INTERNATIONAL JOURNAL OF INTEGRATED LAW REVIEW

Volume 2 | Issue 1

2021

Cybercrime in the Times of Covid 19 Pandemic

ABHINAV SHUKLA[1]

ABSTRACT

In an effort to combat the Coronavirus pandemic, cities around the world have been shut down, compelling people to stay at homes. People are largely reliant on Internet services for social connection, shopping, leisure, and, of course, work as their mobility is limited. Governments all across the world are using digital media to communicate with their constituents. All of this increased online activity gives cyber criminals exactly the sort chance they're looking for to launch cyber threats. Attacks on health-care institutions, hospitals, and medical institutes are on the rise. Also the WHO's computer networks are more prone to hacking. The proliferation of Corona virus is being used by cyber thieves to launch a range of destructive attacks. Spear phishing, corporate email breach, malware, ransomware, and fraudulent websites are among the attacks, as per Trend Micro, a cyber security firm. In this article the author has highlighted the evolution of cyber-crime in India and the rise of cyber-crime amid Covid-19. In this article the ways to detect cyber-crimes have been detected and how young adults are impacted. The author has also shown light on the state responsibility in curbing cyber-crime.

Keywords: *Cyber-Crime, Social Distancing, Covid-19, Pandemic, Online, Companies.*

I. INTRODUCTION

The spread of the novel corona virus pandemic (COVID-19) around the world is generating exponential fear, but health risks are not the only curse resulting from this disastrous event. It has been observed that this era of social distancing and disinformation also provided opportunities for dark elements in society.

Cybercrime and Corona virus: There has been an influx of fake apps, domain names and websites that take advantage of two facts: first, the fear of the public and their search for information about this pandemic and secondly the companies around the world. The world is migrating to “work from home” via the online environment. Let's tackle the two scenarios individually.

[1] Author is a student at Ajeenkya D.Y. Patil University, Pune, India.

Anyone trapped in their home in the middle of this blockade is trying to stay up to date on all COVID 19-related information and stay away from the infected. Malware authors take advantage of this situation.

One of these apps available in the Google Play Store was "***Corona Live 1.1***", which is said to be a live monitoring tool for corona virus cases. Users of the app thought they were watching the pandemic, but the malicious app invaded their privacy and gained access to photos, videos, a location and a camera. The information collected can be used in many ways to compromise your bank accounts or even blackmail the owner of photos and videos.

To stop the growth of fake apps, the Android play store has removed many of these apps from the play store, set rules for these types of apps, and placed all of these apps in the Sensitive Events category.

The apps are now available on fake websites like coronavirus app site, which has the link to download the app. These cases sufficiently show the increase in cyber crime as a result of the corona virus.

Every organization, big or small, is forced to work remotely because of the block. This poses an increased security risk, as proprietary data can be accessed by laptops and PCs, which can have the same firewall and the same level of security as a desktop.
You may have noticed that the number of emails in the spam folder claiming to be an indication of COVID-19 has increased. These emails trick the user into opening malicious attachments and, once opened, the malware author can gain access to his system.

Because malware attacks one of the systems, there is a potential risk that the security of your colleagues' systems will be compromised. This can affect the entire network of systems to which the organization remains connected and massive loss of sensitive data can occur. This has led to an increase in cybercrime cases following the outbreak of corona virus in India and around the world.

In these cases, organizations may rely on the ISO / IEC 27000 family. ISO / IEC 27000 a global reference certificate issued to organizations following the Information Security Management System (ISMS). An ISM not only improves the structure and direction of organizations, but also protects your confidential and your customers' data from cyber attacks.

II. THE EVOLUTION OF CYBER CRIME IN INDIA

(A) Historical background (Varsha, 2020)

Cybercrime, as the name suggests, is a form of crime in the cyber world. This crime is a new type of crime that has its roots in almost all aspects of internet life. In our Indian law, cybercrime is not defined as such, but a law has been passed to combat this type of crime which we refer to as the Information Technology Act, 2000[2].

The term cybercrime is very broad and therefore cannot be defined in one or two sentences. However, if we look at the nature of this crime, we can say that it is the type of crime that uses, or more precisely abuses, computers and computer networks, and the crime is committed by or "for" them. According to IPOs study, the incidence of complaints filed by Indians is much higher, 32% higher than in the US, UK and other technologically advanced countries where it only varies by 11 to 15%. They are for litigation, but for undisputed cases.

One of the main causes of such rapid growth in the cybercrime business is our addiction to the most basic things like groceries, payment, ordering groceries, etc. that we will definitely benefit from.

The first cases of cybercrime in which young people were known to use the telephone occurred in the 1870s. In the 1990s, the Internet was considered a unique medium with the fastest speed in human history and an increasing dependence on technology. The first cybercrime took place in 1992, causing the first polymorphic virus. One of the first cybercrime incidents in India was Yahoo v. Akash Arora[3].

That case occurred in 1999. In this case, Defendant Akash Arora was accused of using the trademark or domain name "yahooindia.com" and filed for a permanent decree. The other case is that of Vinod Kaushik and the ors. vs. Madhvika Joshi and ors[4]. It has been found that access to the e-mail accounts of your spouse and father-in-law is prohibited without your permission under Article 43 of the Information Technology Act, 2000. This case was decided in 2011. All these matters are related to the development of criminal cybernetics, especially with regard to the developments in India.

Eventually, as social media became more popular, cybercrime rates began to rise as criminals had easier access to the user's personal life. With this development, one of the most barbaric forms of crime emerged, namely the non-consensual sharing of intimate images (NCSIA). According to the National Crime Registration Body, 569 of the 5,987 cybercrime incidents were motivated by sexual exploitation in 2015-2016. In these cases, obscene photos of the

[2] Information Technology Act, 2000 Act No. 21 of 2000 (India).

[3] 78 (1999) DLT 285.

[4]Vinod Kaushik & Another **v/s** Madhvika Joshi & Others, https://www.lawyerservices.in/Vinod-Kaushik-and-Another-Versus-Madhvika-Joshi-and-Others-2011-06-29.

victim are posted on the Internet without the person's consent. It is also referred to as non-consensual pornography.

