDMARK CASES & IMPORTANT INCIDENTS

i. ONLINE SEXUAL EXPLOITATION

- In the case of *Saurabh Kumar Mallick v. Comptroller & Auditor General of India*[6], the Delhi High Court made certain compliances. In this case, an elderly woman officer had made a complaint of sexual importunity against the replier. The replier was facing a departmental inquiry and contended that he couldn't be indicted of sexual importunity at the plant as the contended misconduct had taken place not at the plant but at a sanctioned mess where the woman officer was abiding. The Delhi High Court while stating that this was a miscalculated notion observed that the end and ideal of the formulating the Vishaka

[6] WP (C)No.8649/2007

Guidelines was egregious in order to ensure that sexual importunity of working women is averted and any person shamefaced of such an act is dealt with brutally. Keeping in view the ideal behind the judgement, a narrow and pedantic approach cannot be taken in defining the term 'workplace' by confining the meaning to the generally understood expression office. A person can interact or do business conference with another person while sitting in some other country by way of videotape-conferencing. It has also come a trend that the office is being run by CEOs from their hearthstone. In a case like this, if such an officer indulges in an act of sexual importunity with a hand, say, his private clerk, it would not be open for him to say that he hadn't committed the act at plant but at his hearthstone and get down with the same."

- Another case of significance is that of *Jahid Ali v. Union of India*[7] , the Delhi High Court answered the question of whether dispatches with sexual saturations or depreciatory dispatches transferred on messaging platforms by the employer or colleague to the woman would be covered under the compass of sexual importunity at plant indeed though it happened via online mode. The Delhi High Court stated that transferring sexually coloured dispatches to the Superior Lady Office would be considered as Sexual Importunity at Workplace. These cases show that work is no way confined to the four walls of the office and it's now well accepted that a plant isn't only limited to the physical place of work but goes beyond the physical boundaries of the primary plant or office structure.

ii. CYBER EXTORTION

- In the case of *Ramesh Chandra Arora v. State of UP*[8], it was held that it comprises two corridors as stated over. In the instant case, the accused had been charged with the offences of felonious intimidation by threatening him of the heinous offence of sharing the nude pictures of the daughter if a particular sum was not paid to him. Obviously, the intention was to hang them and beget alarm in their mind. The trial court condemned the indicted under Section 503/506, IPC, 1860 which was affirmed by the high court.

[7] MANU/ DE/7886/2017
[8] AIR 1960 SC 154

- *Elonis v. United States*[9], (2015), was a United States Supreme Court case concerning whether conviction of threatening another person over interstate lines:

a) requires evidence of private intent to hang or whether it's enough to show that a "reasonable person" would regard the statement as threatening.
b) In contestation were the purported pitfalls of violent rap lyrics written by Anthony Douglas Elonis and posted to Facebook under a different name.
c) The ACLU filed an amicus detail in support of the supplicant. It was the first time the Court has heard a case considering true pitfalls and the limits of speech on social media. The court held that the proper legal test for determining whether someone made a trouble is an objective one whether reasonable people hearing the comment would perceive it to be a trouble.

iii. CYBER TERRORISM

26/11 INCIDENT: Mumbai Attack

The date 26th November 2008 was a dark day for witnessing a veritably woeful incident of 12 match firing and bombing that lasted 4 days across Mumbai. This was indeed one of the major cyber attacks of the country. There were ten Pakistani men related to the phobia cluster terrorist group attacked structures in Bombay, killing 164 individualities, 9 markswomen were killed throughout the attacks, one survived. They began their trip from Karachi, West Pakistan to Bombay via boat. Commandeering a fishing giller and killing four crew members and incising the captain's throat. The terrorists thrived in the Bombay megacity quarter close to the hall of the Republic of India monument. They commandeered buses, police vans and used automatic munitions and grenades.

The terrorists used colorful computer and cellphone bias to hack the systems of Taj Hotel, Leopold cafe, Shivaji Maharaj Terminus, Oberoi Trident, Cama Hospital, Nariman House which gave them access to all the data of the hostel and other places. Their targets were the Outsider guests from the U.S, England and other places. The blasts lasted four days. 26/11 was one of the major incidents

[9] 575U.S., 135 S.Ct. 2001; 192 L. Ed. 2d

in our country which made the government apprehensive of the cybersecurity and cyber trouble and what way should be taken for it.

The *WannaCry* outbreak incident

With perfecting computer security ways, worm outbreaks have come rare as it's veritably hard to wangle a piece of malware that automatically executes on a remote machine without any stoner involvement.

In cyber language, the WannaCry was a worm. It was a type of a piece of malware that was suitable to spread itself to be far more dangerous than a normal computer contagion. This kind of worm tone-replicates, bouncing from host to host, and adhering all the rules, growing dramatically and taking off when they infect well- connected bumps through the perpetration of the Garçon Communication Block protocol.

