688

The Evolving Nature of Cybercrime and Technological Development: An Overview

[1] Ravindra K. Rajput, [2] Prof. Dr. Suresh. V. Nadagoudar

[1] Research Scholar, University Law College & Department of Studies in Law, Bangalore University, Bengaluru & Asst. Prof. SDM Law College, Mangaluru.

[2] M.A., LL.M., Ph. D, Presently working as Registrar, KSRDPR University, Gadag (On deputation) & Professor, University Law College & Department of Studies in Law, Bangalore University, Bengaluru.

Abstract: Cyber criminals enjoy the anonymity and lack of territorial jurisdiction or boundaries in cyberspace, making the internet an attractive tool to commit crimes. The conventional crimes are now seen to be committed through Information Technology devices such as computers and mobile. These criminals are not effectively tracked through their IP addresses due to the availability of technology to fake IP addresses or use proxy IDs and such criminals are flourishing in their criminal activities. The social networking websites, E- commerce, E-Banking have provided a platter to commit various crimes on these platforms, where adequate security measures are not adhered to.
With the technological development there have been new forms of cybercrimes which are seen today. The various forms of cybercrimes which we can say were traditional are still prevalent; however, there are new forms of cybercrimes which are evolving and being seen affecting individuals. The law seems to lack the pace to evolve itself to this fast growing technology and the evils that come along with it. This paper intends to highlight how cyber crimes are evolving to new forms with the advent of the new form of Information Technology and in this context it states how new technologies are evolving and new forms of crimes are seen in and around us. The paper attempts to make a few suggestions with regard to self regulation that can be taken up by the individual rather than waiting for the law to help after the commission of the crime.

I. Introduction

The Millennial is seen to be dependent more and more on information technology in the present day era. The internet and technological advancement have made the world a global village. This has brought about a lot of opportunities which could never be dreamt off. With access to the internet and information technology devices like cell phones, laptops, tabs, etc. communicating with people in the remotest area has been made possible. This has led to the development in major areas such as commerce, entertainment and governance.

The place where we find these people coming together virtually is known as cyberspace. New technological advancements were seriously taken up in order to enlarge the scope of commercial activities and reaching to each other even in the remotest places for business and other activities. These technological advancements indeed have benefited most of us and have become part and parcel of our daily life. However, as we were blessed with good things, evil aspects also come to be part of our lives, similar to that of as in the case of the real world too. With every positive or good technological development we have seen loopholes or negative aspects also being part of such advancements.

The criminals who are found in the real world have become anonymous in the virtual world, making it difficult for the enforcement agencies to catch them and prevent the crimes in cyberspace. The Law Enforcement Agencies and the Law Makers have grappled with these problems in the 21st century. With Cyber Laws in place, it tries to touch all factors and activities on the Internet and as a whole in cyberspace. However, with innumerable opportunities that have been created by technological development, it has become a haven for cybercriminals.

II. Defining Cybercrime

The word Computer crimes and Cyber crimes are often used interchangeably. However, according to Donn B. Parker, distinguishing the two, he states that computer crime is one in which the criminal uses special knowledge about the computer technology and cyber crime is one in which the criminal uses special knowledge of cyberspace.[1]

As per the U.S. Department of Justice: "....is an illegal act requiring knowledge of computer technology for its perpetration, investigation and prosecution"[2]

[1] Dr. Talat Fatima, *Cyber Crime*, Eastern Book Company, Lucknow (2nd edn, 2016), p. 89
[2] *Supra* note 1, p. 89

According to OECD: "Computer abuse is considered as an illegal, unethical or unauthorised behaviour relating to the automatic processing and transmission of data"[3]

It is interesting to see that the Indian legislation that is the Information Technology Act, 2000 does not define cybercrime or computer crime, but the 2008 Amendment Act to the Information Technology Act, 2000 has used the term "computer related offences".

However, it is also interesting to see that in few of these definitions the term internet is rarely used, where in fact cybercrimes can be seen as products of the internet.

III. Growth of crimes in Cyberspace

In understanding the term crime one has to see both crime and law together. As the criminal jurisprudence state crime is an act which has violated the law of the land of a particular nation at a given time. However, due to the fact that law has not been universally defined, an act maybe crime in a particular nation and not in another. It is here that moral sentiments of a society may also be a factor to term and act as a crime.[4]

In regards to computer crimes, a computer can either be a "tool" or "the target", in order to perform an unlawful act. Where computers are used as tools, it may be in furtherance of conventional crime and in certain cases it may be the target. With the development of new technology and a realisation that such new technologies have become an integral factor of human lives, crimes that have evolved through the use of such new technology are bound to affect the rights of an individual as well as the society at large. And thus a need arises to have a sound legal regulation in place to cope up with the fast changing technology.