The penetration rate of these images on the Internet has increased by 104% in recent years, according to the NCRB[5] report. Most of these cases go unreported, mainly because they do not want their families to invade or intervene in the police or the courts, and the victims will continue to pursue these cases. . Blame the victim. Criminals know these facts and use them. It is a crime that can hurt anyone who suffers it, whether it is a big celebrity or just a girl, as was the case of the actress Bella Bella Thorne recently. This is a big issue to worry about, especially in India, as there are no specific laws to address these crimes. Probably because most cases have not been reported, parliamentarians are not yet aware of the seriousness of the crime. If such a case arises, the Indian Criminal Law (IPC) and IT law have few provisions to help process these cases.

(B) From Landline Hacking To Crypto Jacking. (madson, 2019)

Cybercrime has to evolve, of course, to survive. Not only are cyber security professionals constantly striving to close the loopholes left by hackers and prevent zero-day events, but the technology itself is constantly evolving. This means that cyber criminals are constantly creating new attacks to respond to new trends and adapting existing attacks to avoid detection. To understand how cyber crime might develop in the future, let's look back to understand how it originated in the past.

The origins of Internet crime lie in telecommunications, the "hacker culture" as we know it today from the "phreaking phone" that reached its peak in the 1970s. Phreaking was the exploitation of weak points and frequencies devices in a telephone network. , often to benefit from free or reduced telephone tariffs. As wired networks got smarter about security and then fell out of favor, phone calls became less and less common. But he was not completely eliminated. In 2018, a bystander carried out a series of horrific attacks on New York's Wi-Fi hotspots to remind us that a rock was overlooked but certainly wasn't gone.

(C) CryptoJacking: The Cutting Edge? (madson, 2019)

Cryptojacking[6] is the process of embedding JavaScript code on a website, which can use the processing power of all devices visiting that site by using the device's processors to determine the host's crypto currency. This resource theft shrinks systems, but is often stormy enough to go unnoticed which makes it very attractive to hackers. The number of crypto jacking URLs

[5] *National Crime Records Bureau,* https://ncrb.gov.in/ (last visited May 27, 2021).
[6] *Norton life lock Employee*, NORTON (https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html

detected doubled between September and December 2018, and crypto jacking attacks officially outpaced the spread of the ransom ware.

"Crypto jacking is virtually free and has a much less illegal footprint," Moffitt said. "When criminals use the victims' hardware (CPU) and performance to encrypt me, the rewards are excellent. Despite the volatility of the price of cryptocurrencies, large campaigns can generate hundreds of thousands of dollars in just a few months. It is estimated that over 5% of the Monero crypto currency in circulation is the result of illegal mining. "

Until recently, a crypto currency mining service called Coin hive was responsible for 60% of all crypto currency attacks. Coin hive announced in early March 2019 that it will end the service. This is by no means a death sentence for crypto jacking - competitors are already competing to bridge the gap, not to mention finding new ways to deviate from existing crypto jacking techniques.

III. TYPES OF CYBER CRIMES IN TIMES OF COVID-19

There were mainly three types of cyber crimes at the time of COVID-19:

2.1) Virus Attacks.

2.2) Phishing Attacks.

2.3) Fake News or Rumors.

(A) Spyware, Malware, Ransom Ware and COVID19 – Virus Attacks (Deewan, 2020)

During this embargo period, people are more likely to access social networks like Instagram, Facebook, Twitter etc., watch films and series, and subscribe to web channels like Netflix, Amazon, HotStar, Zee 5 etc. You can also indulge in online games by installing various applications. All of these activities are accepted over the internet. People typically provide access or consent to personal information available on their phones, laptops or social media accounts in order to use the apps' services. Users can often use financial information to buy apps or access online services. With the government's notification of "stay home, stay safe", people are increasingly relying on multiple payment gateways to replenish their bills, rewards, cell phones, and purchase medicines and supplies. Online and enjoy others online. All of these activities open the door to spyware and rescue software attacks. Spyware steals a user's sensitive personal information, while rescue software supports person authentication and other critical credentials. These attacks can cause tremendous losses to people, not just financially but in other ways.

To prevent such attacks, various authorities suggest countermeasures and healthy practices

that can be followed. Protected operating systems and applications regularly send updates to their users to fix security vulnerabilities and provide additional security. Cyber-attackers have attempted to reach hospitals and large medical facilities in 194 countries including India in order to obtain information about COVID 19 through rescue and software programs, according to a recent report by the International Criminal Police. Almost 22 malware were discovered in India. It is therefore important to protect mobile devices, computers and applications, install anti-virus systems, and make the necessary security settings to avoid the loss or compromise of sensitive data.

(B) Phishing Attacks: Banking Frauds, EMI Moratorium Frauds (Deewan, 2020)

Currently, banks operate with limited resources and it is recommended to use the Internet or telephone banking service to obtain banking services. Cyber attacks make calls or send phishing emails or text messages to bank customers who pose as bank employees and request confidential information, such as account number, credit or debit card number, CVV, OTP, etc. Recently under COVID 19 As part of the Reserve Bank of India regulatory package, banks are granting a moratorium by delaying the payment of EMI / term loans and interest / working capital interest for three months from March 1, 2020. Also cybercriminals target contact debtors now as an excuse to discuss postponing EMI payments and ask them to share an OTP, CVV, password or PIN code linked to their accounts so they can use the moratorium feature to file a claim. Therefore, do not click on links, open email attachments from trusted sources or divulge confidential information.

(C) Fake News or Rumors (Deewan, 2020)

Another big problem is fake news or rumors that spread quickly across the country. Some examples of rumors and their side effects are discussed below. In March, misleading social media reported that "chicken is a carrier of the corona virus" has cost the poultry industry an estimated loss of Rs 1.6 billion a day. In another case, an audio clip went viral on social media claiming vegetable vendors licking / spitting vegetables to spread the corona virus. Eventually, the government intervened and issued a statement claiming the audio clip was forged. There was another rumor that the Supreme Court advised the government to restore 4G internet to J&K within 24 hours. A false document in this regard was circulated by social networking sites that looked like an original court judgment. There are also rumors that the government will cut the pension by 30% during the lock-up period. Several rumors about the COVID19 virus were found to be false as well, aimed at creating tension or anxiety in humans. A false message is circulating that a treatment for COVID 19 is being processed.

