IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security-Modern Era Challenge to Human Race and it's impact on COVID-19

Dr. Sumanta Bhattacharya

Cyber Crime Intervention Officer under NSD ,Associate Member of National Cyber Safety and Security Standards, C.E, Ch.E, Zonal advisory at Consumer Rights Organization

Bhavneet kaur Sachdev

Political Science (Hons) Calcutta University , Post Graduation Diploma in Human Rights, Indian Institute of Human Rights.

Abstract

Cyber crime bloomed from the early 2000s when social media came into picture and people started uploading their personal information on different social media site which resulted in the rise of ID theft , which further resulted in different types of crimes like cyber bullying , child pornography, sexting , online sextortion and the gaming world which has also become a place of cyber crime, where everything happens on a digital platform and there exist no direct involvement , with the advance in technology and the use of Internet of all kind of official and unofficial purposes , simultaneously there has been a rise in cyber crime cases, cyber crime is an unlawful act and it is done using an electronic device. With the rising of COVID-19 situation , a global pandemic we see a rise in the number of cyber crime specially against women and children , in every 10 minutes a cyber crime case is reported ,debit/credit card fraud are at a rise with everything going digital . Today India has 650 million Internet users .

Keywords-Cyber Crime, Covid-19,Cyber Space, Going Digital.

Introduction

Cybercrime is unlawful acts. This affects the computer data or systems. These are illegal acts where a digital device or information system is a tool or a target or it can be the combination of both.

Whenever an act is done with any Ill intention or with Mens Rea, and it is also done accordingly, then we call it an Offence.

To the law, the wrongful act is an offence and to the Society, it's a Crime. So Cyber Crimes are no doubt it is an Illegal Act to the Society and also the state, thus in the eye of law it's offences are punishable.

It's Blessing of the technology that in this pandemic situation all the communications and transactions can be done through the internet without getting direct touch with the Human Society, It also raises the Questions of Law and Justice when a person is being affected or becomes a victim of the Cyber Crimes.

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW made a global framework for the formation Electronic Commerce and being the signatory to it, India with their mutual legal provisions and model of

Law, India Adopted the Information Technology Act.

Now is the Digital Sphere due to increase of the Digital Equipments it is inevitable to amend the existing laws on this regard. It not only influences the E-Commerce laws but also made an Impact on Indian Penal Code, Code of Criminal Procedure, Indian Evidence Act and other statutory acts related to it. So there were certain Changes done safeguard laws in the Dynamic Digital Sphere which has taken place in the last decade. So this way Information Technology Bill was introduced in the parliament and soon the IT Act of 2000 came into force. Slowly due to the rise of the Internet users the Cyber Crime cases started to increase and it has taken a high rate of growth in the last decade.

Similarly the Indian laws were gradually amended according to the necessary changes and it also made various structural changes in the procedural laws also to secure cyber safety and do justice.

Cyber Crime

The cybercrime can also be called as electronic crime, e-crime, information age crime, high technology crime. In simple words, we can say that cybercrime is the type of crime in which there is the use of a computer or digital system to do unlawful or illegal acts. As there is no specific definition of cybercrime given in the IT ACT 2000, its definition may be accepted in a wider aspect. Cybercrime can be committed in two ways – one in which a computer is a target of the cyber attack, and the other is which a computer is used to commit a crime against a person. The alien mark of cybercrime is that the sitting target and the felon will never have a face to face junction

Cyber Crimes are not needed to be committed through online, the Crime can be a combination of both online and offline as well.

Types of Cyber Crime

1.Child pornography

Child pornography also known Child sexual abuse material, is a kind of pornography where children are stunt for the purpose of sexual excite. It is assembled either by direct participation or through sexual violence/assault of a child or called child sexual abuse images.

2.Cyber Bullying

Cyber bullying also known as online bullying where a person is harassed through the medium of an electronic device such as laptop , computer or mobile phones . It can also happen through Text online apps, social media forum and many gaming apps in which people share and get involved .It incorporates , projecting or sharing detrimental content about someone else on an electronic platform.

3.Cyber Stalking

Cyber Stalking involves the use of electronic devices to plague someone , track a person or try to communicate with a person who is showing complete disinterest , Cyber stalking is done by sending e-mails , messages etc . It can target an individual , organization or a group .

4.Cyber Grooming

Cyber Grooming is a process by which an adult tries to build an emotional relation / connection with a young person with the intention of using that person for sexual activities and trafficking .

