A Crticial Study of Cyber Crime: It's Impact During Covid-19

Kriti Bhatia[1]*, Dr. Sonu Agarwal[2]

[1]*Research scholar, school of law, Manipal university, Jaipur Phone number – 9461625016
Email: kritibhatia4@gmail.com
[2]Associate professor, School of law, Manipal university, Jaipur. Phone number - 99281 59638
Email: sonu.agarwal@jaipur.manipal.edu

***Corresponding Author:** Kriti Bhatia
*Research scholar, school of law, Manipal university, Jaipur Phone number – 9461625016
Email: kritibhatia4@gmail.com

Abstract:
At the beginning of the 21st century, there were many important technological changes that changed the way people talk to each other. The digital age has spread all over the world, making it easier for people to take part in their social, political, and economic lives. The number of people using computers and other electronic devices has grown a lot all over the world. Because of these changes, criminal activity has gotten a lot worse, especially online.. As a result, the number of illegal activities online keeps going up. Even though the international community has tried to fight the problem and lessen its effects, the number of scary cybercrimes has continued to rise around the world. They include setting up a clear legal framework, building and strengthening law enforcement agencies to deal with cybercrime, and providing cutting-edge infrastructure and surveillance technology. Cybercrime is the term for attacks that are done on purpose. These attacks can cause serious problems for society, such as economic problems, mental illnesses, and threats to national security. So, this article gives an overview of cyber crimes, including how they affect society and what might happen in the future.

Keywords: Cyberspace, Cyber Attacks, Potential Economic Impact, Consumer trust, National Security.

1.1 INTRODUCTION:

A staggering number of computers are linked to the internet. In spite of its many advantages, hardly one realizes the fact that certain criminals exploit it to their advantage. Cybercrime is the term for this type of crime. If you're found guilty of a cyber crime, you've violated a law that forbids or compels you to do so, and you'll face criminal charges. Because of today's fast-paced atmosphere, it is hard to make optimal use of time to boost performance. You'll need an internet connection to complete this task. When we talk about the "Internet," we're talking about a vast network of millions of computers connected by a variety of electrical techniques. To learn more about what is meant by "cyber crime," click on the link provided. Crimes involving computers, such as hacking into another person's system or database, stealing or altering data that is stored or accessible on the internet, or sabotaging technology and data are all instances of "cyber crime," according to the FBI. The Internet, or "cyberspace," is expanding at an accelerating rate, and so are online criminal.

As a result of IT improvements, online communication, profitable enterprises, and international involvement on social media platforms have become more accessible to everyone. However, illegal actions taking place throughout the globe in cyberspace put these accomplishments in jeopardy. Illegal computer use has become a big worldwide problem, and it is a serious worry for international security. New technology and faster internet connections have given thieves more access to private and corporate computers. According to Interpol figures, millions of people have attempted to tamper with the personal information of others by getting illegal access to it. Every day, people all around the world produce new forms of malicious software and viruses. Software of this type is available on PCs. Every day, the

personal information of almost 400 million people is made vulnerable due to malfunctioning computer systems (DCIMS, 2019).

Cybercrime has caused a great deal of harm, not just to individuals but also to businesses, because it prevents people from working and reduces trust in how organizations operate online. Damages around the world are anticipated to exceed $2.8 billion USD annually. Large social media businesses, including Facebook and TikTok, have made data breaches an industry standard. A data breach occurs when unauthorized individuals get information without authorization. This frequently compromises the security or integrity of the individual's personal information. In the year 2020, a committee of the United States Senate presented evidence that a Chinese corporation had violated privacy regulations by maintaining a database of consumer information and sharing it with third parties. Cybercrime is an issue that each nation must address on its own, and each nation should take measures to secure its institutions and provide them the authority they need to build an organized campaign to combat cybercrime that monitors what occurs in cyberspace. Criminals who violate the law online anywhere in the globe may only be apprehended if there are adequate and effective regulations in place to stop them. In order to avoid being a victim of cybercrime, you must also take preventative steps and employ proactive approaches (Howard & Gulyas, 2014)

1.2 Kinds of Cyber Crime:

1.2.1 Hacking:

Hacking is gaining unauthorized access by circumventing security safeguards. In order to combat cyber threats in the domains of business, politics, social media, and national security, there is a demand for information security specialists who are proficient in hacking techniques, despite the fact that doing so may be illegal in many nations. According to Gupta, there are three primary sorts of cybercriminals: (2019). "White hat" hackers are the initial category of hackers, and it is their role to prevent other hackers from infiltrating networks. They are permitted to do so by their company, which is mostly recognized for providing security.

