EMERGING CYBER CRIME TRENDS IN INDIA AND PREVENTION STRATEGIES

Author: Bhagavatula Naga SaiSriram, V year of B.B.A.,LL.B.(Hons.) from SASTRA University

Abstract

As India is advancing in to the digital era Internet access is required. Any kind of information can be shared with anyone in different formats such as in audio, video and pdf formats etc. through the usage of an interconnected network which is known as Internet in common parlance. The usage of internet has grown rapidly in India since the past decade. In India almost every single family owns a gadget with Internet access. Today the Internet is widely used for all daily activities such as payment of bills, transferring money, E commerce and online shopping, exchanging business information and many more which are heavily dependent on Internet. As the usage of Internet is mounting day by day the vulnerabilities faced by the internet users is also increasing. In this decade, the misuse of the internet has been widely spreading for the commission of various crimes on cyberspace which are generally known as cyber-crimes or computer related crimes or internet related crimes. There is no substantial difference between the crime committed in cyber space and a crime committed in real world except the medium used for the commission of crime. Cyber-crimes are nothing but the crimes of the real world perpetuated in the cyber space through the usage of various mediums such as computers and internet. In the contemporary eraCyber Crime is not only a matter of national concern but also it has become a matter of global concern as trans-national crimes are being committed. Therefore the world at large has to come forward to deal with this problem of cyber-crimes. The present research paper starts with introduction and ends with suggestionsandconclusion. An attempt has been made to focus on the Definition and Evolution of cyber-crimes, Forms and Categorization of cyber-crimes, Reasons for such cyber-crimes, systematic analysis of historical development of the Cyber-crimes including Emerging Cyber-crimes in India during various periods. Finally the Conclusion and Suggestions part contains the recommendations as well as concluding remarks of the present research area and highlights the suggestions for improvements in the current scenario related to cyber-crimes at the national and International level.

Keywords: Cyber Crime, Internet, Cyber Space, Emerging Trends, Cyber Crime Prevention.

Introduction

In today's era of technology, now the internet and computers, smartphones are being used in almost every sector, and our day to day activities have become completely dependent on the internet, smartphones and computers. Cybercrime threats have also increased with the increase in digitization and internet usage by the people. Several forms of cyber-crime increased the concern of cyber security. Cyber-Crime is rampant throughout the world in this decade and cyber-criminals have no distinction between poor or rich nations; they attack both equally. When it comes to technical advancements and aspects of cyber security, developing nations usually fall behind. Developing countries like India are an easy target for cybercrimes because the countries are not familiar with Cyber Security and effective legislations to prevent cyber-crime. Cybercrime is an emerging global issue as it is both difficult to detect and emotionally draining to investigate and identify the sources or cyber-criminals.

The word cybercrime was first time proposed by Sussman&Heuston in the year 1995. The Cybercrimes are also generally known as electronic crime, computer crime. The term "cybercrime" encompasses any unlawful activities carried out through or targeting a digital device, computer or information system. A distinguishing feature of cybercrime as compared to real world crimes is that in cyber-crimes the victim and the wrongdoer have no direct connection. Most of the time, cyber-criminals carries out their operations such as hacking from a country where there are non-existent or weak cybercrime laws. Because of this reason the chances of reduction of cyber-crimes and prosecution of cyber-criminals become very less. Cybercrimes are directly proportional to cyber law as they form an essential part of the study. There is no concrete definition for the term cyber law but in common parlance, it can be stated that the laws which are governing cyber space are cyber laws.

Definition and evolution of cyber crimes

As per the definition available at Britannica "Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy"[1]

[1] "Cybercrime" available at https://www.britannica.com/topic/cybercrime

In simple terms it can be stated that it is a criminal activity which uses computers or information systems as the source, instrument or target of the crime.

In recent days, we have witnessed various incidences such as hacking, email bombing, spreading of viruses, ransom ware attacks and obtaining unauthorized access to sensitive data and information. That's the reason why it can be stated that crimes committed in cyberspace relating to technology/devices or information systems are to be regarded as cybercrimes. Some of these crimes committed through the internet include hacking, phishing, fraud, pornography, theft of Intellectual Property (IP) such as copyrighted books and music illegally, piracy as well as other forms of cybercrime like viruses, worms and spyware attacks.

Evolution

Starting from the Morris Worm to the ransomware, piracy and data leaks cybercrime has evolved. Despite the efforts of several nations, including India, which have passed legislation relating to the regulation of cyber space and to prevent cyber-crimes these acts continue to alter and influence the country. The changes in cybercrime may easily be tracked and compared to the changes in the Web. Of course, the initial offenses were simple intrusions into neighbouring networks to steal data yet as the Web turned out to be more established so too did the attacks turned out to be more advanced which completely drains the online users data.