A mysterious hacking group called The Shadow Breakers refocused out a weakness in Microsoft's Windows operating systems that could be used to automatically run programs on other computers on the same network in April 2017. Indeed, with the kill switch active, the outbreak caused huge damage. After infecting Windows computers, the worm translated lines on the computer's hard drive, making it insolvable for druggies to pierce the drive. Along with the loss of access, the malware also demanded a rescue payment in bitcoin in order to decipher them, failing which the lines would have been permanently deleted.

The WannaCry outbreak shut down computers in around 80 NHS associations in England due to which 20000 movables were cancelled, hospitals diverted ambulances being unfit to handle exigency cases. There was a trouble to life, health and major finances due to the malware. It's estimated this cybercrime caused around$ 4 billion in losses across the globe.

It was believed that the U.S. National Security Agency discovered this vulnerability and misused the information by developing a law to exploit it called Eternal Blue rather than reporting it to the Infosec community. Microsoft handed with SMB patches which were released 2 months before the cyberattack, but patchless PCs were still vulnerable and extensively affected by the outbreak. The company claimed it did little damage affecting only a many products machine. Boeing was

suitable to stop the attack and settle back in due to the hype of the attack and the readily available patches by Microsoft.

WannaCry spread like campfire throughout computers across the world cracking hundreds of thousands in further than 150 countries in a matter of hours. It was a first time experience for the world that a malware that encrypts a stoner's lines and also demands cryptocurrency in rescue to unlock them has managed to spread across the world.

This led to serious consequences for the NHS and its capability to give care to cases which could have been averted if the NHS had agreed to follow introductory IT security practices that had been released and handed down. Therefore, there's a need to get the world's act together to ensure that what happened in the case of the NHS is better defended against unborn attacks.

iv. CYBER CRIMES AND IPR VIOLATIONS

- In *Mahindra and Mahindra Ltd. v. Ajay Kumar*[10]the M & M company lodged a complaint against the cyber squatter Ajay Kumar that the latter was using former's domain name 'mahindra.com' and had transferred his original address in India to one in the United States in order to escape the jurisdiction of the Indian Courts. Disposing of the complaint, the WIPO arbitration centre (World Intellectual Property Organisation's arbitration centre) upheld the claim of M & M. Earlier also M & M had to move the WIPO centre for taking back their domain names mahindra.net and mahindra.org from the same respondent (Ajay Kumar) in which they had succeeded. The contention of Mahindra & Mahindra in this case was that the trademark 'Mahindra' had been registered both in India as well as in the United States. The WIPO's penalists decided in favour of Mahindra & Mahindra and held that 'mahindra.com' was identical to the trademark 'Mahindra' to which the respondent had no right.

- In yet another case, namely *Dalgit Titus, Advocate and others v. Alfred A. Adevare and others*[11], decided by the Delhi High Court, the plaintiffs were running a law firm which consisted of advocates specialised in different legal fields. The defendants were working

[10] AIR 2002 SC 117
[11] 2006 (32) PTC 609 (Del.)

with the plaintiff's firm and were paid remuneration while they retained control over the professional organisation. They claimed copyright ownership over the work which they had done while working in the plaintiff's legal firm. The plaintiff's, on the other hand, contended that since the defendants were a part and parcel of the plaintiff's firm, they could not claim exclusive right in respect of database of the list of clients and the expert opinions and advice rendered to them as they were under an obligation to maintain confidentiality.

Consequent to the dispute regarding the copyright ownership, the plaintiffs alleged that one of the defendants came to their office after the office hours and downloaded 7.2 GB of database of their crucial data, write-up. through the plaintiff's local area network and allegedly have stolen the hard copies compressed over ten proprietary drafts of the plaintiffs and therefore, they prayed for protection of their exclusive data under the Indian Copyright Act, 1957.

After hearing both the parties, the Court came to a conclusion that plaintiff had prima facie copyright in the database which the defendants had taken away from the plaintiff's office. The Court noted that the defendants were free to carry on their legal profession, utilise the skill and information they had mentally acquired by experience gained from working with the plaintiff's legal firm but restrained them from copying material of the plaintiff in which the case clearly envisages the need for a careful drafting of different clauses of plaintiffs alone had the exclusive copyright.

- The WIPO Administrative and Mediation Centre's decision in the arbitration case of *Bennett Coleman & Co. Ltd. v. Steven S. Lalvani along with Bennett Coleman & Co. Ltd. v. Long Distance Telephone*[12] Company laid down certain principles of cyber law on domain names which may provide effective guidelines for the prevention of cybersquatting and the related crimes. These principles are:

a) Daily usages of newspaper titles/marks in hard copy or electronic publication leads to a substantial reputation which cannot be allowed to be hijacked in cyberspace by a squatter.