A "black hat" hacker is the second type of hacker; they operate illegally. These hackers, sometimes referred to as malicious hackers, conduct their operations without authority. The grey hat, or the third sort of hacker, carries a double-edged blade. Depending on the benefits, they are capable of both attacking and defensive activities. Grey hackers are hackers who occasionally engage in unlawful activity but whose primary objective is to warn others about their vulnerabilities.

Four unique phases comprise the hacking procedure: reconnaissance, scanning, getting access, and maintaining access (Grispos, 2019). During the early phase of the assault, the hacker will actively or passively attempt to gather as much information about the victim as possible. In order to obtain sensitive information about the target, the attacker will collect a great deal of additional information about the target through scanning and other analyses. During the third phase, often known as gaining access, the attacker executes the hack. The attacker capitalizes on the situation and then exploits the vulnerability to get access. To maintain access, the attacker will install backdoors or Trojans in the subsequent phase of the attack. In order to prevent being discovered, they destroy logs and other information. According to the findings of this study, the Lizard Squad is an example of a hacker group that fits the description of a black hat. The group's origins and operations may be traced back to 2014, when it launched an attack on the Xbox and PlayStation game consoles while hosting on those companies' servers. The organization was also responsible for a number of harmful attacks, including the one that caused North Korea's internet to be shut down, the one that attacked the PlayStation network, and the one that caused Destiny's website logo to be altered (Grimes, 2017).

1.2.2 Computer Fraud:

Phishing is another term for this type of online criminal conduct. The criminals disguise themselves as employees of reputable businesses in order to steal money from bank customers who are ignorant of the fraud (Doyle, 2011). Scams and scams used to be

carried out via outmoded communication methods like telephones and postal mail. Email, text message, and social media arguments have surpassed previous cybercrime strategies. Fraudsters can use email to impersonate senders such as bankers in order to get access to sensitive information such as account numbers and user IDs. Massive amounts of text messages are sent out in this type of cybercrime in an attempt to deceive unsuspecting victims into providing personal information to fraudsters. Offerings that appear to be too good to be true may also be promoted by cybercriminals. After a length of time, they may claim to present victims with "investment" options, only to leave with their money.

According to the 2019 Verizon Data Breach Investigations Report, this form of cyber crime was involved in about a third of all data breaches. According to Casey, you don't have to worry about phishing if you don't know how to use computer software (2011). In the final stages of Hillary Clinton's presidential campaign, phishing attempts were successful in getting vital credentials from members of her campaign team. Several University of Kansas employees lost their jobs after providing their bank account information to phishers in the same year. According to Grispos, phishing kits have made it simple for hackers to launch attacks even if they have no knowledge of the subject (2019). Grispos,(2019). They may be found on the dark web, which is commonly used for illegal operations including drug trafficking and extortion.

1.2.3 Denial of Service attacks:

By flooding a host network with traffic, these assaults make it unavailable to normal users. As a result of these attacks, users are unable to access a network or system. Affected computers can no longer transmit or receive regular internet traffic since the assault sends data to the victim's computer across many devices all over the internet. Businesses that rely on the internet to operate have been harmed as a result of such assaults. A denial of service attack is made on a network server by a person or group that sends a lot of requests to it. This causes the system to crash (Doyle, 2011). When the victims' computers try to figure out who sent the requests, they get confused because the requests have fake return addresses. Because of this, the system ends up being overworked and unable to do its most important tasks. The Smurf Assault and the SYN Flood are the two Dos attack types that are used most often.

1.2.4 VIRUSES, TROJANS, AND WORMS:

Trojan is the name given to a Trojan horse in Greek mythology. The Greeks' ambitions to conquer Troy were stopped by the city's sturdy walls. They disguised their best troops as a Trojan horse and deceived their opponents by enabling them to enter their guarded perimeters. A Trojan horse, on the other hand, is a piece of software that is secretly placed on a victim's computer. It allows the perpetrator to gain remote access to the victim's laptop or desktop computer (Shea, 2012). By attaching itself to apps or data and then propagating to other computers, a virus can infect other systems. Computer viruses are like human viruses in that they can vary in how bad they are and damage a computer's software, hardware, and data. If malicious programs are run or launched on victims' computers, they can be infected. The warm virus is just as dangerous as the cold virus. It is a subgroup of the virus that can move from one computer to another without the help of a person. Worms are a serious problem because they can spread quickly and cause a lot of damage.

