Volume 31, March 2024 ISSN 2581-5504

"Analysing Cyber Crime, Cyber Criminals and Culture of Fear Associated With it"

Gargi Shukla
ICFAI University,
Dehradun

Abstract

The digital revolution has already changed how people live, work, and communicate. And it's only just getting started. But the same technologies that have the potential to help billions of people live happier, healthier, and more productive lives are also creating new challenges for citizens and governments around the world. From election meddling to data breaches and cyberattacks, recent events have shown that technology is changing how we think about privacy, national security, and maybe even democracy itself.

We will discuss how the fear culture about cybercrime, shapes public expectations of online risk, the formation of law and the subsequent interpretation of justice. Fear is an incredibly powerful tool. It has been used as a weapon throughout history to manipulate and control the cyber world.

Despite the increasing prevalence of cybercrime and its study by criminologists, very little research has examined the extent, nature, and impact of fear of cybercrime. To understand cybercrime and its various forms, one must be familiar with criminality in general. How individuals perceive crime, and how much they fear it. Users believe that using computers for work, exchange of data and browsing multimedia contents is mostly safe, but relatively unsafe when they are directly connected to the Internet and are downloading general data.

Using the computers for our day-to-day transactions is quite common now a days. For example, we pay our life insurance premium, electricity bills, reserve flight or train or bus tickets, order book or any other product online using personal computer, smart phones, public browsing etc.

Methodology of Research Study

This is a doctrinal research on cyber crime.

Introduction

Cybercrime is a dangerous attack a company or an individual may face. There are many cases where the cyber attack has brought massive loss to the company and individuals due to the data hack. We live in a technology-driven era, and every piece of information is now fed on computers. These attacks are also affecting the economy of the country if not controlled in the initial stage.

The number of users doing online transactions are growing rapidly ever since, because of the convenience it gives to the user to transact business without being physically present in the area where the transaction happens. Criminals committing cybercrime are also growing day-by-day with the increased number of users doing online transactions.

Volume 31, March 2024 ISSN 2581-5504

Ever since the creation of the Internet, people have been finding ways to conduct illegal activities using it as a tool.

Unfortunately, the same technology that gives us so many opportunities also makes it possible for various malicious elements to exploit it for their own nefarious purposes. The development of the Internet and the proliferation of computer technology has created new opportunities for those who would engage in illegal activity. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity, it has also resulted in the emergence of what appear to be some new varieties of criminal activity.

Introducing the Electronic Crime

"*People are twice as afraid of having their computer hacked than they are about having their car stolen or their house burglarized."*

What is cyber crime

What image comes to mind when one hears the term computer crime? One may think of pimply-faced teenage hackers locked up in a dark bedroom littered with diet soda cans, accessing top-secret files on super-secret government computers. Others may think of a creepy old man, hiding behind a keyboard in his attempts to lure children into an illicit rendezvous .Still others may see the Nigerian e-mail scammer, or the auction fraudster, or the identity thief. The important point here is that the term computer crime has different connotations depending on the situation, the person, and their individual frame of reference.

Examining "Computer Crime" Definitions

Donn Parker is generally cited as the author that presented the first definitional categories for computer crime. Parker clearly favours the term computer abuse as a higher-level definition and describes it as "…any incident involving an intentional act where a victim suffered or could have suffered a loss, and a perpetrator made or could have made a gain and is associated with computers". Parker further goes on to describe the ways in which computers play a role in computer abuse:

1. The computer is the object, or the data in the computer are the objects, of the act.
2. The computer creates a unique environment or unique form of assets.
3. The computer is the instrument or the tool of the act.
4. The computer represents a symbol used for intimidation or deception.

These categories have proved to be broad enough to encompass both the computer abuses described by Parker in 1976 as well as the modern computer crimes we see today.

Robert Taylor also notes the problematic nature of attempting to define computer crime in the book Digital Crime and Digital Terrorism, in which they state "Defining computer crime sufficiently is a daunting and difficult task." Taylor and company expand on Parker's definitions and present four categories of computer crime:

Volume 31, March 2024 ISSN 2581-5504

1. The computer as a target The attack seeks to deny the legitimate users or owners of the system access to their data or computers. A Denial-of-Service (a.k.a., DOS or DDOS) attack or a virus that renders the computer inoperable would be examples of this category.
2. The computer as an instrument of the crime The computer is used to gain some other criminal objective. For example, a thief may use a computer to steal personal information.
3. The computer as incidental to a crime The computer is not the primary instrument of the crime; it simply facilitates it. Money laundering and the trading of child pornography would be examples of this category.
4. Crimes associated with the prevalence of computers This includes crimes against the computer industry, such as intellectual property theft and software piracy.