Not only are such messages unethical, but they can also have serious consequences.

With the number of fake news growing, the cyber police in Maharashtra and Karnataka have decided to take action against anyone who finds misleading and unconfirmed information about COVID-19 on social media. It was also decided that in such a case a person who shares false information about the application groups, the "group administrator" is personally responsible for that content in his group and will be punished according to the law. The Indian government, social media and police are taking action to stop the spread of rumors. The Government of India has launched a Chabot on WhatsApp to answer user questions, ask frequently asked questions, and reduce rumors about the corona virus pandemic. Facebook has also launched a similar Chabot for India that will help check out fake news and limit the spread of rumors.

IV. IMPACT ON YOUNG ADULTS

Today's teens are Generation Z, young people born and raised in a new era of technology who cannot imagine an offline world without access to the Internet or social networks. From an early age he juggles between computers, tablets and smart phones, the accessories he uses every day. Together, the data also shows that cybercrime is attracting and reaching more and more young people.

A survey by the UK's National Crime Agency (NCA) found that 61% of hackers identified in the country start working before age 16. In 2015, the Bureau of Crime Statistics and Investigations reported that cyber fraud crime was committed by people under the age of 18, with an increase of 26% over the past two years and 84% over the past three years. In a recent survey by an online security company, around 1 in 6 teenagers in the US and 1 in 4 in the UK said they had tried some form of internet hacking.

(A) Why Are Teens Engaging In Cybercrime Activities? (AYLING, 2019)

Nowadays, it takes fewer skills to commit cybercrime than ever before because you don't have to be a computer or programming expert to know how to hack. A variety of inexpensive hacking tools are available to online users. There are hundreds of digital tutorials and guides that provide step-by-step instruction on how to log into computers or steal passwords on media, social media, and websites related to children's content.

One example is video game environments, which, in addition to tutorials with tips and tricks for certain video games, also show how to crack them or get game licenses. In these contexts, many adolescents are injected with the cyber fraud virus in order to obtain free products and

services through hacking techniques, which may lead many of them to continue and intensify their cybercrime activities.

And when you take into account that the cyber prefix doesn't make crime less important, serious or dangerous to society, you see that teens start to get closer to crime. Although in the past the underworld could be identified and limited spatially and geographically, it no longer exists today in cybercrime.

As the above shows, it is not necessary to live or have grown up in the underworld or in a slum to witness or participate in cybercrime. This crime also occurs at a young age, which affects the learning processes of the social value and beliefs of these young people.

V. WAYS TO DETECT CYBER CRIME

With the advancement of technology, computer access to the Internet has reached every corner of our country. Anyone with an active network connection now has access to the wealth of information the Internet has to offer. Therefore, the Internet is the most important and richest source of information that ever existed. With the development of even more systematic and sophisticated search engines, obtaining information, albeit to a limited extent, is easier than ever. This brings us to the topic of cybercrime detection.

(A) Ways to Deal With Different Cyber Crime(s) (Aggarwal, 2016)

- Cyber Crime(s)where computers act as a means.
- Cyber Crime(s)where computers are the targets.

(B) What's the Process of Investigating Cyber Crime(s) (Aggarwal, 2016)

1. Cyber Crimes Research and Development Unit (CCRDU)
2. Cyber Crime Investigation Cell (CCIC)
3. Cyber Forensics Laboratory
4. Network Monitoring Centre

Cyber Crimes Research and Development Unit[7]

The Cybercrime Research and Development Unit is responsible for monitoring developments and changes in this constantly evolving field. This involves:

- Provide cooperation and cooperation with state police.

[7] *Details About Indian Cybercrime Coordination Centre(14C) Scheme*, MHA GOV https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

- The collection of data on cybercrime cases has been reported to the police for investigation.
- The detective will take action to determine what to do next.
- Find and locate areas requiring the attention of state police, including software experts.
- This includes collecting data on cases in other countries and preparing a monthly network report.

Cyber Crime Investigation Cell (Ccic)

The CCIC was established in September 1999. However, it did not enter into force until March 2000. It is part of the economic crime department and has jurisdiction over all of India.

Therefore, you can investigate cybercrime under the Information Technology Act 2000. Interpol is also a 24-hour contact point for cybercrime in India and is also a member of the "network". Cybercrime Information Center "Japan.

Cyber Forensics Laboratory[8]

CFL was founded in November 2003 and has the following functions:

- Provides media research in support of criminal investigations of the CBI and other law enforcement agencies.
- Provides assistance in finding and confiscating your computer upon request.
- Advice on investigations or activities where media analysis is likely or not yet completed.
- Make expert statements.
- Provide adequate research and development in the area of forensic cybernetics.
- The information thus collected will be used as evidence in court.

In order to guarantee the admissibility of such evidence, it is therefore necessary to ensure that all formalities are correctly completed. This means that all documents will be legally confiscated and the chain ofcustody will not be broken. In addition, the analysis thus performed must be performed on a copy of the image and not on the original media file itself.

[8] *Cyber Forensics Services*, PWC INDIA https://www.pwc.in/consulting/forensic-services/services/cyber-forensic-services.html.

The purpose of the new cybercrime departments is to monitor the internet to make sure that certain cybercrimes can be stopped before they are committed. To this end, the network monitoring center has received a network monitoring tool developed by I.I.T. Kanpur. It is also used to enable similar tools to accomplish this.

(C) How Does a Cyber Crime Cell Work In India

The first thing a detective should do when looking for evidence of cybercrime is to develop a preventive investigation plan.

The plan should include:

- Places where the officer must carry out this search.
- A list of suspicious computers or computer networks that could be investigated for this purpose.

In most cases, forensic experts at a forensic lab are still involved with the detective. When this is not possible, information about type, make, model, operating system, network architecture and type can be collected and the location of the data, remote access features, etc., which can then be passed on to forensic experts. This would help prepare for the collection and archiving of evidence.

The second step is to manage the place.

It must be ensured that the accused or suspect in the crime does not have physical or internet access to the system.

This means that you need to make sure that the system is not accessible via network sharing, WLAN, LAN, mobile phone, or any other device. The investigator must be very vigilant and have special support to ensure that the system remains isolated from access attempts.

The third step is to take the necessary precautions to ensure that the test goes smoothly.