1.3 CAUSES OF CYBER CRIME:

Cybercriminals commit crimes for a variety of reasons. The primary aim is to generate money as rapidly as possible. These organizations are frequently motivated by avarice and engage in activities such as internet shopping, online banking, and fraud. Second, cybercrime may be used to attract attention and demonstrate bragging rights. The majority of those who breach the law here are young individuals who want to stand out. They might be idealists who want to be noticed but don't want to do harm to others. Third, people might engage in cybercrime to support a cause that is dear to them. The evil people in this scenario don't care if they cause harm or destruction as long as they obtain what they want.

1.4 IMPACT OF CYBERCRIMINAL ACTIVITY ON THE WORLD:

There isn't much difference between traditional crime and cybercrime, since both involve breaking the law. Cybercriminals have used a wide range of methods, from spreading bad emails and websites to more obvious crimes like downloading music without permission. Wall (2007) says that international criminals steal intellectual property either for their own benefit or for the benefit of the country they are working in. The annual losses are expected to be $10 billion. Industrial espionage losses in Germany are estimated to be between $25 and $50 billion, with a major chunk of that sum owing to a lack of appropriate internet protection. Despite the fact that most businesses do not keep track of cybercrime losses, the total might be far greater. Other hacked companies choose to keep the material hidden to avoid alarming their customers and shareholders. The financial sector has been the target of an increasing number of cyberattacks. They frequently target automated teller machines, credit cards, and online bank accounts. A Russian gang stole $9.8 million from ATMs over the Labor Day holiday weekend.

1.5 IMPACTS OF CYBER-CRIME:

Lunda Wright, a Rhodes University legal expert who specializes in digital forensic law, made a unique study discovery on her blog in October 2005. Here's a link to Wright's find. According to the data, the number of cybercrime prosecutions has lately climbed. [A reference is necessary] The number of initiatives to prevent cyberpiracy in the area of film and music works has increased. New sorts of litigation are evolving, as are new approaches to legal conflict. Commercial and government entities are increasingly depending on the abilities of computer forensics professionals. Finally, the number of government-to-government interactions has increased. Internet fraud and theft are two of the most typical activities conducted by organized criminal gangs using the Internet. Recent discoveries indicate that organized crime is involved in white-collar crime. As thieves abandon traditional methods of operation, internet-based criminality is becoming more widespread. Because it causes investors to lose money and makes criminals millions of dollars each year, stock fraud carried out over the Internet is a lucrative way to engage in unlawful activity. Because legitimate investors lose money while criminals make money through the scheme, it is a lucrative way to engage in unlawful activity.

The majority of police agencies in the United States have confirmed that they have received an increase in similar complaints in recent years. This is consistent with a nationwide pattern that has arisen as a direct result of wider computer usage, increased online trade, and the advent of technically skilled criminals. In 2004, cybercrime earned more money than drug trafficking, and this trend is expected to continue as technology becomes more extensively utilized in developing nations. According to Scott Borg, the leader of the US Department of Homeland Security-funded United States Cyber Consequences Unit, denial-of-service assaults will not be the next big thing in cybercrime. When compared to the prospect of attacks in the near or far future, worms and viruses are regarded "not yet evolved."

1.5.1 POTENTIAL ECONOMIC IMPACT:

Over 74 million Americans were victims of cybercrime in 2011, according to a Norton report. Direct damages were 32 billion dollars as a result of this illegal behavior. 69 percent of internet users have been victims of cybercrime, which translates to one million victims per day, according to a research. There is a widespread belief among the general public that doing business online puts you at danger of having your computer infected by malicious malware. Modern customers are more vulnerable to cybercrime than ever before due to their increased reliance on computers, networks, and the data they save and control.
According to prior research, up to 80% of firms surveyed reported financial losses as a result of computer security breaches. It is estimated that a total of $450 million was affected. Almost 10% admitted to committing financial fraud [14]. Every week, new risks to the availability, integrity, and secrecy of computer systems are reported in the press. This might vary from the

theft of personally identifiable information to attacks on service providers. As the economy becomes increasingly reliant on the internet, it becomes more vulnerable to the variety of cybercriminal threats. Buying and selling stocks, conducting bank transactions, and making credit card purchases are all instances of internet-based transactions.