5.Online Job Fraud

Online job fraud are at a rise with everything going digital , its a fake job scam which aims are stealing personal information about the users .This is very common in cases of work from home job market. It uses false application , false money transaction , false advertisement to get access to an individual data and information. With the global pandemic and lockdown situation , many people have lost their jobs in private sector , and work from home is the order of the hour and everything going online , there has been a rise in online fraud cases with people

looking for jobs online , many people have become a victim of online job fraud.

6.Sextortion

Sextortion is a crime which happens on an online platform where a person is forced or threat to send or share sexual pictures of his or her online or present sexual favours on a webcam .Sextortion can happen on any site , dating apps or even while playing online games.

7.Vishing

Vishing is an electronic fraud in which individuals are mislead by unauthorised entities to provide personal information and finance related information like Banking password ,OTP, ATM PIN etc using mobile phones .Vishing can be done without using Internet also .

8.Sexting

Sexting is the practice of taking sexually picture of yourself typically from a cell phone and sending it to someone , it also includes steamy text messages.

9.Smshing

Smshing is an artifice that uses the tool mobile phone to send text messages, pretending to be from well respected companies so that individuals are convinced to disclose their personal information such as credit card or debit card details , ATM PIN etc.

10.SIM SWAP SCAM

SIM Swap Scam is a type of subterfuge where the attacker intention is to get hold of your personal information , so that they can get access to your bank account. It is a kind of buyout account fraud generally aims a fragility in two-component validation and two-pace confirmation .

11.Debit/credit card Fraud

Debit or credit card fraud refers to the unlicensed utilize of credit and debit card or alike payment tools to illegally obtain money or property. Credit or debit card number can be acquired through unsecured websites or through the identity theft scheme.

12.Impersonation and identity theft

Impersonation and identify theft refers to an artifice where a person uses other person's personal information such as password , electronic mark for economic purpose.

13.Phishing

Phishing is a kind of cyber attack that uses email as an instrument to gather personal/ sensitive information of a user like bank account details , password. The aim is to mislead the beneficiary through mail saying that this message will provide them maximum benefit bu downloading a link or attachment .

14.Spamming

Spamming happens when a person accept an unsought trade messages by email, SMS, or any other alike electronic means . They may try to coax the beneficiary to purchase or avail a service, or visit a website by which can try to ruse him/ her into imparting bank account or credit card details.

15.Ransomware

Ransomware is a kind of malware that encodes a users files, designed to block or limit the users access to his or her system until you pay an amount as ransom .

16.Virus, worms and Torjan

Computer virus is an application to enter into your computer or laptop to damage files and data and then replicate themselves.

Worms are destructive programs which spread copies of themselves from one computer to another and can replicate themselves without human involvement and does not require to connect themselves to any software to cause damage .

Torjan horse or Torjan is a kind of software which is planned to destroy , disarrange or steal or impose some harmful exertion into your data or network.

17.Denial of Service Attack

Denial –of-service attack is a cyber attack by which computer and other devices becomes unavailable to the intended users by interrupting the device's functioning . DoS attacks functions by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed .A DoS attack is characterised by a single computer to launch the attack.

18.Data Breach

A data breach is a security occurrence in which data can be obtained without sanction.

19.Website defacement

Website displacement is an ambush on a website which changes the perceptible image of a website or a web page. The attacker might try to upload sensitive images , videos etc on the web page.

20.Online drug trafficking

Online drug trafficking means selling and purchasing of drugs on an electronic platform ,Drugs are traded on the dark web , using cryptocurrency

21.Espionage

Espionage or spying is the process in which you get access to the user's data and information without their knowledge .

Being a vast sphere, this cyber crimes and its procedure to lodge a Fir is quite complex and this results a confusion to the victims to understand how to lodge a complaint or Cyber Crime FIR. Unlike general FIR Procedures that is lodged at police station, the Cyber Crime FIR procedure is lodged at Cyber Cells in various cities all around India. The first city to register a Cyber Cell was Delhi, there after Visakhapatnam, Chennai, Hyderabad, Bangalore and lastly Kolkata. The Cyber Law has a Global Jurisdiction, that means if a Person has suffered a Cyber Crime at his Place at Bangalore but presently he is at Kolkata, he can complain at Kolkata and it shall be sent to Cyber Cell of Bangalore and FIR will be lodged there.