Before starting the investigation, the investigator should decide whether to enter the data on site or to use the equipment for investigations in the forensic computer laboratory.

While an on-site data call has the benefit of not having to carry a lot of material, the assistance of a forensic scientist may be required to download the data for analysis and archive it for court records. If in doubt, a forensic expert should be consulted on site to decide whether to enter the data or the material.

If a specialist is not available, the detective is advised to plan everything.

There are cases when the computer system cannot be physically erased and the data copied to

another drive. In such cases, the examiner or specialist should load the necessary media, software and other special items, as well as special packaging materials, to avoid data loss, e.g. B. Data from magnetic media, dust swelling and electrostatic support.

In such circumstances, the investigator should always have the following equipment available:

- Hard drives or cartridges are devices used to save copies of files on your computer when the hardware cannot be removed.
- Tags to identify various pieces of evidence, eg. B. Cables that connect to different parts of your computer. Record to hard drives without damaging or destroying data.
- Screwdrivers and other tools used to dismantle the equipment are confiscated.
- The latent impression glove, if present, can be easily removed from the holder or hardware.
- Packaging materials such as rubber bands, duct tape, boxes, bubbles or paper bags should be used to transport evidence (as they are less static than plastic bags).
- Photographic equipment to record and photograph the scene of interest.

After completing these steps, **the auditor should document the system configuration and perform next steps.**

This includes:

- Label and photograph the entire installation in advance so that the system can be easily disassembled and reassembled, if necessary.
- The detective must take a photo with all the important aspects and check that all the pieces are correctly labeled. You may need professional help to do this.
- You need to make sure the system is turned off. That is, if the system is turned off, it should not be turned on, because hackers and IT professionals in enabled systems often issue cleanup commands if you enter the wrong password or a disk is missing.

After shutting down the system, the **next step** is to disassemble the shipping system. However, before sending, make sure that all relevant documents, such as manuals and peripherals, are available. In particular, software manuals and related notes, such as password records, must be provided.

The **last step** in the process is to protect and move data securely. As mentioned above, the researcher must always have the necessary tools. In addition, it is important to make sure that

the components of the system are packed correctly before being sent to the forensic laboratory.

Think of simple things like that

- These systems must not be loaded into the trunk of a police car.
- It must be packaged to reduce vibrations that can shake a part.
- Also, be sure to keep your computer in a cool, dry place away from any electromagnetic signals.

VI. EXISTING CYBER CRIMES POLICIES

Indian cyber law is no different. It is a combination of legal obligations, property, information protection and privacy. There must be strong computer rules as computers and the Internet cross every corner of our lives. Cyber laws regulate digital phone streams, software, information security, e-commerce and money transfers.

(A) What Is The Information Technology Act, 2000?(Shalini, 2016)

Information Technology 2000 explores the differences between the new age Information on technology, mobile devices, software and the use of the Internet are the means and means of these crimes. All kinds of crimes such as theft, fraud, impersonation, lying and fraud are cybercrime. These issues are discussed in Indian criminal law.

If the focus was on the need for cyber security laws, enforcing IT laws in India was imperative. For this reason, the Information Technology Act 2000, also known as the Indian Cybercrime Act or Internet Act, came into force in India. Since its publication, Internet laws in India have been designed to include all electronic records and all online / electronic activity for legal recognition purposes. IT legislation addresses important security issues that are critical to the success of electronic transactions.Internet laws in India not only validate digital signatures, but also regulate how documents can be verified, accepted and generated using digital signatures.

The Information Technology Act has changed since the introduction of the Computer Act as a cybersecurity act to protect cyberspace. IT laws were amended under:

- Indian Criminal Code
- Indian Evidence Act
- The Law on Bank Books

- Indian Reserve Bank

The main goal of cyber law in India is to prevent:

- Cyber crime
- Forgery and recording of electronic data in electronic commerce
- Electronic transaction

The Computer Law of 2000 was changed in 2008. These were enacted in the light of cybercrime laws - the Computer Act of 2000 through the Computer Act of 2008. They were implemented in early 2009 to strengthen the laws. Changes to the Information Technology Act 2008 include a change in the definition of terms such as communications equipment. Changing the definition of a communication device should include:

- The current use
- To validate the digital signature
- Hold the owner of the IP address accountable
- Liability is charged for data protection violations

(B) Parallel Provisions In The IPC And IT Act.(Ray, 2020)

Hacking and data theft: Section 43 and 66 of the IT Act penalize a range of activities, including hacking a computer network, stealing data, introducing and spreading viruses via computer networks, computers or computer networks or computer programs, and computer or computer malfunction of the System or computer network, an authorized person has denied access to the computer or computer network, corruption or destruction of information on the computer, etc. The maximum penalty for the above crimes is a prison sentence of up to 3 (three) years or a fine or Rs. 5,000,000 (five coats) or both.

IPC Section 378 on "theft" of movable property applies to online or other data theft, as IPC Section 22 requires that the words "movable property" contain a description other than the country. and things attached to the ground or permanently attached to things on the ground. According to Section 378 CPI, theft is punishable by a prison sentence of up to 3 (three) years or a fine or both.

It could be argued that the word "body" which is "physical" or "matter" would exclude digital properties from the scope of Section 378 of the IPC above. The opposite argument would be that the publisher intended to cover the characteristics of every description except for things and things that are permanently attached to the ground or permanently attached to the ground.

Section 66D of the Information Technology Lawprovides for a sanction for "personalized computer fraud" and provides that anyone who cheats personally using a communication device or a computer device is punishable by imprisonment at any time. He will be fined in 3 (three) years and up to R. 1,000,000 (rupees per ton).

Section 419 of the IPC also provides for the punishment of "fraud of character" and provides that anyone who cheats by nature is punished with 3 (three) years in prison or a fine, or both. . A person would be guilty of "deception of the character" if he had deceived by imitating another person or replacing him knowingly or by describing that he or someone else was someone else when it came to someone else.

(C) Conflict Between The IPC And The IT Act: Case Law.