Although it is universally agreed that cybercrime exists, there is no universal definition of what it means but still we can say that ***Cyber crime is a criminal activity that uses a computer to target the computer or it maybe defined as a crime where a computer is the object of the crime and is used as a tool to commit an offense.***

Cybercrimes fall under State subjects as per the Seventh Schedule of the Constitution of India. Cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime". Examples include hacking, identity theft, fraud, and cyberstalking etc.

As the internet and its associated advantages grew in popularity, so did the notion of cybercrime. Cybercrime targets can be individuals, businesses, governments, and other organizations. Anyone who uses the internet, computer systems, or other digital devices is vulnerable to cybercrime. While anyone can be a target of cybercrime, women and children can be particularly vulnerable.

Major reasons for Cybercrime

- **Financial gain**: through stealing financial information, such as credit card numbers and bank accounts, or through demanding ransom in exchange for stolen data or resources.
- **Espionage**: Some cyber criminals engage in cyber crime to steal confidential or proprietary information for competitive advantage or to damage the reputation of an organization.
- **Political or ideological motives**: Some cyber criminals target organizations or individuals for political or ideological reasons, such as to promote a particular cause or to advance a particular agenda.(e.g. ISIS targets military websites, Govt websites for spreading hate and propaganda).
- **personal motives**: Some cyber criminals engage in cyber crime to harass, defame or harm individuals or organizations.

Volume 31, March 2024 ISSN 2581-5504

- **Opportunism**: Some cyber criminals engage in cyber crime simply because they can, taking advantage of security vulnerabilities in technology or in people to steal information or resources.
- **Lack of Awareness:** Many cyber crimes are committed by individuals who are unaware of the consequences of their actions and the legality of their activities.

Effects of Cybercrime on Different Entities

Cybercrime is a growing threat to individuals in the digital age. With the increasing sophistication of cyberattacks, individuals are becoming more vulnerable to financial loss, identity theft, emotional trauma, and damage to their reputations.

1] On Individuals

- **Financial loss or loss of income :** One of the most common effects of cybercrime on individuals is financial loss. Cybercriminals often use various methods such as phishing, hacking, and malware to gain access to an individual's financial information, such as credit card numbers, bank account details, and passwords. This can result in the loss of money through unauthorized transactions, which can be difficult to recover.

- **Identity theft:** Identity theft is another significant consequence of cybercrime for individuals. Cybercriminals can use stolen personal information such as social security numbers, driver's license numbers, and dates of birth to open new accounts, take out loans, and commit other types of fraud in an individual's name. This can result in financial loss and significant legal and administrative headaches in recovering the individual's identity.

- **Emotional trauma:** In addition to financial loss and identity theft, cybercrime can cause emotional trauma. Victims of cybercrime often feel violated and vulnerable, leading to fear and anxiety. This can have a long-lasting impact on an individual's mental health, especially if they feel isolated and unable to seek help.

2] On Businesses

- **Financial loss:** Cybercrime can have devastating financial consequences for businesses, particularly small and medium-sized enterprises. A successful cyberattack can result in the loss of funds, intellectual property, and customer data, which can be costly to recover. In some cases, businesses may even be forced to shut down due to the financial impact of cybercrime.

- **Damage to reputation:** Cybercrime can cause irreparable damage to a business's reputation. A successful cyberattack can expose sensitive customer data, undermining trust and confidence in a business's ability to protect its customers'

Volume 31, March 2024 ISSN 2581-5504

information. This can lead to losing loyal customers, decreasing revenue, and reducing market share.

- **Legal repercussions:** Businesses can face significant legal repercussions as a result of cybercrime. Data breaches can result in legal action, fines, and penalties, particularly in heavily regulated industries like healthcare and finance.

- **Loss of intellectual property:** Cybercriminals can target businesses to steal intellectual property, such as trade secrets and patents. The loss of intellectual property can be a significant blow to businesses, particularly those that rely on innovation and research to remain competitive. It can further lead to decreased revenues, lost opportunities, and reduced market share, potentially affecting the long-term sustainability of the business.

3] On Society

- **Economic impact:** Cybercrime can have a significant impact on the economy. It can result in financial losses for individuals, businesses, and governments. The cost of repairing damage to systems, recovering lost data, and preventing future attacks can be substantial. It can also impact consumer confidence in online transactions, decreasing business sales and revenue. Additionally, cybercrime can result in the loss of intellectual property, negatively affecting industry innovation and competitiveness.