Such transactions are vulnerable to fraud, which has a direct impact on the financial health of the organization and on the economy at large. Another potentially disastrous result may be a disruption in global financial markets, which is still a major source of concern given the worldwide structure that today's enterprises have, which includes several countries and time zones. In light of the global economic system's interconnected structure, any disruption in one region's economy has the potential to affect other regions. The challenge arises when these systems are disrupted because the effects extend beyond the market. Because of this, productivity suffers.

Worms, viruses, and other security threats divert the user's attention and time away from more productive duties. Machines may become less efficient, servers may become unavailable, networks may get congested, and so on. These kinds of attacks have a big effect on how much work both the user and the company can get done, both individually and as a whole. It affects the quality of the company's customer service because outside customers see it as a negative part of their interactions with the company. Furthermore, customer fear of being a victim of fraud prevents a sizable proportion of online buyers from completing purchases. It is self-evident that consumer hesitancy, uncertainty, and fear create considerable revenue loss for internet enterprises. These sorts of customer trust issues might have major ramifications, therefore it's worth looking into them more.

1.5.2 IMPACT ON MARKET VALUE:

Firms and insurance companies that provide cyber-risk coverage are concerned about the economic consequences of data breaches. Consider doing something that will benefit Ingram. According to Micro, "actual damage" refers to the physical destruction or degeneration of computer circuitry, as well as the loss of its functionality and usability. This new and ever-changing concept of damage is becoming increasingly essential as the number of enterprises that rely on information technology and the Internet grows. As a result of this precedent, many insurance companies may be required to compensate firms that have suffered losses as a result of cyber attacks or other security breaches.

Because the features of security breaches fluctuate, businesses must do frequent threat assessments of their IT environment. FUD (fear, uncertainty, and doubt) has been used by CIOs in the past to convince upper management to invest in security. In recent years, it has become more and more usual to accurately predict the expenses associated with computer malfunctions and hacker assaults. These estimations, however, are difficult to generate due to a paucity of historical data. According to numerous industry insiders, the charges for these programs are mostly based on guessing.

1.5.3 IMPACT ON CONSUMER TRUST:

Customers are irritated and discouraged from returning when a hacker obtains access to another person's account and attempts to disrupt the logic of a website. Despite the fact that the criminal who coordinated the concealed assault is to blame, the site in issue is referred to as "fraudulent." As a result, the client loses faith in this website, the internet in general, and its own abilities. More than 80% of those polled by the Better Business Bureau Online said that they were concerned about security when doing business online.

When prompted for their credit card information, 75% of internet customers abandon their transaction. Credit card fraud and Internet security threats are becoming more widely recognized as threats. This has been a major source of concern in the world of online purchasing. In contrast, consumer perceptions of fraud overstate the severity of the situation. When it comes to influencing buying decisions, the public's impression is just as important. As a result, many internet buyers avoid doing business because they are afraid of being duped. This is what makes a

shopper hesitant to do business with an e-company owing to concerns about its safety or crowded nature. Even the slightest suggestion of a security breach or questionable business practices can be catastrophic to a company's long-term sustainability.

1.5.4 AREAS RIPE FOR EXPLOITATION:

Interests of the Nation's Protection The current military forces of most countries rely heavily on high-tech computers. Following the September 11 attacks, there has been a greater emphasis on Information Warfare (IW), which involves network assaults and exploitation, as well as defense. IW is intriguing since it is highly effective, inexpensive, and provides the attacker with a high amount of anonymity. Malware can easily propagated from computer to computer, causing network connections to fail and false information to spread. Because it focuses on various types of conflict, information warfare is an excellent research topic.

1.6 CYBER CRIME DURING COVID -19:

So far, the covid-19 virus has spread to more than 50,000 people. In response to the growing threat, the Indian government has ordered a statewide lockdown to start on March 25, 2020. During the first part of the shutdown, no business or government work is done in India. People who work for you have suggested that you work from home. With the click of a mouse, employees can now get to financial information, customer lists, and other private information from the comfort of their own homes. To stop sensitive information from getting out and data breaches from happening, employees must keep business data safe and keep it out of the hands of family and friends. Personal and financial information, as well as business information, are at risk because of cyberattacks.