[12] Administrative Panel decision of Arbitration & Mediation Center delivered by Panelist W.R. Cornish of the WIPO on March 11, 2000.

b) According to the principle of presumption, the moment anyone registers a domain name which has the trademark or other mark of any other entity, it shall be presumed that the said person was fully aware of the existence of the said mark at the time when he applied for the registration of the domain name.
c) The website being a "postal address" to other sites, it will be presumed that the defendant is adopting domain name to take advantage of the good reputation of the plaintiff's domain name.

The facts of the case were that the complainant of Bennett Coleman & Co. Ltd. were the publishers of two reputed papers, namely, "The Economic Times", which had an average daily circulation of around 35 lakhs, and the "Times of India", which had a circulation of nearly 1.52 crores per day. Besides, they were carrying out publication of certain supplemental material using the brand name "Times" and held domain names www.economictimes.com and www.timesofindia.com, using them for electronic publication of their respective aforesaid two newspapers.

The complainant was registered in India under the "The Economic Times" and "The Times of India". The defendant, Stevens S. Lalvani, a resident of Lipper Montclair, USA got the domain name www.economictimes.com registered with Network Solution (NSI). He also got the domain name www.thetimesofindia.com registered with NSI for his Long-Distance Telephone Co. having the same address. Thereafter, Steven S. Lalvani and Long-Distance Telephone Co., both built up websites of the two domain names with the result that any net users who legitimately wanted to go to the site of the Economic Times, when typed the same name in his browser, was redirected to the site of the defendant's website and thus resulted in great damage and harm to both the reputed publications of the plaintiff i.e. Bennett Coleman & Co. Ltd. This situation continued unabated until 1999 despite several notices and negotiations with the defendants but the latter did not mend his ways and continued his illegal activity of cybersquatting.

The numbers of cases registered under the IT Act and IPC have been growing continuously. The cases registered under the IT act grew by more than 350% from 2010 to 2020. There was almost a 70% increase in the number of cyber crimes under the IT act between 2019 and 2020.

The cases registered under the IPC increased by more than 7 times during the period between 2010 and 2020. Similar trend is observed in the number of persons arrested. The government also acknowledges the increase in the number of such crimes and that the introduction of technologies, devices including smart phones and complex applications, and rise in usage of cyber space for businesses has resulted in such an increase.

❖ PERPETRATORS OF CYBER CRIME

There are three following categories of people who are involved in committing cybercrime:

1. Idealists (Youngsters)

This category includes the youngsters between the age of 13 to 26 who seek for social recognition. They are usually not highly trained or skilful. Their motive is just to have a spotlight on social media. Most often they attack the systems with viruses they create and that harm negligently on an individual basis but the actions are globally damageable. Also when this age group has matured and understood the weight of their actions, they with the passage of time lose their interest in such activities and stop thereby.

2. Greed Motivated

This category of Cyber criminals can be called the Career Criminals. They are dangerous in nature because they are usually ready to commit any type of crime as long as they fetch money from them. They are also very smart and organised in their actions and they know how to skip the law enforcement agencies. These days such cybercriminals are spontaneously committing grievous crimes and damages particularly like child pornography, cyber gambling, Bank frauds are serious threat to the society.

This also covers the identity thieves who try to gain access to their victim's personal information like name, address, phone number, place of Employment, Bank account, credit card information and other details which they use to make financial transactions by impersonating their victims. And today this practice of Identity theft has progressed in scope and technique to advances in technology that can even be capable of hacking into a government or Corporate database to steal high volume personal information.

3. Cyber Terrorists

These are considered the most dangerous group of Cyber criminals and their primary motive is not just gaining the money but they are also specified in certain causes which can also be politically planned. They attempt to steal data and corrupt the corporate or government computer system and networks resulting in harm to the countries, businesses, organisations and even the individuals. They usually engage in sending the threat mails and destroying the data stored in mainly Government information systems.

The threat of Cyber terrorism is as dangerous as of nuclear or chemical threats. Osama Bin Laden was considered as one of the most wanted Cyber Terrorist who said to use steganography to hide secret messages within pictures. For example, a picture of Amitabh Bachchan posted on the website could contain a hidden message to blow up a building. And the surprising fact to the effect is that these hidden messages do not alter the shape, size or look of the original pictures in any way.