- **National security concerns:** Cybercrime can pose a serious threat to national security. Attacks on government and military networks can compromise sensitive information and disrupt operations. Cybercriminals can also use technology to engage in espionage, stealing state secrets, and disrupt critical infrastructure, such as power grids and transportation systems. Additionally, cybercrime can be used for political and ideological purposes, leading to social and political unrest.

- **Impact on healthcare and public safety:** Cybercrime can have a significant impact on healthcare and public safety. Attacks on healthcare systems can compromise sensitive patient data and disrupt medical services, which can have life-threatening consequences. Additionally, attacks on critical infrastructure, such as emergency response systems and transportation networks, can put public safety at risk. Cybercriminals can also use technology to commit identity theft, which can financially harm individuals.

- **Increase in cyberbullying and harassment:** Cybercrime can lead to an increase in cyberbullying and harassment. Cybercriminals can use technology to target

individuals and groups, spreading malicious content and harassing messages. This can result in emotional and psychological harm and damage to reputations and relationships. Cyberbullying and harassment can also hurt mental health, leading to depression and anxiety. Additionally, cybercrime can spread misinformation, which can have serious social and political consequences.

- **Social media manipulation :** A social media manipulation is a form of cybercrime involving using social media platforms to influence, deceive, or manipulate individuals or groups for political, financial, or personal gain. This can take many forms, including spreading false information, creating fake profiles or personas, and using bots or automated accounts to amplify messages.

The Psychology of Cybercriminals: Understanding the Mind of a Hacker

What Drives Cybercriminals?

Cybercriminals are motivated by a variety of factors, including financial gain, personal satisfaction, and even political or ideological beliefs. Financial gain is a significant motivator, as many hackers engage in cybercrime as a means of making money. This can include stealing financial information, selling stolen data on the dark web, or even holding data for ransom. Personal satisfaction is another motivator, as many hackers are driven by the challenge of breaking into secure systems. These hackers often see themselves as skilled and knowledgeable, and the successful exploitation of a system can bring a sense of achievement and self-esteem.

Hacktivism is another motivation for some cybercriminals. These hackers may be motivated by political or ideological beliefs and may use their skills to attack websites and systems associated with organizations or individuals they oppose.

The Psychology of Cybercriminals

Cybercriminals often exhibit certain psychological traits, such as impulsivity, thrill-seeking, and a lack of empathy. These traits can lead to a lack of concern for the consequences of their actions, including the harm they may cause to individuals or businesses. Many cybercriminals also exhibit a high degree of intelligence and creativity, which they use to find vulnerabilities in security systems and develop sophisticated methods of exploitation.

Cybercriminals are becoming increasingly merciless and show no signs of pity towards individuals or organizations. It is evident that cyber criminals will stop at nothing to gain unauthorized access to confidential information. To effectively combat malware attacks, strict cyber laws are necessary, and the use of malware is punishable in many countries. In today's world, we are constantly dealing with the troublesome and often devastating effects of increasingly sophisticated malware attacks. Not only criminal organizations, but even well-respected businesses and organizations have been found to be involved in spreading malware. One does not need to be a skilled programmer or have specialized technical knowledge to

purchase, design, or spread malware. With the aid of malware kits, one can easily create powerful malware and distribute it within an organization. Purchasing malware is also incredibly easy - it can be done in just a few minutes. Paid malware tools typically come with customer support, including free updates and troubleshooting services

Cyber criminals have shown no mercy towards individuals and organizations, and their malicious activities continue to rise unabated. It is evident that cyber criminals will stop at nothing to gain unauthorized access to confidential information. Therefore, strict cybercrime laws must be enforced globally to address this pressing issue and ensure the safety of individuals and organizations in the cyberspace. Cyber security attacks are not confined to any specific jurisdiction, unfortunately, every corner of the world is affected by these actions. however at the same time the advantage of cyberspace actually is acting as a disadvantage at this moment when any offender use malware while sitting in one country and affecting and targeting the computer systems of any other country or jurisdiction. To penalize any offender act should be declared as an offense in any law but unfortunately, the emergence of this new crime challenged the criminal justice system of every country to counter these illegal activities.