Forms and categorization of cyber crimes

Forms Cybercrimes have numerous forms such as crimes committed against the individuals, Government, property, organization. Phishing, Hacking, Identity theft, Email bombing, piracy including copyright infringement and pornography are some common forms of cyber-crime in the present day scenario.

Categorization Cybercrimes can be categorized into two ways[2]. In one way, where the computer organization, information systems or PC based gadgets are focusing on causing a

[2] "Cyber Law & Information Technology" by Talwant Singh Additional District & Sessions Judge, Delhi at p.2

denial of service, communicating of virus or malware in to another device. In the second direction where offences are facilitated by computer systems or gadgets like smart phones. Online stalking, digital extortion, identity theft, spamming, and leaking of sensitive or delicate data of individuals can be stated as examples.

Cybercrime can be divided into the following major categories [3]

a) **Cyber-crime against individuals**–Few examples of cybercrimes committed against individuals such as: -Email-based harassment is a form of harassment, Dissemination of pornographic material, the practice of cyber-stalking, and defamation are both crimes. Affectation of a computer system or exposure to obscene content without authorization, Phishing for email addresses, Fraud[4]

b) Cyber-crime against Property- Vandalism of computers, crimes targeting Intellectual property of the persons, online threats, and other crimes against property are examples of this kind of crime. The following are examples of Intellectual Property (IP) crimes: - Computer thievery, Virus transmission, trespass, Software piracy, Copyright Violations, and Trademark Violations are all examples of intellectual property offences,

c) Cyber-crime against Government - Cybercrimes against public organizations and companies is the term used to describe certain types of cybercrimes. To instil fear in the public, these types of crimes are performed. Crimes against a government, such as cyber terrorism, are referred to as such. When it comes to cybercrimes against the government everything from cyber-attacks on government websites to cyber terrorism on military ones can be included to the list. Control of a computer system without authorization. Unauthorized possession and leaking of information related to a particular country can also be included in this type of cyber-crime.

d) Cybercrimes against society – Cybercrime against society are those which harm society as a whole. Examples of these crimes include: Pornography involving children, the indecent exposure of financial crimes, contaminating children, the sale of unauthorized goods, Trafficking, Forgery, and Gambling such as Rummy and inducing people related to these activities.

[3] Cyber Space- Cyber crime- Academike, Available at https://www.lawctopus.com/academike/cyberspaceandcyber-crime/
[4] https://www.cybrary.it/blog/0p3n/introduction-to-computer-forensics/

Reasons for cyber crimes

Predominantly Cybercrime is the result of technological development.The reasons for the cyber- crimes may quickly be expressed as follows

1) Increasing the number of internet users makes the job of cybercriminals easier as much personal information of the users is stored online.

2) The lack of awareness to the users.

3)Money is a main motivation for the cyber-criminal as they demand money by hacking and ransom ware attacks.

4) Lack of efficiency of police and lack of resources to identify and prosecute cybercriminals.

Emerging cyber-crimes in India during various periods

2.2.1 Cyber Crimes in the Period of 1820 To 2000

- In 1820, Cyber Crime was recorded first time. The modern period commenced with the analytical engine of Charles Babbage. It was called as the primary recorded cyber crime in the set of experiences. On that time, cyber crime was disruption of the phone organization. The history of the Hacking was indicated or copy by the use of new branded Telephone in the year of 1870 for the Telephone Phreaking by the teenagers.
- In 1970s, in USA, the main purpose of the hackers was damages to the computer centers. German had passed a law against cyber crime named as Data Protection Act 1970 by the use of new digital technology. It was the world's first Computer Specific Law.
- In 1990, Hackers hacked in the Griffith Air Force Base, computer at NASA. In the year of 1992, Dark Avenger developed first Polymorphic virus.

2.2.2 Cyber Crimes in the Period of 2000 To 2010

- In the year of 2000, New Delhi Police investigate a case named Phone Tapping Operation and found out that a cricketer of the South Africa who was captain in the team named as Hansie Cronje had committed an offence of the conspiracy with SanjeevChawla (Indian Bookmaker) to fix a South African tour to India in February-March 2000.

- Then in India, in the year of 2004, there was a landmark case. The case named as **State of Tamilnadu v SuhashKatti** This is a 1st case of punishment of sec 67 of IT act,2000. In this, criminal posted some obscene, defamatory and provoking or irritating messages against the victim on the Yahoo. Then she filed the First Information Report. After the investigation it was found that he was guilty. Then it was held by the court that offender was convicted for the annoying phone calls and messages under the section of 469 and 509 of IPC, 1860 and sec 67 of IT Act, 2000.
- Later in 2009, public websites named as Facebook and Twitter had spreading with the high level. On Social sites, now users can post his personal information also. In other way we can say that now user posted his personal details just like his hometown, current location and job details etc. Then criminals had started to collect the personal details of the users. At this time, cyber criminals had become very professional or expert for the commission of cybercrime. Now they started stealing the details of credit card of the users also by contacting them from the details available on the net.