Covid-19 protects against ransomware, spyware, and other potentially harmful viruses. Consumers are more likely to use social media sites like Twitter, Facebook, and Instagram to watch television episodes and movies during the lockdown period than web channels like Amazon, Netflix, Zee 5, HotStar, and others. Among these web channels are Twitter, Facebook, and Instagram. These two goals can be met by using the internet. To use the app's capabilities, users must grant the app's makers access to any personal information stored on their mobile devices, tablets, desktop computers, or social media accounts. Customers are routinely asked to provide financial information in order to purchase software or use internet services. Citizens are increasingly reliant on payment gateways to pay their power bills, recharge their mobile phones, buy crucial goods and medicines online, and engage in a range of other internet-based activities. Ransomware and other types of malware are easily exploitable as a result of these actions.

Ransomware keeps track of a user's login and other important credentials because it steals important personal information. People can be hurt in more ways than just their finances when these kinds of attacks happen. Different groups have come up with countermeasures and safe ways to do things to help stop these attacks. More and more programs and operating systems are getting regular updates that fix security problems and add more layers of protection. One way that money can be stolen is through a "phishing attack." People are told to do their financial business online or over the phone because banks don't have as many resources as they used to. Cybercriminals pose as bank employees and send phishing calls, SMS messages, or emails to bank customers. They ask for personal information like their account number, debit or credit card number, one-time password, card verification value, and other sensitive information. As part of the COVID 19 regulatory framework set up by the RBI, payments on term loans, EMIs, and interest have been stopped for three months. Cybercriminals are getting in touch with loan holders and asking for credit card information, one-time passwords, PINs, or passwords as a cover so that they can get an EMI payment deferment. 41 Reports That Are False or Wrong Another important issue is the spread of fake news or rumors across the country..

Here are some examples of how rumors can have negative consequences. The poultry sector lost 1.6 billion rupees in a single day in March due to a false allegation on social media

that "chicken is a carrier of Coronavirus." Another example had vegetable sellers licking their merchandise in order to transmit the Corona virus. Following that, the administration issued a statement denying the veracity of the audio clip. Government pensions were intended to be reduced by 30% during the shutdown. 42 The Cyber Police in Karnataka and Maharashtra have promised to take strong action against anyone detected on social media spreading misleading and baseless information about COVID-19. If it is discovered that someone is posting deceptive information in the What's App group, the admin will be held personally liable in his group for the material he publishes and will be held liable under the applicable legislation. The Indian government, police, and social media platforms are working together to prevent disinformation from spreading.

Fraud is a Citibank contact center based in Pune. MphasiS In this instance, the defendant scammed four City bank clients. $3,500,000 was sent to a fictitious Pune account. In certain cases, the defendants are contact center agents who gained the plaintiffs' trust and obtained their personal identifying numbers (PINs). They then began to use these pin numbers to attempt online fraud. In this situation, we must consider how vital data security is. It is clear that "Unauthorized Access" to the victims' "Electronic Account Space" was used in this case. The IT Act of 2000 specifies "cyber crimes," allowing criminal components not covered by the IT Act but protected by other laws to be categorized as "written document" crimes. Other laws, such as those in the IT Act-2000 dealing with "cheating," "breach of trust," and "conspiracy," apply in this scenario as well. Sections 66 and 43 of the Information Technology Act of 2000 make the infraction a crime. Individuals who were implicated face prison time and penalties, as well as the duty to pay up to one crore rupees in compensation to each victim, under the "Adjudication Process," which may be launched.

1.7 CASE STUDY:

1.7.1 SONY SAMBANDH COM CASE:

This is the first person found guilty of cybercrime in 2013. Sony India pvt. Ltd. filed a complaint, which set off the whole thing. Sonysambandh.com is their website for NRIs. NRIs can buy Sony products online and send them to friends and family in India as gifts. The business will sell its goods to anyone who wants them. A cybercrime case study says that in May 2002, someone posing as "Barbara Campa" logged on to the site and bought a Sony Color TV and a wireless headset. When she placed her order, she did so with the help of a credit card number and specified that the goods be delivered to Arif Azim in Noida. The credit card company validated the payment, after which it was processed further in the system. After conducting the appropriate research and evaluations on the products, Sony presented them to Arif Azim for his use.