---

*There are two maxims explaining the concept of criminal liability. First, "**nullum crimen sine lege,**" meaning one cannot be punished for doing something which is not prohibited by law, and "**nulla poena sine lege,**" meaning that one cannot be punished for doing any act for which no punishment is prescribed in law. These principles state that any action that is not expressly prohibited by law is not a crime. These maxims explain that a person cannot be punished for any wrongful act unless it is prohibited by law, and similarly, no one can be punished if the act is not prescribed by the law. Over time, due to advancements and new kinds of wrongful acts, different actions have been committed, but people are not prosecuted until they are expressly prohibited by law. This was the time when offenders got the benefit of the non-availability of relevant laws hence they escaped from the legal liability for such acts.*

What is fear culture in cyber crime

Illegitimate activities, factors or consequences arising out of the cybercrimes which creates fear in the mind of an individual is a fear culture.

Not only physical mobility, but also the development of information technology has further facilitated the "erasure" of borders; it is becoming more difficult to uncover and track certain illegal activities. Perpetrators thus gained access to a new world of unlimited opportunities. We are daily provided with news about new developments in information technology and communications. The evolution of the Internet has boosted development in other areas of information and communication technology. Mobile devices and cloud computing are among

Volume 31, March 2024 ISSN 2581-5504

the biggest technological breakthroughs, because they facilitate simple and fast connections to the Internet. Cybercrime provides numerous beneficial opportunities, but also dangers for the naive users.

Cybercrime should be analysed from at least two standpoints – one of the victim, the other of the perpetrator. there can be no fear until people are aware of the threats, but on the other, excessive sensibility to deviant behaviour can lead to exaggerated reactions to information security threats. The fear of cybercrime is related to an evaluation of personal danger and an estimate of the cost of mitigating the damaging consequences if one becomes a victim of cyber criminals.

Besides being aware of the numerous benefits of using cyberspace, one should also give thought to various threats 'lurking' in cyberspace. How aware a user is of the potential dangers depends on how well he knows their sources and how risky he thinks working in cyberspace is. Users believe that using computers for work, exchange of data and browsing multimedia contents is mostly safe, but relatively unsafe when they are directly connected to the Internet. An attentive individual usually worries about cybercrime, and he performs the required precaution in order to avoid being a victim of cybercrime. A habitual individual is unconcerned about being a victim of cybercrime, but he does his best to follow the standards and procedures that are given to him.

individuals with prior cybercrime victimization experiences, women, and individuals with lower social status and lower confidence in their ability to use the Internet report higher levels of fear.

There is a concept called vulnerability that is often used in the literature on victimization. Falling victim to a crime may have economic, physical, emotional and social repercussions for an individual. How vulnerable the status of the victim is in relation to the victimization experience has a significant impact on how grave these consequences are. vulnerability is seen as the intersection between two axes: risk and harm. Any given individual may be plotted in respect of his or her level of risk of being victimized and the amount of harm the victimization experience may cause , In this context, **fear** can be described as the behavioural outcome caused by the cognitive assessment of victimization risk. For example, fear of crime reflects an emotional reaction, such as how concerned or afraid one is of being victimized while walking alone at night, When looking at cybercrime, studies have found that women report higher levels of fear of crimes such as cyber harassment and bullying or online interpersonal victimization.

Despite the increasing prevalence of cybercrime and its study by criminologists, there is little evidence about the extent, nature and impact of fear of cybercrime. The limited evidence that does exist suggests that individuals may be more concerned about becoming victims of cybercrimes than of most types of terrestrial crimes. For example, preliminary data in England and Wales show that individuals are more worried about cybercrime victimization than they are about burglary or physical assault victimization.

Volume 31, March 2024 ISSN 2581-5504

Gaps in cyber crime

Earlier cyber crime laws were non-existent, information on the topic was scarce, and there were only a handful of investigators working these types of cases. Today, cyber crime laws are still poorly worded or simply don't apply to the types of crimes being investigated. Additionally, many cyber crimes laws still vary from state to state. Attempts to address cyber crimes in the law are thwarted by the speed at which technology changes compared to the rate at which laws are created or revised.

To be very honest uniform law can hardly be applied when It comes to electronic crime. . It is found that laws were often outpaced by the speed of technological change. These gaps in the law were created by the length of time it took for legislation to be created or changed to meet the prosecutorial demands of cyber crimes. legal issues will continue to be raised as lawmakers and legislators struggle to find ways to respond adequately, and immediately, to change when technology affects the law.