Below mentioned are the NCRB's report on various cyber crime motives:

Cyber Crime Motives - 2020

SL	State/UT	Personal Revenge	Anger	Fraud	Extortion	Causing Disrepute	Prank
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
STATES:							
1	Andhra Pradesh	83	39	1149	56	15	2
2	Arunachal Pradesh	1	0	26	0	0	0
3	Assam	654	164	242	447	85	35
4	Bihar	84	34	1218	102	19	12
5	Chhattisgarh	0	1	75	7	41	0
6	Goa	0	0	25	0	10	0
7	Gujarat	6	31	875	26	203	43
8	Haryana	14	3	157	17	9	1
9	Himachal Pradesh	2	1	19	9	15	0
10	Jharkhand	4	4	1069	14	2	0
11	Karnataka	147	13	9680	74	368	0
12	Kerala	44	34	96	21	58	10
13	Madhya Pradesh	7	6	292	13	66	2
14	Maharashtra	36	105	3413	45	76	32
15	Manipur	0	2	40	0	3	0
16	Meghalaya	6	10	81	7	9	0
17	Mizoram	0	0	3	0	2	3
18	Nagaland	0	0	5	0	1	1
19	Odisha	1	33	1380	175	0	0
20	Punjab	4	19	164	29	19	3
21	Rajasthan	22	10	641	42	73	11
22	Sikkim	0	0	0	0	0	0
23	Tamil Nadu	83	57	134	112	43	7
24	Telangana	96	24	4436	115	3	0
25	Tripura	14	1	11	0	2	0
26	Uttar Pradesh	78	210	4674	1055	547	87
27	Uttarakhand	11	5	98	33	6	0
28	West Bengal	66	8	72	12	3	3
	TOTAL STATE(S)	**1463**	**814**	**30075**	**2411**	**1678**	**252**
UNION TERRITORIES:							
29	A&N Islands	0	0	0	1	0	0
30	Chandigarh	0	0	7	1	0	0
31	D&N Haveli and Daman & Diu	0	0	0	0	0	0
32	Delhi	2	4	23	15	0	0
33	Jammu & Kashmir	3	4	33	9	28	2
34	Ladakh	0	0	0	0	0	0
35	Lakshadweep	2	0	0	0	0	0
36	Puducherry	0	0	4	3	0	0
	TOTAL UT(S)	**7**	**8**	**67**	**29**	**28**	**2**
	TOTAL ALL INDIA	**1470**	**822**	**30142**	**2440**	**1706**	**254**

• As per data provided by States/UTs

TABLE 9A.3 Page 1 of 4

•States/UTs may not be compared purely on the basis of crime figures

Cyber Crime Motives - 2020 (Continued)

SL	State/UT	Sexual Exploitation	Political Motives	Terrorist Activities			
				Terrorist Activities (Total)	Terrorist Recruitment	Terrorist Funding	Others
[1]	[2]	[9]	[10]	[11]	[12]	[13]	[14]
STATES:							
1	Andhra Pradesh	169	67	0	0	0	0
2	Arunachal Pradesh	0	0	0	0	0	0
3	Assam	483	24	0	0	0	0
4	Bihar	32	7	0	0	0	0
5	Chhattisgarh	35	0	2	0	0	2
6	Goa	4	0	0	0	0	0
7	Gujarat	37	3	0	0	0	0
8	Haryana	70	1	0	0	0	0
9	Himachal Pradesh	34	3	0	0	0	0
10	Jharkhand	13	0	7	7	0	0
11	Karnataka	191	18	0	0	0	0
12	Kerala	138	10	0	0	0	0
13	Madhya Pradesh	119	3	0	0	0	0
14	Maharashtra	612	9	0	0	0	0
15	Manipur	10	10	0	0	0	0
16	Meghalaya	9	1	1	0	0	1
17	Mizoram	1	1	3	0	0	3
18	Nagaland	0	0	0	0	0	0
19	Odisha	239	0	0	0	0	0
20	Punjab	58	2	0	0	0	0
21	Rajasthan	67	4	0	0	0	0
22	Sikkim	0	0	0	0	0	0
23	Tamil Nadu	192	108	0	0	0	0
24	Telangana	85	8	0	0	0	0
25	Tripura	3	1	0	0	0	0
26	Uttar Pradesh	560	73	96	0	0	96
27	Uttarakhand	44	1	0	0	0	0
28	West Bengal	44	1	0	0	0	0
	TOTAL STATE(S)	**3249**	**355**	**109**	**7**	**0**	**102**
UNION TERRITORIES:							
29	A&N Islands	2	0	0	0	0	0
30	Chandigarh	7	0	0	0	0	0
31	D&N Haveli and Daman & Diu	3	0	0	0	0	0
32	Delhi	20	0	0	0	0	0
33	Jammu & Kashmir	12	1	4	0	0	4
34	Ladakh	0	0	0	0	0	0
35	Lakshadweep	0	0	0	0	0	0
36	Puducherry	0	0	0	0	0	0
	TOTAL UT(S)	**44**	**1**	**4**	**0**	**0**	**4**
	TOTAL ALL INDIA	**3293**	**356**	**113**	**7**	**0**	**106**