India's progress towards a vision of Digital India is also a Very Important factor that has taken a 'J' Curve in the growth of the Internet users in India. This began with the demonization in 2016 and a huge number of people started to use the Online Transactions in a one night wonder. Gradually Online Applications and Transactions started to increase and people started to connect their online businesses with the online platforms. The growth rate continued with the availability of affordable handsets that started to sale along with the affordable data packs. Today almost 650 Million Internet Users are in India.

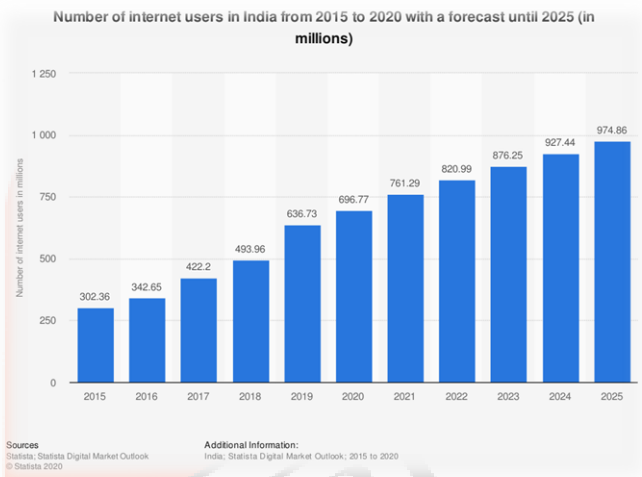

Figure 1 : Number of Internet users from 2015 to 2020.

Thus there is vast number of User of the Internet who uses the Internet for the Business that saves the Rent of any Store and the other Charges for a Shop that needs any Physical Existence. This also created a possibility of Cyber Crimes that takes place with the users, not only in Economical aspect but also in Social Aspects also.

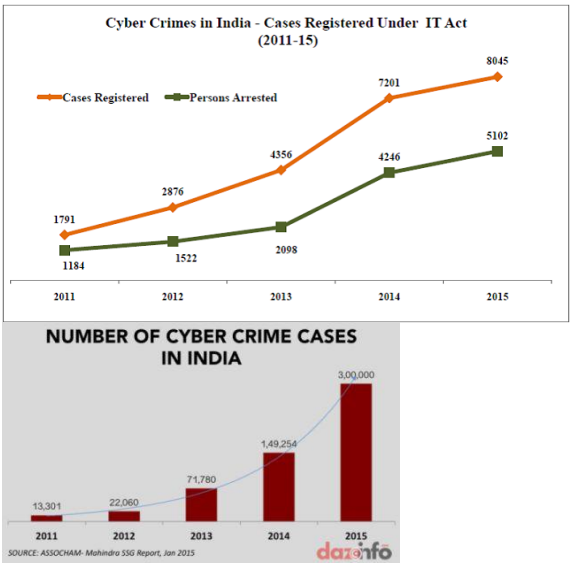

Figure 2 and 3 : Show the rise in cyber crime cases from 2011- 15

In a Study it has been found that in India after 2016 one Cyber Crime is reported in Every 10 minutes. The Cyber Crimes against women and Children is also rising. Thus Cyber Cells are developing their sphere and under Section 150 of the CrPC , the Global Jurisdiction of Cyber Crime features to lodge a complaint in any nearest Cyber Cell of the Victim, no matter from where the offender's I.P. Address belongs, the police officer shall transfer the matter to appropriate Cyber Cell.

The COVID Situation necessitated the growth the Internet Users and Online Transaction. For the first time ever, the whole world is doing Online Meetings irrespective of Government and Private Organisations. The Online Classes and exams are also being taken officially. All these things made increase on the Rate of Cyber Crimes in the whole world including India. These Cyber Crimes are not only limited to Civil matter but also Criminal and International matters as well

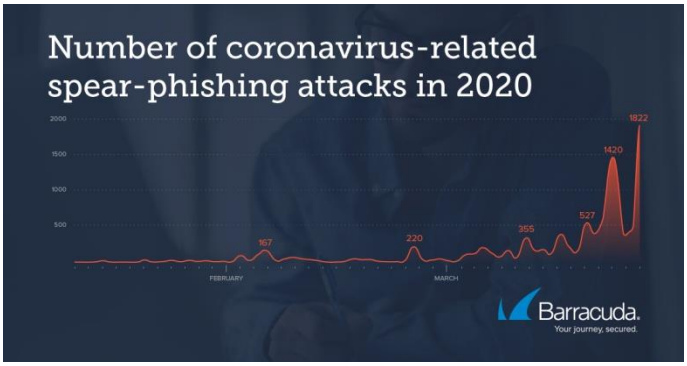

Figure 4 :Diagram shows rise in cyber crime cases during COVID-19

Covid and rise of cyber crime

After the rising of the COVID situation the Cyber Crimes tent to rise in India as the Internet users are using more and more Internet facilities for the purpose of " Work from home" and to keep themselves connected with Social media in order to socialize and keeping alive their creativeness and social interaction that maintains the motto " Stay home, stay safe" This has led to the magnification of Online businesses, meetings and online classes which has resulted in the mandatory use of Internet by Childrens.