When we remove the veil of mystery surrounding cyber-related crime, an amazing thing happens: we start to remember that a crime has occurred. Unfortunately, when dealing with computer crime investigations, many investigators forget that ultimately the underlying fact is that someone committed a crime. Almost every cyber crime has, at its base, a good-old-fashioned crime attached to it. In a computer tampering case, there is some act of criminal mischief, larceny, or destruction of property. In a cyber stalking case, there is ultimately an underlying harassment. In fact, only a few "True Cyber Crimes" could not exist without the use of a computer. Crimes like web site defacing, Denial-of-Service attacks, worm propagation, and spamming could not occur without a computer being involved. Even though a computer is required to commit these types of crimes, the acts themselves may still be covered under traditional crime definitions.

> *once an investigator removes the computer aspect of the crime out of the criminality equation (Computer + Crime = Cyber Crime) the investigator will ultimately reveal the underlying crime that has occurred (Crime = Crime).*

There are many challenges in front of the government of any country to fight against the growing cyber crime. Few Of The Cyber Crime Challenges Are Given As Under:

1) Lack of trend and qualified manpower to implement and development the rising issues of Cyber space
2) There is lack of social awareness and cyber attacks have not only given rice to the cyber terrorism but also the cyber crime hackers are getting better Day After day as there is sample of material available in the internet about cyber crimes and hacking.

Volume 31, March 2024 ISSN 2581-5504

3) Research and development programmes and promotions of the ICT department is not up to the mark.
4) There is minimum knowledge of computer sectors in Indian cyber cell most of the candidate in the cyber cell department are illiterate and they have less amount of knowledge than young hackers in society.
5) The government budget passed for security purpose of the cyber law enforcement and training programs is lesser as compared to other crimes in the country which needs to be taken care of.
6) The latest technologies & the working speed of young & updated cyber hackers always beats the progress of speed in the government sectors and departments that are taking care of Cyber cell due to which the government is unable to identify the original sources of Cyber crime networks usually and is unable to catch the hackers or the cyber terrorist.
7) The current laws and regulations made by the government for the betterment of Cyber cells in India is not sufficient that needs more development and more strict laws should be past for the betterment of Cyber space and internet users should be well aware by the government programs and schemes like other criminal activities the cyber crime is also an essential part of our daily life and betterment of the national privacy

How cyber criminals operate?

Before the Internet, criminals had to dig through people's trash or intercept their mail to steal their personal information. Now that all of this information is available online, criminals also use the Internet to steal people's identities, hack into their accounts, trick them into revealing the information, or infect their devices with malware. Most cyber crimes are committed by individuals or small groups. However, large organized crime groups also take advantage of the Internet. These "professional" criminals find new ways to commit old crimes, treating cyber crime like a business and forming global criminal communities.

Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities. It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location on the globe. Many computers used in cyber attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country too, which can make things really complicated when a criminal launches an attack in another country.

Attack techniques

Here are a few types of attacks cyber criminals use to commit crimes. You may recognize a few of them:

- **Botnet** - a network of software robots, or bots, that automatically spread malware

Volume 31, March 2024 ISSN 2581-5504

- **Fast Flux** - moving data quickly among the computers in a botnet to make it difficult to trace the source of malware or phishing websites
- **Zombie Computer** - a computer that has been hacked into and is used to launch malicious attacks or to become part of a botnet
- **Social Engineering** - using lies and manipulation to trick people into revealing their personal information. Phishing is a form of social engineering
- **Denial-of-Service** attacks - flooding a network or server with traffic in order to make it unavailable to its users
- **Skimmers** - Devices that steal credit card information when the card is swiped through them. This can happen in stores or restaurants when the card is out of the owner's view, and frequently the credit card information is then sold online through a criminal community.

Some identity thieves[2] target organizations t[1]hat store people's personal information, like schools or credit card companies. But most cyber criminals will target home computers rather than trying to break into a big institution's network because it's much easier.

By taking measures to secure your own computer and protect your personal information, you are not only preventing cyber criminals from stealing your identity, but also protecting others by preventing your computer from becoming part of a botnet.

Social engineering is a tactic used by cyber criminals that uses lies and manipulation to trick people into revealing their personal information. Social engineering attacks frequently involve very convincing fake stories to lure victims into their trap. Common social engineering attacks include:

- Sending victims an email that claims there's a problem with their account and has a link to a fake website. Entering their account information into the site sends it straight to the cyber criminal (phishing)
- Trying to convince victims to open email attachments that contain malware by claiming it is something they might enjoy (like a game) or need (like anti-malware software)
- Pretending to be a network or account administrator and asking for the victim's password to perform maintenance
- Claiming that the victim has won a prize but must give their credit card information in order to receive it

[1] Stealing somebody else's personal information to pretend to be them. People usually do this to steal money from someone's bank account or buy things with their credit cards.