In the present day scenario we see phishing attacks increasing at a very high rate, similarly the effects of ransomware are also quite visible. We see a reasonable increase in cyber crime, which the experts agree on and say it's getting worse. There are several factors which are causing this and the impact of it is felt in the short-term and beyond. A few to state are[5]:

1. Lack of awareness

   Lack of awareness can be considered to be one of the important factors for the growth of cybercrimes. It is seen that those individuals who lack awareness are found on the receiving end of crimes and scams. This human error in cyber security is one of the leading causes for many Cyber crimes.

2. Lack of training to new internet users

   In the last decade, the number of users using internet has doubled, over half the population is online and millions of users are coming online every year. What we see is the rate at which the new internet users are educated, is being out paced buy number of new net users. And this has led the new threat actors to go online and pull off a quick scam.

The other reasons for the increase in cyber crimes may be due to, low cost and high payoffs to the hackers, usage of public WIFI, usage of Cloud and IOT devices.

IV. Changing nature of Cybercrimes

Cybercrime has now turned itself into an industry, an industry which is evolving at a high rate. This industry is seen to be built on enterprise data (data stored by companies). Data has now taken centre stage in today's digital environment. To put in simple terms, data is everywhere now, available through many applications (web or mobile based), which is accessed by many people and the cyber criminals have many places to sell it now. We now see that many criminals don't get caught today because of the combination of Bit coins and Dark web, which in turn has reduced the costs and dangers associated with being cyber criminal now.[6]

In the present day, the economy is knowledge driven and companies now have two important assets:

i. Data
ii. Applications (Apps)

It is commonly seen now that cyber criminals make money either by extortion or theft and these methods are put to use to earn quick money by targeting the core assets of these companies that is the data and applications.

Extortion or theft can be done through denial of service (DOS) or ransom ware attacks. In case of denial of service, extortion can be by targeting the company's applications. For example: in case an individual has his house installed with IOT devices, where the doors, lights and other utility facilities are connected by an application through their mobile, the perpetrator may lock that individual out of their home by denial of service attack and demand for ransom, a situation where one has to pay to enter into his own house.

[3] *ibid*

[4] *ibid*, p. 54

[5] "What's Causing the Rise in Cyber Crime" 7 March, 2018, available at https://www.vircom.com/blog/the-rise-in-cyber-crime/ (accessed on 30/06/2019)

[6] Morgan Gerhart, "The Evolution of Cybercrime and What It Means for Data Security", Jun 27, 2017, available at https://www.imperva.com/blog/the-evolution-of-cybercrime-and-what-it-means-for-data-security/ (accessed on 30/6/2019)

Ransom ware attacks have been in existence from a very long time, however, in the recent times it has become more prevalent due to the simple ways of not being detected, thanks to Bit coins and Dark web. And then there may be malicious insiders, who know where the data is available and can access it in order to steal it for their gains with an opportunity and finally the careless attitude of consumers or users who expose themselves or their data to be accessed by cyber criminals.[7]

The trends that cyber criminals are adopting in recent times are[8]:

a) Advanced phishing attacks

It is seen that new forms of malwares are created every second and phishing remain to be one of the most desired attack vectors throughout the world. As phishing sites are online for just a few hours, the percentage of the report of such attacks become very low and due to this it is stated that only around 65% of URL's are trustworthy today.

b) Attacks through Smartphone's

We see today that most of the cyber attacks are through our smart phones, either due to unsafe browsing and fake applications. There is a growing trend where we see people trying to manage their financial operations or sensitive data through a network which is outside their home network. For example: using public Wi-Fi which makes them more vulnerable to cybercrimes or where money is stolen through UPI(Unified payment Interface).

c) Home automation and IOT (Internet of Things) devices

The internet of things industry is expected to grow potentially in near future. These devices are presumed to be safe due to the misconception that as such devices do not have user interfaces and thus they are not vulnerable. In fact these devices could have the capability of collecting vulnerable data which in turn could lead to denial of service attack or an entry point for attackers.

d) Use of Artificial Intelligence

Big companies have been using machine learning and artificial intelligence in order to automate their processes and to improve their overall performance. Artificial intelligence is a technology which has be used and developed by cyber security agencies to prevent cyber threats, whereas hackers are trying opportunities to be more effective through this technology, which is cybercriminals now have the potential to use artificial intelligence to evade cyber security and pass through to cyber security filters.