• As per data provided by States/UTs

TABLE 9A.3 Page 2 of 4

•States/UTs may not be compared purely on the basis of crime figures

Source 4: NCRB Report, 2020

❖ CYBERSPACE CRIMES: INTERNATIONAL AGENCIES AND INTERNATIONAL CONVENTIONS

The 21st century has seen the rise of entirely new challenges and one of the fastest growing forms of transnational crime is cyberspace crimes. Cyber security is considered to be an emerging topic in international law today and very pertinent to international security discussions. It is crucially important that civil society have access to a safe and secure internet. Witnessing these challenges, the international community has come together setting up agencies and framing conventions to address the emerging cyberspace crimes.

I. Budapest Convention

The most comprehensive and coherent international agreement on cybercrime is the Convention on Cybercrime of the Council of Europe, commonly known as the Budapest Convention was adopted by the Council of Europe's Committee of Ministers at its 109th session, on November 8, 2001 and was opened for signature in Budapest on November 23, 2001. In 2003, it was complemented by a Protocol on Xenophobia and Racism committed via a computer system. The Convention entered into force on July 1, 2004. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with offences against and by means of computer systems and data, such as illegal access, illegal interception, data and system interference, computer-related fraud, child sexual exploitation material or other violations of network security. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. The Convention focuses on harmonisation of domestic laws of member states and increasing cooperation among them. The Convention was drawn up by the Council of Europe with the participation of its observer states Canada, Japan, Philippines, South Africa and the United States.

The Convention aims principally at:

(1) harmonising the domestic criminal substantive law elements of offences and connected; provisions in the area of cyber-crime;

(2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or electronic means; and
(3) setting up a fast and effective regime of international co-operation.

The Convention provides the 'substantive' and 'procedural' provisions which are needed to be adopted by State parties in their domestic legislations in order to implement the Convention.

A. The Convention provides for four broad categories of substantive offence:

- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related offences
- Content-related offences
- Infringements of copyright and related rights.

B. The procedural law provisions cover:

- Expedited preservation of stored computer data
- Production Orders
- Search and seizure of stored computer data
- Real-time collection of computer data[13]

II. INTERPOL's Response

With the vision of connecting police for a safer world, INTERPOL supports 194 member countries in combating all forms of transnational crime. INTERPOL has five regional working groups for the Heads of Cybercrime units in Africa, the Americas, Asia, Europe and the Middle East. They meet regularly to advise INTERPOL on formulating policies and implementing projects to combat cybercrime.

According to INTERPOL's recent study, criminals are exploiting the fear and uncertainty caused by the unstable social and economic situation around the world due to the COVID-19 pandemic to

[13] National Cyber Security Alliance. http://www.staysafeonline.info/

launch cyberattacks. At the same time, the higher dependency on connectivity and digital infrastructure due to the global lockdown has increased the opportunities for further cyber intrusion and attacks. In June 2020, INTERPOL Cybercrime Directorate's Global Malicious Domain Taskforce identified and analysed about 200,000 malicious domains affecting more than 80 countries. INTERPOL also identified a spike in online scams, phishing, ransomware, data-harvesting malware and misinformation related to COVID-19.

INTERPOL's Global Cybercrime Strategy

Source 5: World Economic Forum

INTERPOL's Global Cybercrime Strategy outlines five action streams, with the common goal of helping member countries to identify cyberattacks and their perpetrators. They are listed below for the members to access the model's strategy:

1. Threat assessment and analysis, trends monitoring: Detection and positive identification of cybercrime, cybercriminals and cybercrime groups through threat assessments, analysis and trends monitoring.

2. Access to and exploitation of raw digital data: Facilitate access to data linked to cyberattacks, and the relevant tools and partners to consolidate the collection of data and enhance its exploitation.

3. e-Evidence management process: Manage digital evidence processing for the purpose of investigation and prosecution: lawful collection of digital clues, preserving the evidence, making it intelligible and acceptable for the court system.

4. Correlation of cyber and physical information: Bridge the gap between digital traces and physical identification so as to identify the location of possible perpetrators.5. Harmonization and interoperability: Improve operational interoperability and global coordination, and encourage legislative harmonization.

5. Harmonization and interoperability: Improve operational interoperability and global coordination, and encourage legislative harmonization.