All these factors creating a situation that giving internet access to minors and other digitally incompetent persons who have less awareness and knowledge on the Technical and Internet material.

This is no doubt a high time for Hackers, Cyber Terrorists, and Cyber offenders to commit various kinds of Cyber Crimes in huge numbers.

The rate of Cyber Crimes was eventually rising up to 86% during March April of 2020 after the Lockdown Effect of the COVID Issue. The Cyber offences are quite becoming creative in nature also like Fake Fundraising links that appears behalf of the Government, Fake News that Offers or gives access to Corona Virus safety tips, Fake Job offers, Fake Flash Sale offers, Fake Recharge offers of Data Packs and Free Internet with unlimited calling offer, Fake Apps etc. Beside these Civil misconducts, there are Criminal Acts as well like Sexual Offences through internet against Women and Children. The more untrained users are having compulsory access to the internet, the more they are being

affected. All these factors have resulted a huge rise to Cyber Crimes during the COVID situation and the rate is still increasing.

Here are some types of Offences faced by Internet users in India During COVID19 :

Increase in phishing attacks:

During this COVID Situation, the Phishing attacks rate increased. These Emergency situations, Lockdowns and other serious matters became created Confusion to the public that they are scrammed by fake apps and Fundraising Links. The more people are being engaged with Charity or Religious institutions and NGOs, it is also creating more confusion and trusts with such links to the common people. Since January 2020, one of INTERPOL's private partners, Trend Micro, detected 907,000 messages linked to COVID-19 . Taking advantage of the economic downturn and people's anxiety during the pandemic, cybercriminals have enhanced their social engineering tactics by using COVID-19 as a basis in their attacks

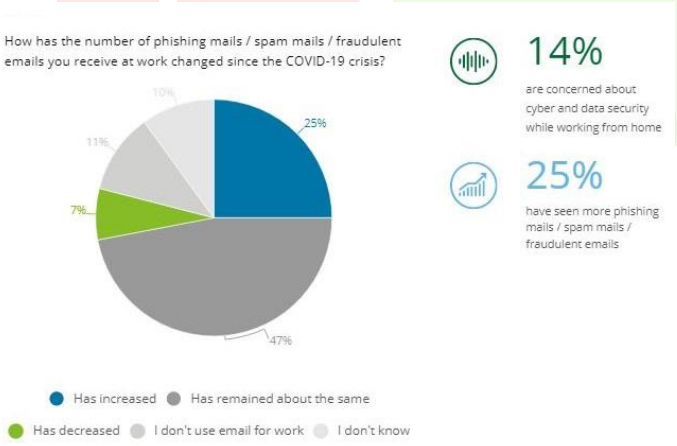

Figure 5 : Increase in Cyber Crime cases over the years especially during Covid-19

Fake Job Offers and Frauds:

During this COVID Situations a huge mass of people lost their jobs especially in the Private sector, they anxiously were searching for new jobs and facilities like earning money from home. Beside the jobless, there were many unemployed people including women and students who were looking for new jobs especially OnlineJobs and earning opportunities they faced so many Fake Job Offers and Frauds that resulted to a huge loss of money.

Fake News or Rumours:

With fake job offers and phishing, there have been large numbers of fake news as well. For example, the fake news of "Chicken carrying Corona virus", Hot water treatment of Corona at home etc.However, some of the measures were taken by the government specifically in a few regions. The Whatsapp Messages that used to contain any word relating to Covid-19 used to be tracked and the Group Admins were held liable for spreading fake news in some cases. The fake news relating to Corona Virus was taken very seriously and specifically in Hooghly the Internet Connection was banded for a few days to stop the spread of fake news and other fake data relating to COVID and lock situations. It was also taken into action just to stop the Rumours relating to community clashes. But however, in spite of these efforts to the spread of fake news, it failed

Fake treatments and Fake Anti-Corona Medicines:

One of the most irritating contents that were ever shared and spread in Social Media and Online selling website that is fake treatments and anti-COVID medicines that would have been able to cure any person of the corona by boosting up the immune system. Various Popular brands were also engaged in such things against which legal action was taken later on. This resulted in fraud in the medicine business and those who were engaged with it were legally charged.