The artificial intelligence has its adversarial impact in few ways[9]:

i. Impersonation

The AI would be highly tailored and the malwares will have the capacity to learn individual behaviour and language by learning the emails and social media posts. This knowledge would be replicated by the AI where it would be almost impossible to distinguish from original communication.

ii. Blending

When an organisation or individual is specifically targeted, the cyber criminals maintain their presence for a very long duration and move slowly and cautiously in order to evade the conventional security systems. This would help them to discretely blend in and spread in their digital environment and maintain its stealth capabilities. These AI malwares will be able to analyse a vast volume of data rapidly, with an advantage to identify valuable data and not valuable data, thus saving the time and effort of cyber criminals.

iii. Faster attacks with effective results

In the present day, for a cyber criminal to target an individual would require observation of their activities on the social media and other platform over a long period of time. An offensive AI can achieve the same results in a fraction of time and in huge numbers. As AI have the capability to evolve at a very great pace, it would be difficult for a conventional security system to curb it.

e) 5G network

The design of 5G network will take the world into a new era by 2025, where billions of new devices will be connected through internet and run critical applications and infrastructure at a speed nearly 20 times that the current speed. Here, indeed 5G will enable great prosperity and help people; however it has the potential to increase the speed of spread of cyber attacks as well.

V. Suggestions for prevention of against Cyber crimes

As the idiom states "Prevention is better than cure", in cyberspace self regulation can be considered as the most important factor to curb the increase of cybercrimes, rather than expecting the law enforcement agencies to catch the cyber criminals.

[7] *Supra* Note 6

[8] Einaras von Gravrock, "Here are the biggest cybercrime trends of 2019", 04 March 2019, available at https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/ (accessed on 21/06/2019)

[9] William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks", 19 Jun 2019, available at https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence (accessed on 30/06/2019)

Few steps that can be taken up to avoid being victims of cybercrimes are:

a) Education

By educating oneself about the various types of scams that exist one can avoid them. Information is power and this information should be the information to protect oneself against cyber criminals. For example: in case of phishing, hackers would attempt to lure individuals to reveal personal data. Thus, if one knows in advance the scams which are prevalent, one can help himself from being a victim of cybercrime.

b) Software is updated

The operating system and security software need to be updated time to time. Cyber criminals exploit the lacunas and loopholes in such software and gain access to computers and other devices. For example: in case of ransom ware attacks such as WannaCry, Windows computers were seen to be affected the most and this was in cases where the operating system was not updated.

c) Use of secure wireless networks:

This can be done by enabling the Firewall on their routers and changing their router passwords frequently, as cyber criminals often know the default passwords. This further can be strengthened by allowing people to access with passwords that are encrypted.

d) Strong passwords

A strong password can help secure the information in the long run, as every service provider requests their subscribers to change the password frequently, which most often is not taken into consideration seriously and thereby fall prey to cybercrimes. A good password with at least 10 characters containing a combination of special characters, numbers and letters is normally considered to be ideal.

e) Manage social media settings

The social engineering cyber criminals most of the time get personal information from data that is posted or shared publicly. For example: in case of an need to change the password, one is required to answer few common security questions such as dogs name or mother's name, where the cyber criminals can obtain such information from the social media information shared.

f) Educate the younger generation/ children about internet

Educating the children about the evils of internet is an important factor. This is because in case they are experiencing any form of online bullying, stalking or harassment, they must have been educated to report such instances immediately to their parents or concerned authorities.

g) Use of common sense

In spite of warnings cybercrimes are on the rise and this is due to the common mistakes people make by responding to spam emails or downloading attachments received from unknown people. The principle of "click with caution" should always be kept in mind when one is surfing or shopping online.

VI. Conclusion

Indeed to protect oneself from being a victim of cybercrime one needs to put in some effort to be safe. There are resources and tools which can help protect one from cybercrimes and by adopting best practices and few precautions every individual can help in the prevention of rise of Cyber crimes.

The cyber security community can be seen heavily investing in the new future. One of the tools that would be the used will be defensive artificial intelligence in fighting cyber attacks, as the new forms of cyber attacks would outwit the current defence systems. There are technologies available and the time to prepare ourselves against all adversaries is now.