Source: Interpol

INTERPOL uses 'Purple Notices' to alert member countries to emerging and high-risk cyberthreats, providing technical guidance to victim organizations for their recovery efforts. INTERPOL has been assisting member countries for prevention, detection and investigation of

cybercrime, including the Heads of National Central Bureaus (NCB) and regional cybercrime units, the INTERPOL Global Cybercrime Expert Group, etc. To make the cyberspace safe and secure, INTERPOL launched a Global Cybercrime Programme within its Cybercrime Directorate based in Singapore in 2016. It focused on three core pillars of Cybercrime Threat Response, Cybercrime Operations and Cyber Strategy and Capabilities Development. INTERPOL has the Cyber Fusion Centre (CFC) which brings together cyber experts from law enforcement and industry to gather and analyse all cyberspace crimes and to provide coherent, usable intelligence which can be used to both prevent crime and aid in the identification of criminal. INTERPOL is also developing new cutting-edge policing tools in consultation with private partners in the cyber industry, and new private technologies with a view to their use by law enforcement.

❖ CYBER CRIME CHALLENGES

There are various challenges faced in cyber laws implemented to combat cyber crimes. Some of them here are discussed below:

i. Lack of consciousness and the culture of cyber security, at individual as well as departmental level.
ii. Lack of trained and qualified workforce to implement the effective measures.
iii. Lack of email account policy especially for the defence forces, police and the security agency personnel.
iv. Cyber attacks are occurring not only from the terrorists but also from neighbouring countries contrary to our national interests.
v. The minimum necessary eligibility to join the police doesn't include any knowledge of the computer sector so that they are almost illiterate to cyber-crime.
vi. The speed of cyber technology changes every time it thrashes the progress of the govt. sector due to which it fails to identify the origin of these cyber-crimes
vii. Promotion of Research & Development in IT Sectors not up to the mark
viii. Security Forces and Law enforcement personnel are not trained and equipped enough to manage or handle high-tech crimes.

ix. Present protocols of investigations are yet not completely autonomous or self determined which identifies the investigative responsibility for crimes that stretches to an international level.

x. Budgets for security purposes by the government distinctly for the training of law enforcement, crime security personnel and investigators in ICT are not adequate.

7. LIMITATIONS OF THE PRESENT STUDY

a) Lack of awareness in the arena of cyber crimes and hence availability of limited data.

b) The biggest limitation of our present study is its reliance on secondary data for the purpose of data analysis. So we as researchers do not have any control over the data quality. As the secondary data used in the study is collected by someone else, typically the data can be biased in favor of the person who gathered it. Other than that, the time restraint to complete our study can be definitely seen as a limitation to us completing the study to our very best efforts.

8. CONCLUSION

Cybercrime is inflating at an exponential rate in India and the globe alike. Crimes in Cyberspace inter alia includes intellectual property infringement, cyber terrorism, cyber extortion, sexual harassment, all of which have been analysed thoroughly in this paper with the applicable laws in the context of Indian jurisprudence. The paper also provided a comparative analysis with the Budapest Convention and the Interpol's response to the growth of cybercrimes. International and Indian legal practitioners alike will have to be competent in dealing with a variety of information sources, to conjure new methods of interrogating them, and to be able to utilise the available information in order to provide relevant and proactive advice for their clients. New challenges are presented by the need for security in electronic networks. It is time for Indian legal system to match its pace with the growing cyber crimes and the developing international jurisprudence around it as in the information age, opportunities to grow exist for those who are

best able to utilize both technology and information. With the exodus of information to cyber sphere with the advent of COVID-19 pandemic the need for this change has become more imminent and necessary. Statutory laws, government policies, specialised investigating agencies will go a long way in securing India's cyber spaces. The people ought to be equipped with enough knowledge to be able to defend themselves against the threats of cyber crimes through legal awareness programmes. The future India's digital world lies on a fulcrum and the time to shift the fulcrum towards safety and security vis a vis cyber crimes is now.

9. RECOMMENDATIONS

In view of the expanding dimensions of computer-related crimes, there is a need for adopting appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cybercrime with stern hands. A multi-pronged approach and concerted efforts of all the law enforcement functionaries is much more needed for effective handling of cybercrime cases. A common cybercrime regulatory law universally acceptable to all the countries would perhaps provide a viable solution to prevent and control cyber criminality. It also calls for self-protection initiatives by the people who are vulnerable to cybercrimes. They must have adequate knowledge and awareness about the nature and gravity of these crimes and the dangers fraught by them. Obviously, the media has an important role to play in warning people against the possible dangers and evil effects of cybercrimes on victim(s) as also the nation and the safety measures which are necessary to combat this hi-tech criminality. Some other suggestions to prevent and reduce the incidence of cybercrimes at domestic level are as follows:

1) Technological aspect

a. Intrusion Management

A new preventative strategy called the 'intrusion management 'may be used for testing, discovery and disquisition of cybercrime. It's a process which primarily aims at precluding intrusions in the computer system therefore furnishing effective-security control medium. The computer druggies and e-commerce associations should ensure that functional areas of

vulnerability of the computer system are kept duly controlled so that (i) identification and authenticity, (ii) access, (iii) responsibility, (iv) delicacy, and (v) trustability of data is absolutely shielded. It has been observed that utmost cybercrime examinations end up with the conclusion that the victim's computer system has been damaged due to cybercrime attack but the source of attack couldn't be traced or located. Thus, one of the most important aspects of intrusion operation is to plug the security loopholes so as to render the computer system absolutely safe and secure. The defensive measures contemplated under the intrusion operation system include protection against viruses by using anti-virus strategies, use of firewalls, authentication and encryption technology.

b. Self- regulation by computer and net druggies

Self- regulation may be suggested as one of the practicable results to lead to the prevalence of cybercrime. It's a process of developing a healthy law of conduct by espousing a policy of restraint by both the computer druggies as well as the service providers. Internet Service Providers (ISP) can play a pivotal part barring online crimes by taking some tone-nonsupervisory enterprise. To stan with, ISPS can inclusively set out a ethical law of conduct to be followed by them while extending internet services/ installations to the druggies. Likewise, they can lay down the conditions through a written agreement binding the druggies to refrain from indulging in illegal conditioning. Either, they may also specify the contract that breach of these conditions would lead to termination of the internet services.

c. Use of voice-recogniser, sludge software and collar-ID for Protection

Technology indeed is itself an important tool which has generated crime. Thus, as a first step to help its abuse, the places where computers are popularly used as a means for carrying out routine life conditioning, should be equipped with some safety and security bias to cover against authorised operation of computer systems. For illustration, the ultramodern voice recognition system which relies on voice pattern for activation may be effectively used. So also, anomaly discovery software, which identifies unusual pattern computer use helps the druggies or organisations to respond and frustrate the hacker. Also, sludge software has swung protection against known eats. The use of Collar-IL technology in telecommunication as a defensive assure

may also help in barring e-mail crimes. Analogous technological vices also live to sludge electronic correspondence from unwanted spots.

d. Use of diligent Anti-Virus Softwares

Antivirus software is a computer program which detects, prevents and takes action to protect the system and remove all malicious software programs like viruses etc. They enable the program to download profiles of new viruses so that it can check for the new viruses as soon as they discover them and today anti-virus software is a basic necessity for every system.

Other important measures and suggestions include knowing your network traffic- every organisation has a typical internet traffic pattern. Being aware of the organisation's normal traffic pattern, if any unusual activity happens you can recognize that DDoS attack might be taking place. Practice good cyber habits- regularly changing passwords, secure authentication practices, etc. Utilise cloud- It can't stop DDoS attack but it can mitigate it to some extent by backing up your data. Since the data servers and cloud servers are not at the same place. Scaling up your bandwidth- DDoS creates network jam, one way to avoid it is to increase your network bandwidth. This way the organisation will be able to absorb more volume of traffic, while detecting any DDoS.

2) Legal Aspect

a. Use of encryption technology

It should be obligatory for all government, semi-government and non-government marketable organisations which have resorted to massive computerisation for the transmission of information and marketable deals, to appoint well trained Information Security Officers who should be responsible for overall protection of computer coffers and they should also be made responsible for any lapse in computer security.

b. Use of international treaties & agreements to present a combined front

Presently, cyber terrorism has assumed transnational confines thus, there's need to attack this problem by developing e security technology and espousing strict correctional policy both at the public as well as transnational position. It may be suggested that India should make use of SAARC forum to evolve agreement among the member countries about the need for combined sweats to

check cybercrime particularly cyber terrorism through indigenous co-operation. Sweats should also be made to acquire advanced cyber technology from the developed countries espousing a collective Law of Cyber Legislation.

3) Research Aspect

In addition to all the aforementioned suggestions, we would also like to propose the idea of more detailed and culture based research in the field of cyber crime, so as to curb its menace. Research and innovation in industry and academia will continue to make important contributions to creating this resilient and trusted digital environment. Research can illuminate how best to build, assess and improve digital systems, integrating insights from different disciplines, sectors and around the globe. It can also generate advances to help cybersecurity keep up with the continued evolution of cyber risks.