- Asking for a victim's password for an Internet service and then using the same password to access other accounts and services since many people re-use the same password
- Promising the victim they will receive millions of dollars, if they will help out the sender by giving them money or their bank account information

Like other hacking techniques, social engineering is illegal in the United States and other countries. To protect yourself from social engineering, don't trust any emails or messages you receive that request any sort of personal information. Most companies will never ask you for personal information through email. Let a trusted adult[2] know when you receive an email or message that might be a social engineering attack, and don't believe everything you read.

For a hacker who wants to come clean and turn away from crime, one option is to work for the people they used to torment, by becoming a security consultant. These hackers-turned-good-guys are called Grey Hat Hackers. In the past, they were Black Hat Hackers, who used their computer expertise to break into systems and steal information illegally, but now they are acting as White Hat Hackers, who specialize in testing the security of their clients' information systems. For a fee, they will attempt to hack into a company's network and then present the company with a report detailing the existing security holes and how those holes can be fixed.

The advantage of this is that they can use their skills for a good cause and help stop other cyber criminals. Keeping up with security and cyber criminals is a full-time job, and many companies can't afford to have someone completely dedicated to it. Grey Hat Hackers have real-world hacking experience and know more methods of infiltrating networks than most computer security professionals. However, since they used to be criminals there's always going to be a question of trust.

Modus Operandi of cyber criminals

• Dissemination of Malware through google forms , software downloads etc.

• Social engineering :use of psychological tactics to trick individuals into revealing confidential information .

• Remote Access: exploiting vulnerabilities in software or hardware, IoT devices, tricking a user into providing remote access for tech support.

• SQL Injection: technique used to exploit vulnerabilities in databases to steal or manipulate information.

• Cross-Site Scripting (XSS): type of security vulnerability that allows attackers to inject malicious code into websites.

[2] An adult that you trust, like a parent or teacher, whom you can talk to about anything weird or icky that you encounter in cyberspace. Your trusted adult can help you solve problems and come up with strategies for keeping yourself and your devices safe.

Volume 31, March 2024 ISSN 2581-5504

• Man-in-the-Middle attacks: attacker intercepts and potentially modifies communication between two parties.

Types of malware and their impact

Malware is categorized as viruses, worms, Trojan, spyware, adware, and ransomware. Some types of malware are more dangerous and have severely affected individuals and organizations in terms of financial loss and reputation. For instance, ransomware has proven to be more effective and dangerous during the last decade for the healthcare sector and government organizations.

1. **Viruses and worms -** A computer virus is much similar to the flu virus. It is designed to spread from computer to computer. It needs a host to replicate itself. In order to execute its code and cause maximum damage to its host machine, it attaches itself to some file or program such as a document, email, text message, and even social media scam links.[3] Once, the virus has infected the host machine, the virus can spread through the network and infect other machines on the same network. Mobile devices and smartphones can become infected with mobile viruses through shady App downloads. Stealing passwords, data and even bank details, logging keystrokes, corrupting files, spamming email contacts, and even taking over machines are some of the most devastating, damaging, and irritating things a virus can do.

    a. Similar to computer viruses, worms are also capable to do devastating and damaging things to individuals and organizations. The difference between a virus and a worm is that a virus needs to attach to another program like a word processor or web browser to make it work. By contrast, a worm is self-contained and can run, copy, and send copies of itself all on its own. Some of the most dangerous computer viruses are actually worms[4]

    b. **Ransomware -** Ransomware attack attempts to prohibit computer users from retrieving data stored on a computer or accessing the computer system. The attacker encrypts the whole storage media or some data stored on it and then demands the ransom from the victims to allow access to it. Users are shown instructions on how to pay a ransom to get the decryption key. For the reason that attackers and cybercriminals remain intractable, they demand ransom to pay in cryptocurrency such as Bitcoin which is an anonymous and virtual currency. Some ransomware can also spread to other machines in a network such as, in May 2017 Wannacry malware seriously disrupt and damage the healthcare sector. Similar to easy access viruses and worms kits,

[3] Gupta, Sanskar, et al. "Comparison, analysis and analogy of biological and computer viruses." *Intelligent Interactive Multimedia Systems for e-Healthcare Applications* (2022): 3-34.
[4] Zou, Cliff Changchun, et al. "The monitoring and early detection of internet worms." *IEEE/ACM Transactions on networking* 13.5 (2005): 961-974.

Volume 31, March 2024 ISSN 2581-5504

ransomware kits are also available on the dark web to carry out the ransomware attacks also known as *ransomware-as-a-service*.