2.2.3 Cyber Crimes in the Period of 2010 To 2019

- Then in the year of 2010, Google first time formally declared that it was beat by the Cyber Attack such as Operation Aurora.
- According to the report of NCRB, Cyber Crimes are increasing by 50 percentage from the year of 2012 to 2013. The NCRB recorded only those cases which are registered under the Cyber Crime with motive and suspicion. Mostly Cyber Criminals are arrested under the age of 18 to 30years. In 2013, Maharashtra is in the top list of the cybercrime.

2.2.4 Cyber Crimes in the Period of 2019 To Present

- Cybercrimes are turning into a reality in India as is obvious from the growing internet usage. 88% of associations overall experienced lance phishing endeavours in 2019.
- In 2019, Facebook related crimes were 19%. And 78% are victims of financial loss and identity theft.

2.2.5 Cyber-crime during Covid-19

- During the lockdown period, people are progressively accessing social networking websites just like Instagram, Facebook, and Twitter, as well as watching movies and television shows on web channels such as Netflix, Amazon, Hot Star, and Zee, and engaging in online gaming through a variety of applications.

- For the sake of using the applications' functions, people regularly grant and/or allow rights for applications to access their personal information saved on their phones, computers, and/or social media accounts, which is collected by third-party applications.
- A further consequence of the government's "stay at home, stay safe" message is that more and more people are becoming increasingly reliant on various payment gateways to pay utility bills and insurance premiums, recharge their mobile phones, purchase medicines and other essential commodities online, and engage in a variety of other online activities. All of these efforts have contributed to the creation of an atmosphere that is favourable to spyware and ransom ware attacks.
- Some of society's most vulnerable populations, such as children, are obliged to spend greater time online in order to access services such as schooling and other necessities. As COVID 19 has disrupted the global economy, numerous individuals have often lost the jobs of theirs or even have had to recognize a pay cut. A significant increase in e-crime has occurred as a result of this fundamental shift in our way of life.
- False websites are becoming increasingly sophisticated, and they are becoming almost impossible to identify from their authentic equivalents.
- Reports of cyber harassment were received in the form of actual incidents. In the wake of COVID 19, there has likewise been a spike in sextortion crimes. It's a popular type of spam episode where cybercriminals extort cash by professing to experience an individual's compromising photos or maybe proof of the sexual activity of theirs. They could hack into someone's mobile telephone or any other gadgets and steal those videos/ pictures or perhaps morph a normal picture to really make it appear obscene. The assailant threatens to share some proof with the person's friends as well as employer and family until they pay out ransom cash.
- OTP fraud, social media stalking, lottery fraud, and online retail fraud also started raising.

Various issues under cyber law enforcement

Cybercriminals are contriving several techniques for defeating International Measures dedicated to address the measures taken for prevention of cyber-crimes. Here are some of the difficulties and issues for the cyber law enforcement:

(a) Identity of cybercriminals: Probably the best hindrance against worldwide endeavours towards stemming the hurricane of cybercrimes remains the unknown idea of the character of cybercriminals[5]. There are no simple methods for recognizing who is doing what. To add insult to injury, the IP address of the cybercriminal may be tracked to a particular location, but the next challenge is insurmountable because a criminal's identity remains a secret to the owner or administrator of an Internet specialized company.[6]

(b) Jurisdictional issue: Due to cybercrime's global reach, jurisdiction is a contentious subject to resolving and important issue which needs to be resolved. Whereas section 75 of the Information Technology Act 2000 talks about the extra-territorial operation of law. However, it will only have significance if it acknowledges court decisions and information warrants issued by competent authorities outside of their authority.

(c) Extradition processes[7]: Extradition has likewise been characterized as the acquiescence by one state to another of an individual blamed for submitting an offense in the last-mentioned (Oxford Dictionary of Law, 2002). This process became another issue as there are no uniform guidelines related to the Extradition and for the offences which are committed on cyber space.

(d) The difficulties relating to the nature of evidence: One other obstruction to the effective implementation cybercrime laws is the concept of proof accessible from the crime spot and the acceptability of same, during the course of investigation ofcybercriminals. The proof is what will in general demonstrate the presence of some reality. Physical proof is uncommon in cybercrime arraignment; this is a gooney bird, All that the law enforcement agencies may rely on are basic computer impressions and Internet tracks left by the cyber criminals which have minimal evidential worth and the same is not sufficient to prove the guilt of the accused based on the rules of our legal system.