Sexual Crimes against Women and Children:

The most burning social problem during COVID is the Cyber Crimes that are faced by Women and Children. The COVID Situation necessitated the Online Classes that are taken by Female teachers to the minors and Students who are not well trained in the Online Platform.

It has been seen in many recent cases due to the Excitement of adolescence psychology of the teenagers they have engaged themselves in sexting and sharing their private photos. Although it is a consensual act, those contents were misused in pornographic show business. There are examples of many cases where the children have been brainwashed to share the Debit Card Pin code or OTP that is received by the device they are using during class. Several Children's games are there on the phone which uses the children to expose them and share the OTP or passwords. The Phones are also being used as a device for tracking, kidnapping, and Black mailing.

Infodemic breakout in Social Media :

The Term Infodemic means a massive spread of any information irrespective of true or false that takes place in a short period of time relating to a particular interest or subject.

During the COVID Situation, there were more than 361,000,000 Videos were Uploaded on Youtube relating to COVID and 550 million tweets included the terms Corona virus,

COVID-19. etc. Besides these millions of rumours, Videos and written information were shared in Whatsapp relating to COVID and Lockdown. All these factors created a Confusion in Social Media Users who does not even know how to verify this information. This was one of the worst examples of infodemic ever seen.

Violation of the Right to Privacy :

To track the COVID Infodemic situations through the internet and Social Media, the Government launched various policies that shall track the Information shared through social media by the public. However, it raised a Paradoxical Situation that violated the Right to privacy as well. Right to privacy is a Constitutional Right of every Citizen of India, the exception of the right came in to force when the government started to trace the Personal Data of the devices and also launched various apps for public services that used to have access to Contacts of every smartphone. The Violation of the right to privacy was not limited to the government and public, there were so many hackers and specially programmed Apps that used to share information and personal data of smartphones through its hidden access features. So many women were harassed sexually as their images were used in pornographic purposes and the hacking of Phones and unauthorized money transactions had been very common.

Business-related frauds :

As the online transactions and Social media became very popular during the COVID situation, it gave rise to a huge number of Internet users as well as Consumers. There were a huge number of cases of fraud relating to business. Some of these examples are:
Online Education Applications Scams, Supply Scams, Counterfeit of Drugs, Covid19 Testing and Treatment Package Scams,Duplicate Products related Scams, Healthcare Service Scams, Charity, and Investment Scams.

All these types of Scams raised a huge number of Business related Scams most of which resulted to frauds.

Online Gaming and gambling-related frauds:

During this COVID situation, it was a golden opportunity to get rich by playing gambling online. This resulted in a huge number of frauds that were found fake and many games were related to this gambling which affected a huge number of internet users. These types of frauds are nonjusticiable and illegal itself, that's why the victims were helpless.

Other types of Crimes during Covid:

Besides the above-mentioned crimes, there were few more infodemic kind of crimes that affected so many internet and social media users some of the examples are:

A. Aadhar Card Update related frauds,
B. KYC Update related frauds,
C. Pan Card Linking related frauds,
D. Banking related online frauds,
E. ATM card related frauds,
F. SMS Spoofing,

All these types of social-economical or business-related factors resulted huge numbers of cybercrime cases during the COVID Situation.

Dark Web

The dark web is an untouched part of the internet in general that normal internet user does to have access to it. But the untouched area of the Internet world has a lot to do with cyber crimes as those areas of the internet deals with various illegal activities both in respect of the internet and society. This untouched area of the internet is known as Dark Web. There is no specific data that shows how much users are engaged with such activities but one thing is for sure that it exists and cannot be banded for its illegal activities.

The dark web is not discussed in Legal Researches and Legal Discussion as It is ambiguous matter to itself. There is no exact process to have access to this part of the internet and there is no specific website or procedure to work with it.

It is an Eco-System itself as it has its own Economical Currency and process of business. Mostly it deals with illegal and mysterious activities like selling Human Flesh, Child Pornography, hiring of serial killers, Hacking activities targeting the government websites, selling of arms and drugs, Human trafficking business, etc.