Numerous studies has shown that the vast majority of business organizations and healthcare sectors have experienced significant loss in revenue, damage to the brand's reputation and, even closure of the business due to the successful ransomware attacks. Business and healthcare organizations are struggling to protect themselves from their damaging effects. Ransomware attacks are on the rise. A full recovery of data is not guaranteed even after fulfilling the ransom demands of the attacker. In reality, it has exacerbates the number of ransomware attacks by encouraging the attackers. There is an urgent need to establish, enforce and implement strict cyber laws and punishments to mitigate them.

c. **Spyware -** Spyware is malicious software that is used by cyber criminals to spy on the victim's information and activities. Upon downloading on the victim's device, it secretly monitors and records all the activities of the victim such as login name and password credentials, credit card and bank details, and browsing and searching history. This information is then transferred to the attacker via the Internet who uses this information for his own benefits or sells it to a third party such as advertisers, spammers, scammers, or hackers. Spyware can also cause other severe damages such as locking a victim's device, disabling antivirus programs or security related notifications, recording live videos and taking pictures using a mobile camera (front and back camera), viewing device specifications, installing or uninstalling apps, recording conversations using the microphone, track victim's current geographic location and transferred it to the third party, record incoming and outgoing calls and so on.[5]

d. **Adware -** Adware is a type of malware that automatically generates and displays unwanted and irritating advertisement notifications on computer screens to generate revenue for its developer. Some adware is extremely malicious and upon clicking on the advertisement, redirects the users to the malicious websites containing adult content. It harms the device by slowing down its speed and performance. It also installs unwanted plug-ins, toolbars and extensions in the browser without the consent of a user. Some adware also creates a backdoor for cyber criminals. Fireball, Appearch, DollarRevenue, Gator, and DeskAd, are the most popular adware softwares. Developed in 2015 by the afotech, a Chinese digital marketing agency, Fireball has infected more

[5] Anumula, Kalyan, and Joseph Raymond. "Adware and spyware detection using classification and association." *Proceedings of International Conference on Deep Learning, Computing and Intelligence: ICDCI 2021*. Singapore: Springer Nature Singapore, 2022.

than 250 million computers and one-fifth of corporate networks around the world. DollarRevenue, developed in Netherland in 2005 has infected 22 million devices worldwide by the end of 2007. Its developer was punished by fined one million euros in 2007, however, the decision was revoked after six years of punishment[6]

2. **Trojan -** A Trojan is a deceptive malware that disguises itself as a legitimate program and upon downloading on the victim's device continues to spy on the victim's activities or steal private information. Like viruses, Trojan hides into a file or document to be downloaded and attach to an email, then transfer to the victim's device upon downloading the file or document. Like viruses and worms, they spread from computer to computer through the internet and network.

3. Cyber Criminals use Trojan to gain backdoor access into the business organization and control the devices and network remotely without the consent of the users. A cyber criminal turns a computer system into a zombie to continue the spread of malware into the network. The zombie computer system is also known as a botnet.

Conclusion

Better legislations with increasing Ambit of Cyber internet space is very necessary such legislations should be governing nationally as well as internationally to avoid the issues and contradiction of laws between the Nations having cyber crime problems.

As the growing number of Cyber crime in the country, it is very necessary that the present dispute resolution structure given under information and technology act of 2000 maybe strengthened. The authorities of IT act are responsible for a huge range of concerns which includes data privacy cyber offences cyber security concerns and responsibility of keeping the data of every internet user safe. Such authorities must be developed so that they can bring a well developed and better regulatory structure for the increasing number of Cyber attacks in the nation.

Cybercrime is a significant threat that can bring huge loss to the individual and the organization. It is essential to follow basic online rules to ensure the safety of self and the organization. The Internet is often described as a wonderful tool, an engaging place and a liberating experience but for whom? There is the potential for many of us to become victims to the growing pool of criminals who skilfully navigate the Net. Cyberspace often known as Web is an environment that is intangible and dynamic.

Criminal behavior on the Internet, or cyber crime, presents as one of the Major challenges of the future to India and International law enforcement. As ICT become even more pervasive, aspects of electronic crime will feature in all forms of criminal behavior, even those

[6] https://scholar.google.com/scholar?q=What%20is%20adware%3F%20the%205%20examples%20you%20need%20to%20know.%20URL%20https%3A%2F%2Fsoftwarelab.org%2Fwhat-is-adware%2F#d=gs_qabs&t=1711017387088&u=%23p%3DVjnYITcg9HAJ

Volume 31, March 2024 ISSN 2581-5504

matters currently regarded as more traditional offences. It already feature in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes, and we must be prepared to deal with this new challenge.