When the product was delivered, the company took digital photos to prove that Arif Azim had accepted delivery. After the transaction, the credit card company told the business that it had happened without the cardholder's permission. The cardholder denied buying anything from the business. The case was filed under sections 418, 419, and 420 of the Indian Penal Code. A formal complaint was made to the CBI about cheating online (IPC). Someone looked into it, and the person who did it was caught. Investigators say that the person of interest works at a call center. CBI was able to get the thing that he was given. He said he was guilty because the CBI had enough proof to convict him in these cases. He was found guilty under the Indian Penal Code's sections 418, 419, and 420. For the first time in history, someone has been found guilty of a cybercrime.

When he was arrested, he was only 24 years old, and this was his first time breaking the law. This made the court more lenient. Because of this, the court gave him a probation sentence. This choice affects the health of the country. This was also the first time the case led to a conviction, showing that the IPC could be used to cover more types of cybercrime than the IT Act 2000 does. For the second time in a row, a big decision makes it clear that it's hard to take the law for granted.

1.7.2 THE BANK NSP CASE:

The Bank NSP case, in which a bank management trainee was engaged to be

married, is one of the most well-known cybercrime instances. The pair communicated via computers at their separate workplaces. She started sending emails to the guy's overseas clients as soon as they split up, using bogus email addresses like "indianbarassociations" after creating bogus email accounts. She was able to accomplish this by using a bank-issued computer. Because that boy's business lost a lot of customers, he decided to sue the bank. The bank held email sent through the bank's system liable.

1.7.3 SMC PNEUMATICS (INDIA) PVT. LTD. VS. JOGESH KWATRA:

It is unique in that it is the first time in India that legal action has been pursued for defamation over the internet. As a result, the defendant in this case, Jogesh Kwatra, worked for the corporation at the center of the dispute. He began sending emails to his bosses as well as many subsidiaries of the same company situated throughout the world. These communications were slanderous, rude, and insulting. He planned to tarnish the reputation of both the firm and its CEO, Mr. R. K. Malhotra.

Because the defendant sent the plaintiff disrespectful emails, the plaintiff decided to file a case in order to get a permanent restraining order that would prevent the defendant from continuing his illegal conduct. He claimed that the defendant's actions, which included sending emails to the plaintiff, violated the plaintiff's legal rights and were thus illegal. The defendant is compelled to refrain from sending any of these emails as part of the settlement conditions. The defendant has been granted an ex-parte temporary injunction by the Honorable High Court of Delhi. A preliminary injunction was granted, stating that the defendant was barred from repeating such remarks in the future and that the complainant had built a compelling case against him. According to the decision, the complainant had established a compelling case against him.

The Delhi High Court issued an ex-party injunction to stop the defendant from sending abusive, obscene, insulting, or defamatory emails to the plaintiffs or their subsidiaries. This is important because it is the first time an Indian court has ruled on a cyberdefamation case. The decision by the Delhi High Court is important because it is the first time an Indian court has ruled on a cyber defamation case.

Indian websites about health care have been broken into. Recently, there was an attack on health care websites in India. Cyber security firms in the United States say that hackers attacked a key Indian healthcare website. A hacker stole the medical and patient records of 68 million people.

1.7.4 SHREYA SINGHAL V UNION OF INDIA:

Sec. 66A of the IT Act of 2000 became effective as a result of legislation approved in 2009. In this writ petition, the plaintiff sought to have Section 66A declared unconstitutional. Section 66A, according to the petitioner, has made new, destructive types of crime possible. The petitioner challenges the Act's legality under Article 19. (2). The provision and Art. 19(1)(a) are vague, and no "intelligible difference" form of communication, such as the Internet or another medium of communication, exists. The question was whether Section 69 of the Information Technology Act could be sustained in court. The Constitution's preamble proclaims that "India is a sovereign, democratic, and republican country." We cannot overstate the value of freedom of expression in our democratic constitutional system. In other words, "freedom of speech and expression" might relate to three things: expressing a different point of view, making a case for something, or inciting violence. Article 19(2) may be used only if all three of the following requirements are satisfied.