ABBREVIATIONS

AIR: All India Reporter

ACLU: American Civil Liberties Union

CERT-In: Indian Computer Emergency Response Team

CEO: Chief Executive Officer

DDos: Distributed Denial of Service

FBI: Federal Bureau of Investigation

GATT: General Agreement on Tariff and Trade

GB: Gigabytes

ICT: Information and Communication Technology

Inc.: Incorporated

INTERPOL: International Criminal Police Organisation

IPC: Indian Penal Code

IPR: Intellectual Property Rights

ISAC: Information Sharing and Analysis Centre

ISP: Internet Service Provider

IT Act: Information Technology Act

NCCC: National Cyber Coordination Centre

NHS: National Health Service

MHA: Ministry of Home Affairs

RWA: Ransomware Attack

SAARC: South Asian Association for Regional Cooperation

SC: Supreme Court of India

SMB: Server Message Block

TRIPS: Trade Related aspects of Intellectual Property Rights

UNCITRAL: United Nations Commission an International Trade Law

USA: United States of America

USD: United States Dollar

WIPO: World Intellectual Property Organisation

REFERENCES

- Abirami, A.B. 2020. *Intellectual Property Issues In Cyberspace.* Legal Services India. https://www.legalserviceindia.com/legal/article-3233-intellectual-property-issues-in-cyberspace.html
- Ackoski, J., & Dojcinovski, M. (2012, June). Cyber terrorism and cyber-crime–threats for cyber security. In *Proceedings of First Annual International Scientific Conference, Makedonski Brod, Macedonia, 09 June 2012*. MIT University–Skopje.
- Collin, B. C. (1997, March). The future of cyberterrorism: Where the physical and virtual worlds converge. In *Remarks to the 11 th Annual International Symposium on Criminal Justice Issues*.
- Dr. Farooq Ahmad, Cyber Law in India, New Era Law Publications, Edition 4th, 2011
- Erbschloe, M., & Vacca, J. R. (2001). *Information warfare: How to survive cyber attacks*. New York: Osborne/McGraw-Hill.
- Grove, G. D., Goodman, S. E., & Lukasik, S. J. (2000). Cyber-attacks and. *Survival*, *42*(3), 89-103.
- JN Bagga v Air ltd, AIR 1969 Bom 302
- Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats* (p. 12). Washington, DC: Center for Strategic & International Studies.
- Muragendra .B. T, Copyright and Trademark in Cyberspace, International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012.
- National Cyber Security Alliance. http://www.staysafeonline.info/
- Pollitt, M. M. (1998). Cyberterrorism—fact or fancy?. *Computer Fraud & Security*, *1998*(2), 8-10.
- R.K. Chaubey, Cyber Crime and Cyber Law, 1st ed. (kolkatta: Kamal Law House, 2008), pp712 to 714.
- Schmitt, M. N., & O'Donnell, B. T. (2002). *Computer network attack and international law*. Naval War College.
- Terrorism Questions and Answers : Cyberterrorism Council on Foreign relations. http://www.terrorismanswers.com/terrorism/cyberterrorism.html
- The Information and Technology Act, 2000.

- United Nations Commission on International Trade Law.
- United Nations Office on Drugs & Crime. https://www.unodc.org/unodc/en/cybercrime/index.html
- Vakul Sharma, *Information Technology*, 15 (Universal Law Publishing Company 2013).
- Valeri, L., & Knights, M. (2000). Affecting trust: Terrorism, internet and offensive information warfare. *Terrorism and Political Violence*, *12*(1), 15-36.
- Vatis, M. A. (2001). *Cyber attacks during the war on terrorism: A predictive analysis*. DARTMOUTH COLL HANOVER NH INST FOR SECURITY.
- Washington DC. http://www.csis.org
- A survey on Indian Cybercrime and law and its prevention approach. International Journal of Advanced Computer Technology. [Online] Available: http://jact.org/'volume l issue2/1J0120022.pdf
- Cyber security trends and developments in India 2013[Online] Available:htp:/ptlhb.in/cciciwp-content/uploads/2013/12/cyber-law-trends-and-developments-of-india-2013.pdf
- Cyber security and related issues: comprehensive coverage. [Online) Available:http://cybersecurityofindia.blogspot.in/2014/11/cyber-sccurity-and-related-issucs.htm
- Predictive policing: the future of law enforcement [Online] Available:http/www.nij,gov/journals/266/pages predictive.aspx
- Building a responsible cyber society [Online]Available:http://www.naavi.org
- http://cyberlawsconsultingcentre.com
- Standing committee on Information Technology (2013-2014) [Online] Available:http://164.10047.134/Isscommittee/Information%20Technology15_Information_Technology 52.pdf
- Cyber Regulation Advisor Committe, 5 sept. 2014. [Online) Available: http://deity-gov.in/sites upload_files/dit files/Min-CRAC-5%20Sept.pdf
- http://deity.gov.in/content'eyber-laws
- Relevancy and Applications of Cyber Law in India [Online) Available: http://www.lawyersclubindia.com/articles/Relevancy-and-Application-of-Cyber-Laws-in-India-3587 aspfVo9snCigNmSo