Law enforcement agencies around the world are working together to develop new partnerships, new forensic methodologies and new responses to cyber crime in order to ensure safety and security on the Internet. New skills, technologies and investigative techniques, applied in a global context, will be required to detect, prevent and respond to cybercrime.

REFERENCES:

- https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
- https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-anoverview.html
- https://hbr.org/2023/04/cyber-thieves-are-getting-more-creative
- https://www.drishtiias.com/daily-updates/daily-news-analysis/cyber-crime-4
- https://journals.sagepub.com/doi/10.1177/0032258X221107584
- https://www.infosecurity-magazine.com/cybercrime/
- https://www.un.org/en/chronicle/article/fighting-industrialization-cyber-crime
- https://rjhssonline.com/HTMLPaper.aspx?Journal
- Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 5, Issue 8
- https://cybertalents.com/blog/cyber-crime-investigation
- https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019 survey/articleshow/75093578.cms
- https://www.tandfonline.com/doi/abs/10.1080/13691180802007788#:~:text=Reactions%20which%20heighten%20the%20culture,the%20subsequent%20interpretation%20of%20justice.
- https://www.researchgate.net/publication/228264135_Cybercrime_and_the_Culture_of_Fear_Social_Science_Fictions_and_the_Production_of_Knowledge_about_Cybercrime_Revised_Feb_2011
- https://www.vedantu.com/english/cyber-crime-essay
- https://www.britannica.com/topic/cybercrime
- https://vc.bridgew.edu/ijcic/
- N. Roshan, 'What is Cyber Crime- Asian School of Cyber Laws', available at: www.aclonline.com
- Ashabhari Thakur, 'Determination of jurisdiction in cyber crimes- issues & classification', 2019, available at: www.legalpedia.in
- www.mondaq.com/india/securty/623820/cyber-laws-in-india
- Ikigai law, 'DRM framework of cyber crimes under IT act, 2000,' available at: www.ikigailaw.com

- Dr. S. Poonia, 'Cyber Crime: Challenges & its Classification', Vol. 6, issue 10, available at: www.ijettcs.org
- Ajzen, I., "The theory of planned behavior," Organizational Behavior and Human Decision Processes 50X, 1991, 179--211Google Scholar
- Alshalan, A. (2009). Cyber-Crime Fear and Victimization: An Analysis of a National Survey.Google Scholar
- Saarbrücken: VDM Verlag Dr. Müller Chin, W. W. (1998) "The partial least squares approach for structural equation modelling," In Modern Methods for Business Research (Ed, Marcoulides, G. A.) Lawrence Erlbaum Associates, Hillsdale, 295--336Google Scholar.
- Alshalan A. (2006). Cyber-Crime Fear and Victimization: An Analysis of a National Survey. Mississippi: Mississippi State University. [Google Scholar]
- Clememte F., & Kleiman M. B. (1976). Fear of crime among the aged. The Gerontologist, 16(3), 207–210. [PubMed] [Google Scholar]
- Collins R. E. (2016). Addressing the inconsistencies in fear of crime research: A meta-analytic review. Journal of Criminal Justice, 47, 21–31. [Google Scholar]
- Empirica (2007). Benchmarking in a Policy Perspective: Security and Confidence. Empirica. [Google Scholar]
- European Commission (2013) Eurobarometer 79.4: Social Climate, Development Aid, Cyber Security, Public Transport, Anti-Microbial Resistance and Space Technology. ICPSR36038-v1. Cologne, Germany: GESIS/Ann Arbor, MI: Inter-university Consortium for Political and Social Research [distributors], 2015-07-08 10.3886/ICPSR36038.v1 [CrossRef] [Google Scholar]
- European Commission (2016) A digital single market in Europe: Bringing down barriers to unlock online opportunities. The European Union Explained. Luxembourg: Publications Office. [Google Scholar]
- Ferraro K. F. (1995). Fear of crime: Interpreting victimization risk. Albany: State University of New York Press, Albany. [Google Scholar]
- Killeas M. (1990). Vulnerability: Towards a better understanding of a key variable in the generis of fear of crime. Violence and victims, 5, 97–108. [PubMed] [Google Scholar]
- LaGrange R. L., & Ferraro K. F. (1989). Assessing age and gender differences in perceived risk and fear of crime. Criminology, 7(4), 697–720. [Google Scholar]