[5] The Indian Evidence Act, 1872 as amended by The Information Technology (Amendment) Act, 2008.
[6] Law on cyber crimes :P.K.Singh (2007) Book Enclave, Jaipur, India. Page 22.
[7] Justice T. Ch. Surya Rao, "Cyber Laws – Challenges for the 21st Century", Andhra Law Times, 2004, p. 24

Challenges / Difficulties before the Judiciary

Now computer-related disputes are serious issues for the courts of law because judges and our law enforcement agencies are not well experts. There is no exact definition of the word "Cyber Crime".

There are no territorial boundaries. Law and procedures of Cyber Crimes are different from country to country. Because physical presence of the accused of commission that type of crime is not required.

There is an issue with cybercrime that law enforcement and the judiciary are both dealing with in the case of **State of Punjab v. M/s Amritsar Beverages Ltd.**[8]the court states, "Internet and other information technologies have brought with them the issues which were not foreseen by law. It also did not foresee the difficulties which may be faced by the officers who may not have any scientific expertise or not have sufficient insight to tackle the new situation. Various new developments leading to various kinds of crimes unforeseen by our Legislature came to immediate focus. Information Technology Act, 2000, although was amended to include various types of cybercrimes and the punishments for them, does not deal with all problems which are faced by the officers enforcing the Act.

Conclusion

Every country is affected from the Cyber Crime but there are only a few countries have their law which controls the Cyber Crime with International perspective. The other problem is every country has a different meaning and definition of cybercrime. The IT Act of 2000 does not cover several essential documents, including wills, powers of attorney, trusts, and sales of real estate. The IT Act of 2000 does not define cybercrime either. IPC, 1860 also not defined Cyber Crime. As a result, jurisdiction is critical, as the government may utilize its authority to punish criminals and keep tabs on their illicit operations. In this innovative world, a large portion of individuals has no information in regards to which kinds of offence comes under the classification of Cyber Crime.

To combat digital infractions, these crimes are emerging due to the lack of comprehensive cyber laws and effective enforcement or execution. Only digitally or electronically signed e-

[8] AIR 2006 SC 2820

records are acceptable in court in India. Internet communication is mostly conducted through e-mail. Given that most emails are neither electronic nor digitally signed, the actual issue is whether they are admissible in court or not. The Information Technology Act is empty of any language relating to intellectual property rights, and it makes no specific mention of domain name infringement. Since many commercial activities are performed via internet media, this has an immediate effect on global trade and commerce, information technology is also quiet on Cross Border Tax problems. Evaluation and monitoring of the functioning system, as well as training for judges and prosecutors, are critical for preventing cybercrime. Because the most important teacher and guidance we have is our own experience. It is no longer just a desktop or laptop computer; instead, it includes everything from mobile phones and watches to automobiles and other hightech devices.

Suggestions

Cyber Crime is the overall issue and crime isn't static. Antivirus software, firewalls, and intrusion detection systems are all common security tools which can be used for the prevention of cyber-crimes. One of the most effective mantras against cybercrime is "Protect Yourself." To effectively combat cybercrime, we need both substantive and procedural legislation. One piece of cyber law is required. The ineffectiveness of the enforcement procedures is a critical issue in the fight against cybercrime. Laws in all nations must be updated either via revisions or by the adoption of uniform legislation. Better mechanisms for enforcing the laws are urgently required. The dangers of internet users must be made clear to everyone, both individuals and businesses alike. Everyone should know how to reduce their risk of being a victim of cybercrime. Those who are new to online shopping, banking, or social networking should pay special attention to this. There must be widespread public education initiatives to raise awareness of cybercrime and ways for reducing the threat. There are some recommendations for preventing and reducing cybercrimes at the national and international levels:

- Need to Sign and Update the Convention on Cyber Crime & Need to Frame and Update Mutual Legal Assistance Treaty (MLAT) in relation to cyber-crimes.
- Need to create IT Act more relevant as well as comprehensive considering the latest developments.

- Need for modernization of existing laws, Enactment of New Laws and need to amend the Indian Telegraph Act, 1885
- Net Security be Tightened Up and Usage of Encryption Technology should be encouraged.
- Linking of cyber-cafes to police control rooms, and social networking sites must be regulated.
- Need to Adopt Clarified and Settled Law on Jurisdiction Issues at worldwide Level.

At the individual level:

- Updating computer and mobile phone on regular basis by installing and by installing trusted antivirus software in the devices.
- Non usage of same password in various websites.
- Not to upload personal images and data on internet.
- Not to click on suspicious links and paying attention to website privacy policies.