Dark Web runs on Tor Browser and the websites are encode .There are other encryption tools and corresponding browsers such as I2P (these are not universal, by design) and you have to know the exact URL in order to access the site like onion is a section particularly used on the dark web.

Another coating of invisibility is the method of payment. Silk Road, for example, only accepted payment via Bit coin, which is an unregulated crypto currency. As with the Dark Web generally, there's nothing illegal about using Bit coin. But the anonymity of Bit coin payments is attractive to those making illegal transactions.

This Dark Web helps to commit various offenses to international Criminals. The secret societies use this Dark web to communicate their tribe members. Various Dark Web Activities has been arrested by the laws in various parts of the world, for examples:

Any type of crime with covert transactions, whether it involves drugs, money, or even human beings, can be committed on the Dark Web, some of the crimes include Murder for Hire, Blackmail/Extortion, Illegal Drug Sale, Illegal Arms , Sex trafficking and Terrorism. There has been a rise in dark web crimes over the years and this COVID-19 has provided dark web with the opportunity to gain as much as possible on a global scale .

Conclusion

Cyber Crime is an amplified topic , with the advance in technology we see an increase in the number of cyber crime cases. After the rise of the COVID-19 situation , the rate at which cyber crime tent to increase as Working from home has become the need of the hour for economic gain . Every incident is taking place on a digital platform .The reliance on technology has amplified since lockdown all over the world and we see a rise in cyber crime cases globally . Online traffic has soared due to continuous video conferences, online classes , meetings etc. We have also seen an increase in the mode of payment which has gone online and the uses of apps like paytm , google pay and phonepe for money transaction which has increased the cases of bank frauds, SIM SWAP Scam to a great extent .Now that everything is being done only both official and unofficial work using laptops and computers. Hackers are creating virus and fake website which can directly attack the system and trap the users , there has been a rise in phishing , hacking at companies and offices ,

cyber bullying , debit and credit frauds and many other cyber crimes are taking place in India. There are many cyber laws existing in India , The Information Technology Act 2000 , which deals with cyber crime , cyber laws and provides remedies and punishment.

The Cyber Laws and Policies in India have various loopholes in respect to their implication in various sectors. The Vision of Digital India also Includes Cashless Economy that means all the banking and E-Commerce Transactions shall be done digitally through E-Banking, Net Banking, and Online Payment, etc. However, in this Present Situations, there are many loopholes in the Cyber Laws and Policies that are needed to be looked upon. In many cases, it has been found the Apps which used in the Online payment, net banking, and other Digital Platforms take access to SMS, Debit Card details of the customer by which the Bank Account details are passed on through the Apps without leaving any mark. For the first time ever in the world, Pornography has gained popularity in public without any Charge and that is easily available over the internet. Porn websites have the largest growth in the Digital Economy. However, Pornography is compromised of Legal and illegal provisions. The most obsessive nature of those Websitesare that in most cases cannot do the Age verification of the visitors. Although the publication of these pornographic contents Social media is illegal however it is not quite effective in practice. , Child pornography is strictly banned and illegal all over the world but due to lack of legal Sanctions, the high consumption of the internet, lack of taxation, lack of security provision the pornographic contents remained uncontrolled obscene publications all over the world. There are potential cyber security challenges like lack of cryptographic measures , poor encryption key management , non-existent secure devices on boarding services, weaponized machine learning technologies by cyber attackers , lack of knowledge of social engineering and insufficiency anti-malware software , DDoS attack . We require a strong cyber security system in India and we need to make strong policies and laws to control the rate of cyber crime in India and the development of more cyber cells in every city and state.

References

1.Sarfaraz Shaikh , June 19, 2020 ,Cyber crimes go up in lockdown .

2.Inhof Robert, “Cyber crime and Telecommunication law “(2010). Thesis .Rochester Institute of Technology .

3.Melissa E. Hathway and John E.Savage , Stewardship of Cyberspace (2012), Cyber threats and cyber realities:Law , policy, Regulation in Business , the Professions and National Security.

4.Sushant Kulkari , May 20,2020 , In Maharashtra , 400 cyber crime cases filed on covid issues , mos on hate speech and communal accusations.

5.Press Trust of India , Kanishka Sarkar , June 28,2020 Business e-mail compromise most common online fraud : Delhi police.

6.Ministry of Communication and Information Technology, cyber crime,cyber security and Right to privacy.

7.A.R Raghavan and Latha Parthiban , The Growing case of cybercrime and types of cyber crime on a Global Scale.