1. In the case of Sharat Babu Digumarti vs. Government of NCT of Delhi[9]. The inconsistency between the government provisions of NCT Delhi, the IPC and the IT law was highlighted. In this case, an obscene video was posted on baazee.com ("Bazee") on November 27, 2004. The listing was intentionally placed under the "Books and Magazines" category and the "eBook" subcategory to avoid 'be detected by the filters installed by Baazee. Sold in multiple copies before the offer is deactivated. The Delhi police station subsequently charged Avinash Bajaj, general manager of Bazee, and Sharat Digumarti, manager of Bazee. Bazee was not prosecuted and this contributed to the release of Avinash Bajaj, as it was held that the indirect responsibility of Avinash Bajaj could not be established under Section 292 of the IPC or the Section 67 of the IT law, when Avinash Bazee was itself an employer, was not a defendant. Subsequent amendments against Sharat Digumarti under Section 67 of the IT Law and Section 294 of the IPC were also lifted, but the allegations under Section 292 of the IPC were welcomed. The Supreme Court then considered whether a waiver of charges under Section 67 of the Computer Law was possible under Section 292 of the IPC. The Federal Supreme Court overturned the case against Sarat Digumarti and ruled that if a crime contained an electronic file, only computer laws would apply, as that was the intention of the law. The fixed principle of interpretation is that special laws prevail over general laws and more recent laws take precedence over earlier laws. In addition, Section 81 of the IT Law requires that the provisions of the IT Law continue to be in force, which is incompatible and has been incorporated into any other law currently in force.

[9]2016 SCC OnLine SC 1464.

2. In the state of Gagan Harsh Sharma vs. State of Maharashtra[10], some individuals have been accused of stealing data and software from their employers and have been charged under Section 408 and 420 of IPC and Section 43, 65 and 66 of IT Law. All of these sections except section 408 of the IPC have been discussed above. Section 408 of the IPC deals with breach of trust by officers or employees and states that "Anyone, whether as an officer or employee, or an employee as an officer or employee, is in any way a criminal trust responsible for such property is or is subject to property control, can be punished with a prison sentence of up to seven years and a fine."

The offenses set out in Section 408 and 420 IPC can only be invoked and exacerbated with the approval of the court. The violations mentioned in Section 43, 65 and 66 of the IT Act are credible and exacerbated. The petitioners therefore argued that the IPC charges should be dropped and the charges against them should be investigated and brought to justice under the IT Act. It was further argued that if the signatories adhered to the decision of the Sharat Babu Digumarti Supreme Court, they could only be prosecuted under IT law and not under the IPC for crimes resulting from the same acts.

The Bombay Supreme Court upheld the petitioner allegations and ruled that the charges against them should be brought to the IPC.

VII. ACCOUNTABILITY OF STATE

State responsibility is one of the compensatory mechanisms in international relations. But the development of state responsibility in the digital domain is still in its infancy. This is the post deals with Lex Lata analysis based on applicable liability law and Lex Ferenda Solutions that can be designed to take into account the specifics of the Internet, such as its state Responsibility for the digital activities of non-state actors in their areas of responsibility. Convenient For the case study, the applicability of laws that describe state responsibility: an imaginary cyber attack by country A (DigiLand) on the electricity grid of country. (Cyber Stan) resulting in power failure and serious damage to Cyber Stan. Look for potential Digital solution includes possible enforcement of state laws and practices Liability has evolved in environmental law and other areas of activity International law. In addition, the analysis also examines the interaction between states responding to the practical need for international responsibilities and remedies Scenarios in the digital world.

(A) Application Of State Responsibility To The Internet

[10](2017) 2 SCC 18.

- Types of state responsibility
- Elements of state responsibility
- Damage and reparation

Types of State Responsibility (Kurbalija, 2016)

For Cyber Stan, the legal options to claim responsibility of DigiLand for this attack are summarised in the enclosed table, which presents the main types of responsibility/liability (row) and elements of responsibility (column).

Types of responsibility **Elements of responsibility**	**"FAULT" SUBJECTIVE RESPONSIBILITY**	**"RISK" OBJECTIVE RESPONSIBILITY**	**STRICT RESPONSIBILITY**
Breach of rules of international law	Required	Required	Not Required
Intention to breach the rule (fault/culpa)	Required	Not Required	Not Required
Territorial link (action originating computer or network under state juridiction)	Required	Required	Required
Attribution to state (including its organs)	Required	Required	Not Required
Damage and loss	Required	Required	Required

1. Liability for "fault"

First, Cyber Stan could try to remedy DigiLand's debt payment case, an approach used in traditional international law. This concept has been particularly dominant over time the period between the wars (1918-1941). However, it lost its significance in the second half of

the year the incompatibility of the 20th century between modern states and responsibility for "failures." From I. Brownlie: “There is a connection in the conditions of international life complex communities, which are different institutions and agencies, operate through public law The analogy of ultroviral action is more realistic than the search for subjective guilt Persons who may or may not "represent" the legal person (state). [11]" Brownlie's concern may extend to our case. CyberStan probably doesn't exist you must have sufficient evidence to identify and then prove the guilt of the people responsible for DigiLand[12]. As a result, CyberStan is likely to consider the following option in the Government Responsibility menu.

2. ‘Risk’ Responsibility

‘Risk’ or ‘objective’ responsibility lowers the threshold for responsibility. It does not require fault, but it requires the attribution of the action to other states and their officials. ‘Risk’ responsibility is 26 Ian Brownlie, System of the Law of Nations, State Responsibility, Part I, Oxford 1983, Attribution in cyber cases is discussed under II.B.2 10 based on a breach of rules (ex delicto). In our case, CyberStan would need to find the primary rule of international law that was breached. For example, this could be a breach of the ‘no harm’ principle, which requires a state «to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein... as it was specified in Trail Smelter Case (1941)[13].The application of the ‘no harm’ principle could be linked to an examination on whether a state has taken the necessary ‘due diligence’ measures in order to avoid any negative effects on the territory of other states.

3. Strict responsibility

If CyberStan cannot prove a violation of primary law, the last option is "strict Liability ”, which requires proof that the cyber attack originated in Hungary another state; in this case from DigiLand. Strict liability in its purest form is rarely used. Indeed, states cannot monitor all activities on their territory that could cause harm. to other states. In the digital world, it is extremely difficult to manage all digital activity carried out by non-state actors. In many cases it is undesirable to ask questions about it claims to monitor all digital activity. It can increase surveillance and damage sensitive objects the balance that societies around the world

[11] Michael Akehurst, *System of the Law of Nations: State Responsibility: Part I by Ian Brownlie*, OXFORD: OXFORD UNIVERSITY PRESS, 1983, xvi + 240 + (appendices andindex) 62pp (hardback £25.00): Legal Studies Cambridge Core (2018), https://www.cambridge.org/core/journals/legal-studies/article/abs/system-of-the-law-of-nations-state-responsibility-part-i-by-ian-brownlie-oxford-oxford-university-press-1983-xvi-240-appendices-and-index-62pp-hardback-2500/56ED20AAB42FFBA1617534DFE170A039 (last visited May 27, 2021).

[12] Attribution in cyber cases is discussed under II.B.2.

[13] *Trail Smelter Case (United States v Canada),* Arbitral Trib., 3 UN Rep. Int’l Arb. Awards 1905 (1941).

must find in protecting human rights and protect the public interest. Although it is important to establish a territorial link between cyber activity and other activities This is not enough to justify state responsibility. As discussed below Section II.B.2.b - "Territorial link" must be supplemented by a duty of care; hold a state responsible for not taking all appropriate measures to protect other states complaint.

Elements of State Responsibility

Government liability for Internet events is analyzed based on three main elements: 1) Violation of the rule International law, 2) sentence and 3) existence of damage or loss. The other two aspects The state responsibilities listed in the table are different: failure / failure and territorial relations is covered in more detail in this section. The error is not taken into account because it is a "liability for errors". is no longer used in international practice. It is believed that there is a "territorial link" when it comes to state liability, as in the case of CyberStan. That is, it is the foundation of everything Case 28: Smelter Trail (USA / Canada). Trib, Arbitration, repetitions International of the United Nations. Awards in 1905 (1941). Robert Jennings and Arthur Watts, International Law Oppenheim, 9th edition, Oxford, 2008. DigiLand's responsibility is discussed by starting a cyber event on CyberStan Computers in DigiLand.

Damage and Reparation

In order to enforce state liability, CyberStan must prove the damage and loss resulting from it forms the basis of repairs. Considering the ambitious role of cyberspace in modern life, damage and loss Computer activities can be very different and different from the direct effects on the attacked object (eg. Damage to the electricity grid) leads to damage that adversely affects the health and well-being of the population Population. This should be the starting point for repairing damage and troubleshooting. Preview of the article with three types of corrections. First, Article 35 mentions reimbursement as a means of restoring the status quo before committing the offense.... Refunds can be used if possible e sympathetic. In digital cases, the refund can only be used if the cyber attack has been triggered physical damage is not common in the digital world. Second, if the refund cannot be used, the section 36 compensation is "... financial measurable losses, including loss of profit. “In our case, the most likely is what CyberStan is looking for Compensation for damage caused by cyber attacks. The exact level of the demand the compensation depends on whether or not a causal link between the cyber attacks and the file resulting damage. The third option is satisfaction, which according to Article 37 is "... a Acknowledgment of Violation, Expression of Regret,

Formal Apology, or Other Appropriate Form Fashion. "Satisfaction, as a corrective approach, can be applied in cases of digital accountability to public accountability. The recovery options for a digital box usually depend on the type of damage the result of cyber attacks. Usually the refund is rarely applied, while the other two remain Compensation or satisfaction mechanisms.

VIII. CYBER LAWS IN INDIA

The world is going digital at an unprecedented rate and change will not be happening any faster. Digitization means that everything moves at the speed of light: business, entertainment, trends, new products and much more. The consumer gets what he wants immediately because the service provider can deliver it.

While this digital age offers many opportunities and advantages, there are also disadvantages. One of the biggest and most devastating threats is that our private information is at risk like never before. Hundreds of cases of identity theft, money loss and data breach have been reported over the past decade. Cyber attacks are widespread in nature and affect every person, company and government agency. We are entering an era where cyber criminals can achieve their goals anywhere, anytime. The need for cyber security has never been more critical than it is today.

A typical cyber attack is an attempt by adversaries or computer-controlled criminals to gain unauthorized access to a computer system or network, to modify it or to damage it systematic, commercial, and computerized use of technology to manipulate networks and computer systems to disrupt organizations and the activities that depend on them.

(A) Evolution of Cyber Crime in India

Due to the growing dependence on the use of technology, Cyber Law was necessary. Just as every coin has two sides, this technology has its pros and cons. The emergence of the 21st century meant the development of cyber law in India through the Information Technology Act of 2000 (commonly referred to as the IT Act). The first cybercrime was recorded in 1820

The purpose of India's IT Law is:

- Legal recognition for all electronic transactions.
- The legal signature of digital signatures is a valid signature for accepting online agreements.
- Legal recognition of electronic accounting by bank books and other organizations.

- Protect your online privacy and end cybercrime.

Indian IT Law has updated the Indian Reserve Bank Act As amended by the finance (no. 2) Act, 2019 and the Indian Record Law. With the development of Cyber Law, almost all online activities were examined. One aspect of cyber law, however, is that there are areas where Indian cybercrime laws do not apply, such as:

- The negotiable instrument is not controlled
- Authorized
- An obligation.
- Contract for the purchase or delivery of real estate.
- The national government reported documents or transactions.

(B) The Need For Cyber Laws

In today's world, with more technology, computer laws and cybercrime become more complex. Internet and technology about the future of research and making life easier for the people, but as the Internet usage and the number of people increased, they felt the need of IT laws and India. Because the internet is anonymous, cybercrime is easy. Therefore, many people can enormously abuse this function.

According to lawyer Tanuj Aggarwal, "with the exponential growth of the digital space, it was necessary to implement reforms to ensure the privacy and data protection of citizens."

(C) What Is The Information Technology Act, 2000?

If the focus was on the need for cyber laws or cyber security laws, IT laws should be enforced in India. In India, for example, the Information Technology Act 2000[14], also known as India's Cybercrime Act or Internet Act, came into force. In India, Internet laws were designed from the start to consider all electronic documents and all online / electronic activities as legal recognition. IT legislation addresses important security issues that are essential to the success of electronic transactions. Internet laws in India not only enforce digital signatures but also provide the ability to authenticate accepted and produced documents with digital signatures.