According to the framework of our constitution, it is not within the competence of the state to restrict people's rights to free expression in order to serve the general public's interests. Because "public order" and "public safety and tranquillity" are equivalent, any law that violates section 19(2) is deemed unconstitutional and null and void. "Does a specific act upset current communal life, or does it simply affect an individual, leaving society's peace undisturbed?" is a question that can be used to determine whether or not there has been a violation of public order. This is the

test that can be used to determine whether or not there has been a breach of public order. A clause that produces an unclear crime must be declared unconstitutional and arbitrary when there are no acceptable standards for determining responsibility in a section that constitutes an offense and when neither authorities nor courts nor law-abiding citizens are given clear direction. This is the situation, for instance, when specific instructions are not given to authorities, judges, or law-abiding citizens. Section 66A has a number of confusing, open-ended, or imprecise statements. As a result, a potential offender of section 66A, as well as the section's enforcement authorities, lack appropriate criteria for booking a person for an infraction under the provision. As a result, it is unlawful for Section 66A to violate the right to free expression in an arbitrary, unreasonable, or disproportionate manner. This clause must be knocked down for violating the First Amendment's free expression guarantee and repealed owing to its too broad language and potential for abuse.

Because online speech differs from other modes of communication in terms of "intelligible difference" it will be treated as a separate violation under the law. Section 66A is not discriminatory, according to Article 14. The court, however, determined that Section 66A is unconstitutional because it breaches Article 19(1) of the Constitution (a).

1.8 CONCLUSION AND RECOMMEND-ATIONS:

In both developed and developing countries, according to this study, cybercrime is on the rise. In many cases, computer-related crimes are committed by youngsters and teens who are already familiar with and comfortable using computers. Additionally, many cybercrimes are undetected because of the associated humiliation. Survey results show a gap between the laws and organizations and authorities in charge of fighting cybercrime in different countries. According to this report, traditional laws and regulations are currently ineffectual in curbing cybercrime incidences. Therefore, it is imperative that they remain current with the latest technology advances. Other nations aren't as concerned about the dangers of cybercrime.

As a result, the United Nations' securitization framework does not even include it in the budget. In addition, this research has shown how quickly cybercrime is spreading over the world. This study's findings suggest that the response against cybercrime should also be acceptable. A global standard for cybercrime policies and norms is needed to tackle cybercrime effectively. Cybercrime is a problem that has been addressed in a variety of ways by different governments. The use of computers to categorize offenses is essential for all countries to follow a consistent approach.

This collection of literature focuses not only on obtaining an awareness of cybercrime, but also on elaborating on the effects cybercrime has on all levels of society. This will be extremely beneficial to the community in terms of safeguarding all of the critical internet information firms that are currently at risk due to cybercrime. It will be simpler to find appropriate solutions to the problem if one first understands the motivations of individuals who commit cybercrime and the consequences of such acts on society. The strategy for combating these crimes may be divided into three categories: education, policymaking, and the enactment of cyber legislation (often referred to simply as cyber laws). The aforementioned tactics for countering cybercrime are either yielding very little or no significant gains in many countries, or they are utterly worthless. Because there is so little work being done, it is vital to either improve what has previously been done or create new paradigms for dealing with cyber dangers.

The prevalence of using computers and the internet for clandestine operations and intelligence gathering will increase. Our intelligence services must immediately prepare for this newly found threat. Consequently, it is crucial to construct a "National Cyber Space Security Management Policy" that outlines the roles and activities of numerous authorities while using an integrated architecture. It is a well-known fact that terrorists use the Internet to communicate, extort, intimidate, raise funds,

and plan their actions. Governments at conflict with one another have gained a high level of cyberwarfare expertise. They are capable of bringing down vast portions of communication networks, causing financial collapse, and sowing the seeds of social upheaval. Our level of readiness for all of these possible dangers is woefully inadequate, leaving much to be desired. This steady but dangerous increase should be brought to the government's notice, which should subsequently establish a structure to combat abuse. Cybercrime is one of the types of criminal activity that is expanding at the quickest rate worldwide.