Since the IT law introduced to protect cyberspace is a cyber security law, the following IT law has been amended:

[14] Information Technology ACT, 2002 - It is the law that deals with cybercrime and electronic commerce in India.

- Indian Penal Code.
- Indian Evidence Act.
- The Banker's Book Evidence Act.
- Indian Reserve Bank.

The main objective of India's cyber law is to prevent:

- Cyber criminality.
- Falsification of electronic data and records in electronic commerce.
- Electronic transaction.

The IT law of 2000 was amended in 2008[15]. These were enacted under Cybercrime Laws - IT Law 2000 - IT Law 2008. They were implemented in early 2009 to enforce cybersecurity laws. Amendments to the Information Technology Act 2008 [16]include changes in the definition of concepts such as media. A change in the definition of a medium must include:

- The current use.
- To validate the digital signature.
- Hold the owner of the IP address responsible.
- Determination of the responsibility for data protection.

IX. HOW TO PREVENT CYBERCRIME?

There is no doubt that Indian laws or cyber security laws provide protection against cybercrime. However, prevention is always better than cure. Therefore, the following measures must be taken to prevent cybercrime:

- Unsolicited text messages: We receive all text messages from unknown numbers. You need to be careful not to reply to an unknown number of automatic text messages or voice messages.
- Mobile download: You can download anything to a mobile phone from a trusted source.
- Evaluation and feedback: Always check the evaluations of the seller and the buyer. See the latest comments. Also, look for reviews that are 100% favorable to the seller

[15] Information Technology ACT, 2008 - The main Indian act that addresses legal challenges specifically as they relate to the Internet is the Information Technology (Amendment) Act, 2008
[16]Information Technology Act, 2008

or that are on the same day.

- Requesting personal information: Everyone should receive a phone call or a letter If the person at the other end requests personal information. This includes your CVV card or email with an attachment that requires you to click on the embedded links. Make sure you never reply to these emails or calls.

X. REGULATION IN CYBER LAWS

Cyberspace encompasses the world but has no formal structure. There are no specific measures and restrictions going beyond the functions of the hardware used for access. The absence of a formal structure makes cyberspace a domain in its own right. Cyberspace is not owned or controlled by any person, organization or government. In terms of property rights, cyberspace can be considered zero Incapable of private eviction as well as space[17].

Regulation in cyberspace is becoming increasingly difficult. According to Lawrence Lessing, professor at Harvard Law School, anonymity is implicit in cyberspace. Anonymity stimulates and promotes the exercise of freedom. A child who is too shy to express himself in a physical space can pose as someone else in a virtual space and express himself freely.

The Internet is also fast and easy for transmitting voice and data. Simple communication greatly increases world trade. Instead of the traditional one-to-one method, goods are exchanged through a virtual space. They exchange large sums of money and even cell phones. The card-less transaction is the order of the day. Court documents are also sent electronically. The sums generated by e-commerce are enormous, although the mood for white collar crime is just as strong.

However, the ease of publication and the possibility of anonymity can harm the dignity or reputation of others. The Internet is also a way to shamelessly kill actors and news providers without harming producers.

Internet use also commits crimes with global consequences. Human trafficking, child pornography, ransoms and kidnappings all take place in cyberspace. Therefore, the freedom of virtual space should not be exercised without the simultaneous responsibility of users.

(A) Practical Problems In Extending The Traditional Laws To Cyberspace

Existing laws and regulations are based on the activities of the physical world. “With digitization and automation, many internet companies are widespread, both actors and

[17]Frank E. Lobrigo, *Regulating Cyberspace*, INQUIRER.NET https://opinion.inquirer.net/107924/regulating-cyberspace.

jurisdictions, making it difficult or even impossible to enforce existing internet laws such as physical laws. The main problems and challenges are:

- Different jurisdictions - All legal systems face legal uncertainty due to the anonymity of the internet user, the lack of geographical boundaries in cyberspace and the cross-border effects of internet transactions.
- Legal Vacuum - Legislators and legislators need to find a way to solve problems in cyberspace. However, there are no exemplary laws.
- Police Problem - Lack of technical knowledge, lack of cooperation between different police organizations, etc. It makes the problem very difficult to solve.
- Costly Process: Training police officers to solve the cybercrime problem is very expensive.
- Obtaining Digital Evidence: Obtaining digital evidence is another situation where cybercrime laws are difficult to enforce.
- Electronic contract - some shortcomings in the electronic contract:
    1. Small contracts.
    2. Fraudulent presentation with online advertising.
    3. Wrong legal opinion and factual inaccuracy.
    4. Application problem.
    5. The problem of profitability.

XI. CYBERCRIME IN TIME OF CORONAVIRUS

New Point Delhi, a researcher at Check Point Software Technologies, has suffered 192,000 cyber attacks per week in the past three weeks, a 30% increase over previous weeks.

Nearly 20,000 new areas linked to the corona virus have been recorded in the past three weeks, and about 17% of them are harmful or suspected, Check Point said on Tuesday. Since the outbreak, 90,284 new Corona domains have been registered worldwide. The results suggest that the global response to the COVID-19 outbreak and people's desire for the latest information is accelerating the standard business models used by criminals and hackers for phishing emails and fake sites. . Researchers have uncovered new phishing campaigns hidden in the World Health Organization (WHO) and popular conference platforms aimed at stealing confidential information.

For example, cybercriminals recently sent malicious emails from the who.int domain with the subject line "WHO Emergency Letter: First Human COVID-19 Vaccine Test Results / Update" to lure victims.

E-mails containing the AgentTesla malware contain a file named "xerox_scan_covid-19_urgent information letter.xlxs.exe". The victims who clicked on the file downloaded the malware.

Check Point claimed to have received two samples of alleged blackmail emails sent to the United Nations and WHO by suspected cybercriminals asking to transfer money to a number of vulnerable Bitcoin wallets. Cybercriminals use fake Zoom domains for their phishing activities.

In fact, around 2,500 new Zoom-related domains (2,449) were created in the past three weeks and around 1.5% of those domains are malicious (32) and another 13% suspicious (320). As of January 2020, 6,576 expansion-related domains have been registered worldwide. And Zoom isn't the only platform to include cybercriminals, the researchers warned.

The report shows a stark difference between the cases of Kerala and other states, but does not identify the cause of the inequality. Punjab, for example, only reported 207, Tamil Nadu 184.

"K7 Threat Labs grew 260% in Covid-19 cyber threats from the last week of March to the first week of April, referring to the extent of the opportunities offered by the cyber-criminal pandemic," said J Kesavardhanan, founder and CEO of K7 Computing, in a statement.

According to the report, phishing emails were the most common attack vectors. Emails containing information produced about the corona virus have been widely disseminated on behalf of trusted organizations. According to the study, these emails contain malicious links and attachments to ransom ware, RAS Trojans, and crypto currencies[18]. In addition to other Covid-19-related attacks, online malicious code outbreak monitoring cards are also prevalent. In addition, malicious applications containing disease messages and updates are widespread. In some cases, corona virus applications that had infected ransomware devices had to pay for the decryption.

After Google and Apple began targeting all apps providing information on the coronavirus in March, attackers followed other paths, such as B. Third-party app stores. K7 Computer found that an SMS Trojan attracted many Android users who asked them to install an app called CoronaSafetyMask to get safety masks. Another Android file called Corona Virus.apk was

[18] Jake Frankenfield, *Cryptocurrency*, INVESTOPEDIA https://www.investopedia.com/terms/c/cryptocurrency.asp

distributed in the name of virus information via phishing links.

XII. LANDMARK CASE LAWS

(A) Avnish Bajaj Vs State (N.C.T.) Of Delhi[19]

The defendant is the CEO of Baaze.com, any real estate development company that you receive a commission for and that generates income from the ads displayed on its pages. You obviously don't have a property to sell that can be paid for and delivered by a totally independent agency. In this case, prosecutors alleged that the defendant, through negligence and feelings of guilt, did not interfere with payment through banking channels after learning of the illegality of the transaction. At first glance, this suggests that the sales value has not yet been transferred to the suspect at this point in the investigation. Neither is it the case with the claim that the actual recording appeared on the website. However, he claims that the description of the item "DPS Girl Fun" should have set off the alarm.

A provisional objection was raised that the applicant should have applied to the court first, although that court also has jurisdiction under section 439 of the Criminal Procedure Act of 1973. I have drawn my attention to KC Jyya. and others v. the state of Karnataka,[20]; Rameshchadra Kashiram Vora srl. vs. Gujarat State and Anr.,[21]; and Hajialisher v. Rajasthan State,[22], where the Supreme Courts of Karnataka, Gujarat and Rajasthan supported this view. For Sri Ram v. Panna Lal[23] Moreover, in Article 401 of Delhi, that court laid down the rules of its own Supreme Court, which prohibited appeals in the absence of an appeal, unless the judge of first instance did so. He was contacted. The notification of 15 December 2004 should be subject to a similar review. As the higher courts are also liable, it would be useful to order the applicants to appear in court first. However, that would be an independent restriction comparable to the exercise of extraordinary power under Article 226 of the Constitution. The issue was discussed for a long time and this protest should have been raised by the state at the previous meeting.

(B) Smc Pneumatics (India) Pvt. Ltd Vs Shri Jogesh Kwatra On 12 February, 2014

In this case, the defendant Jogesh Kwatra, a lawyer assistant, began derogatory, defamatory, obscene, filthy, filthy and abusive emails to his employers as well as to various corporate offices around the world to empty them the company and its CEO, Mr. RK Malhotra. The

[19] (2005) 3 Complj 364 Del, 116 (2005) Dlt 427, 2005 (79) Drj 576.
[20] 1985 AIR 1495.
[21] 1988 Crl.L.J. 210.
[22] 1976 CriLJ 1658.
[23] ILR 1976 Delhi 401.

complainant has continued to take legal action to prevent the suspect from committing his or her illegal activities by sending defamatory emails to the complainant.

On behalf of the Complainants, it was alleged that the emails sent by the Respondent were clearly obscene, threatening, offensive, intimidating, humiliating and defamatory. Additionally, the lawyer stated that the purpose of sending these emails is to promote the reputation of applicants in India and around the world. He also argued that the defendant's actions in sending the emails violated the plaintiffs' legal rights. In addition, the suspect is not required to send such emails. It is important to note that the plaintiff discontinued the services of the defendant after the plaintiff's company determined that the employee concerned could send offensive emails.

After hearing the applicant's detailed arguments, the Delhi Supreme Court judge issued an ex parte preliminary ruling finding that the applicant had provided prima facie evidence. As a result, the Delhi Supreme Court has banned the defendant from sending derogatory, defamatory, obscene, threatening, degrading and abusive emails to the plaintiffs or their subsidiaries around the world, including their directors and business departments and marketing. The judge also prevented the defendant from posting, transmitting or disclosing slanderous, defamatory or offensive information to the plaintiffs in real life or in cyberspace.

XIII. CONCLUSION

It's not enough. We also need a stranger technology and above all engineering employees understand and use this technology. Social networks can be abused minutes until the cells are turned on Work very slowly. This can lead to this ten years to solve the cases even now In some delicate cases, the damage has already been done done. It is time to act and respond instead. Sometimes there is an addiction foreign agency. We know there are law varies by country. What are the reasons more delay. There is an urgent ethical need hackers are able to get to the root Criminal. Beware of social growth

We need at least fifty environments in India thousands of ethical hackers. The possibilities are for those job seekers, some of the latest bollywood movies and criminal television series and the process of arresting criminals but a great country where people like India live, criminals be smarter and learn from that Effects. We are members of the company think, think and be fair Guidelines for future generations.

Cybercrime has its roots in technology and critical infrastructure. The number of Internet users is increasing steadily and with it there is also an increased risk of various types of crime. Cyber crime they have a different character due to the development of technologies.

Technological crimes have evolved over time every day and should be treated with the highest priority. These are crime is never limited to computers, but other electronic devices exist as well they are made like machines for financial transactions and telecommunications, Equipment, etc. It is difficult to identify because of its diverse nature Cyber security issues that lead to security being ignored problems. We can organize seminars and free public announcements with the help of government and non-governmental organizations recognize cyber crime and illiteracy start at an elementary level; Institutions, data centers, schools and individuals. However, India has taken a number of measures to prevent this from happening cybercrime, but cyber law cannot be static changes over time.

*****