With the help of different newly created technology, an increasing number of people are engaged in this sort of unlawful business these days. This type of criminal behavior includes attacks on computer data and computer systems, identity theft, the transmission of pictures showing child sexual abuse, and other related activities. Because cybercrime is a global phenomena, thieves in one part of the world can attack a computer in another part of the world. As a result, each country has been obliged to adopt its own set of local restrictions in order to protect its own internet. Because every portion of the world is related to every other component, this is the case. There is a link between growing internet connectivity and an increased danger of online theft, fraud, and abuse. Because we are becoming increasingly reliant on modern technology, we are becoming more vulnerable to cyberattacks. To put it another way, the essence of what we mean when we talk about cybercrime is computer misuse for the goal of committing a crime. Its two main components are a computer and a network..

The computer might be either the perpetrator or the victim of the crime. In India, the Information Technology Act is the only law that addresses cybercrime. The Act is silent on the definition of "cybercrime." However, the Act's many sections make it plain what cybercrime is and what it entails. This Act's primary purpose is to secure e-commerce, e-government, and e-banking, as well as to ensure that cybercrime is penalized. The Act was amended by the ITAA of 2008. However, a single piece of legislation is insufficient to defend a country with such a high crime rate. Furthermore, the Act does not devote enough attention to territorial jurisdiction, which is a major flaw. Evidence preservation is also a major concern. However, the Indian Penal Code covers the majority of cybercrimes, which is excellent news for those investigating them. This is due to the fact that, even if, criminals.

Our reliance on the internet is to blame as a main issue. The Information Technology Act does not cover all aspects of information technology that must be safeguarded. This Act does not go far enough in addressing copyright and trademark infringements. The Act exempts internet service providers from liability for transferring third-party data. Third, the Act is unclear about how the extra territoriality would be implemented, which is an issue. The Act, with the exception of a few exclusions, primarily tackles the most serious aspects of cybercrime.

REFERENCES:

1. Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, [3.] CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/data/definitions/117.html,
2. Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm,
3. Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.
4. DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-NetworkSabotage-or-incompetent-managers-trying-to-,
5. IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/,
6. Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizencentre/ html/cyber_crime_glossary.shtml,
7. Alsmadi, I. (2019). Cyber intelligence. The NICE Cyber Security Framework, 75-90.

https://doi.org/10.1007/978-3-030-02360-7_5
8. Bernik, I. (2014). Cybercrime. Cybercrime and Cyberwarfare, 1- 56. https://doi.org/10.1002/9781118898604.cp
9. Boes, S., & Leukfeldt, E. R. (2016). Fighting cybercrime: A joint effort. Cyber-Physical Security, 185-203. https://doi.org/10.1007/978- 3-319-32824-9_9
10. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.
11. DCMS: Cybersecurity breaches survey 2019. (2019). Network Security, 2019(4), 4. https://doi.org/10.1016/s1353-4858 (19) 30044-3
12. Doyle, C. (2011). Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws. DIANE Publishing.
13. Grimes, R. A. (2017). Hacking the hacker: Learn from the experts who take down hackers. John Wiley & Sons.
14. Grispos, G. (2019). Criminals: Cybercriminals. Encyclopedia of Security and Emergency Management, 1- 7. https://doi.org/10.1007/978-3-319-69891-5_80-1
15. Gupta, S. (2019). Ethical hacking terminologies. Ethical Hacking Learning the Basics. https://doi.org/10.1007/978-1-4842-4348-0_1
16. Howard, P. N., & Gulyas, O. (2014). Data breaches in Europe: Reported breaches of compromised personal records in Europe, 2005- 014. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2554352
17. Krausz, M., & Walker, J. (2013). The true cost of information security breaches and cybercrime. IT Governance Publishing.
18. Moore, M. (2016). Cybersecurity breaches and issues surrounding online threat protection. IGI Global.
19. Rajan, A. V., Ravikumar, R., & Shaer, M. A. (2017). UAE cybercrime law and cybercrimes An analysis. 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security). https://doi.org/10.1109/cybersecpods.2017.8074858
20. Shea, J. M. (2012). Combating computer viruses. Gareth Stevens Publishing LLLP.
21. T., S. (2016). Combating cybersecurity breaches in the digital world using misuse detection methods. Advances in Digital Crime, Forensics, and Cyber Terrorism, 85-92. https://doi.org/10.4018/978-1-5225 - 0193- 0.ch006
22. Wall, D. (2007). Cybercrime: The transformation of crime in the Information Age. Polity.
23. Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml,