JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Overview of Emergence in Cybercrimes: Challenges and Perspectives

Ankit Sourav Sahoo
Assistant Professor,
Lajpat Rai Law College,
Sambalpur University, Sambalpur.

Abstract:
In this 21st century, the internet has become a fundamental element of life. The Internet has become more connected with our daily lives than we can possibly imagine, as technology continues to evolve. In the field of information technology, cyber security has a major role to play. One of the biggest challenges in today's world is to secure information. Cyber crimes, which have risen exponentially in the last few days, are now one of the next things that come to mind when thinking about cyber security. Cybercrime is the illegal activity of either targeting or exploiting computers, networks and networked devices. Cybercrime is the biggest threat we face today. The paper takes a look at the different types of cybercrime, as well as laws and judicial role in India. Cyber crime in the field of international law and its impact on India's society are also covered.

Keywords: Cybercrime, Hacking, Cyberterrorism, Digitalisation, Information Technology

Introduction:

In India, the cyber crime law is still inadequate enough to prevent a significant amount of newly emerging cybercrimes from being detected and numerous problems are faced by Indian judiciary when interpreting existing legislation in view of new evolving characteristics of criminal offences. However, it is also necessary to recognise that cybercrimes do not originate in one particular national territory. Any geographical area in the world and at any time can be used for such offences. In such cases a concrete theory is required in order to determine the competence of law enforcement agencies. In addition, since what is legal in India may not be legal in other countries and vice versa, and cyberspace does not know any national boundaries, cyber crime can also be a reflection of cultural diversity around the world. Consequently, the content which is available on the internet should be monitored at all hours of the day and night by a competent certification authority. In addition, it is necessary to conclude international agreements in order to bring uniformity into the legal system since failure to achieve this could lead to several cyber crimes. In determining the liability of the offenders, those conflicting provisions make it very difficult.

Concept of Cybercrime:

While the term "cyber crime" is not defined, it is commonly used to describe any criminal act that will involve the use of electronic communication or the World Wide Web. Due to the lack of a universally accepted definition, this concept remains nebulous. It is impossible to offer a specific definition of the offence known as cybercrime because there is no one method in which a computer or the internet could be abused. It is required to see the notion of crime, which is, coupled with the computer and the internet, in order to grasp the concept of cyber crime, which is a subset of crime. The idea of committing a crime online is not tremendously dissimilar to the idea of committing a crime in the traditional sense. Both involve the behaviour, whether it is an act or omission resulting in a violation of the rules of the law as well as restitution from the state[1].

During the early stages of the nation's history, the nature of criminal activity was highly variable and was determined by the whims of the sovereign authority. Crime is a social and political issue in modern times, and it has been there for as long as human society has existed[2]. The idea that the crime is legitimate and supported by sanction has developed in tandem with the progress. Today, the term "crime" refers to an illegal act. At some point in the past, when religious organizations were dominant in society, it was determined that some religious practices were incorrect. There was no distinction between sin and the criminal acts. But as the state expanded, the concept of sin was diluted, and the term "sin" or "wrongful act" was finally condensed to "wrongful act."Now we are talking about the concept of a crime or an offense because of this incorrect act. According to Granville Williams, a crime, sometimes known as an offense, is a wrongdoing in the eyes of the law that may end in a criminal procedure and, ultimately, in the imposition of a penalty. The most fundamental aspect of crime is the fact that it involves breaking the law in some way. According to statements made by Lord Atkin, "the criminal quality of an act cannot be discovered by reference to any slandered but: is the act prohibited with penal consequences[3]." Any act or omission that is accompanied by something that the law bans is considered to be a crime. If somebody were to engage in this behaviour, it would be considered a violation of the law, for which they would be held accountable.

Types and various categories of Cybercrime:

The below mentioned are the various types of cyber crimes:

1. Data Crime

(a) Data Interception

In order to obtain information on a target, an attacker will monitor the data streams going to and coming from that target. It's possible that this attack was carried out in order to acquire intelligence that could be used in a subsequent strike, or else the information obtained could have been the intended target all along. Sniffing network traffic is typically included in this attack, however monitoring other types of data streams, such as radio transmissions, may also be a component. Nevertheless, in specific forms of this attack, the perpetrator may endeavour to commence the creation of a data flow or manipulate the characteristics of the data being transmitted. This stands in opposition to the majority of iterations of this assault, wherein the perpetrator remains inert and solely observes standard communication. One of the distinguishing features of this attack is that the data stream is not intended for the attacker, regardless of the specific variation employed. This sets it apart from other methods of data collection. Unlike other forms of data leakage attacks, this particular type entails the perpetrator actively monitoring and perusing the contents of explicit data channels, such as network traffic. By way of contrast, the present category does not encompass attacks that gather qualitative data, such as communication volume, which is not explicitly conveyed through a data stream[4].

(b) Data Modification

The confidentiality of conveyance is absolutely necessary in order to guarantee that data will not be altered or viewed while it is in route. The utilisation of distributed settings entails the possibility of a malevolent external

[1] Cyber crime - Law & policy perspectives, Dr. Mrs. K. Sita Manikyam (2009) Hind Law House, Pune. Page 40

[2] Cyber Crime by Parthasarathi Pati, retrieved from http://www.naavi.org/pati/pati_cybercrimes_dec03.htm Last accessed on January 27, 2019

[3] Proprietary Articles Tread Association V. A.G. for Canada (1932)

[4] CAPEC-117: Interception, Common Attack Pattern Enumeration and Classification (A Community Resource for Identifying and Understanding Attacks), available at https://capec.mitre.org/data/definitions/117.html accessed on 09th February 2019

entity engaging in computer-related illegal activities by tampering with data during its transmission from one location to another. This peril arises due to the fundamental characteristics of distributed systems[5].

In the event that an individual gains unauthorised access to a network, they may execute a data modification attack by intercepting data that is in transit and altering specific portions of said data prior to retransmitting it. One example of the principle in action is modifying the monetary value of a banking transaction from $100 to $10,000.

A counter attack occurs when an attacker repeatedly injects a complete set of legitimate data into a network system. An exemplification of this concept would entail executing an identical lawful transaction involving the transfer of $100 from one financial account to another on a thousand occasions.

(c) Data Theft: When information belonging to a company or another individual is illegally duplicated or taken, this practise is mentioned as "data theft." Typically, this information consists of details pertaining to users, such as login credentials, SSNs, credit card numbers, and other sensitive personal or company data. System administrators and office workers are a major source of data theft since they have access to computers, database servers, desktops, and an ever-increasing number of portable devices that can store digital information. USB flash drives, iPods, and digital cameras are just a few examples. Employees may feel entitled to the company's confidential and copyrighted information because they invest so much time into developing these resources. As a result, they may be tempted to take some of this information with them when they leave the company or to use it inappropriately while they are still employed there. This is because workers invest a great deal of time in building networks and creating proprietary and copyrighted information for their employer. They can be acquired through purchase or sale and afterwards put to use by entities that are complicit in illegal behaviour[6]. Due to the illegitimate means through which this information was acquired, it is highly likely that the individual responsible for the theft will be held accountable and prosecuted to the maximum extent allowable by law upon discovery.

2. Network Crime

(a) Interference in Networks

Interference is anything that alters or interrupts a signal as it passes along a channel between a source and a receiver in the fields of communications and electronics, particularly in the field of telecommunications. In most contexts, the word refers to the process of adding undesirable signals to a signal that is otherwise valuable[7]. Network Intrusion, transfer, damage, deletion, degradation, alteration, suppression, and stifling of data are all examples of network intrusion.

(b) Sabotage of a network:

The term "Network Sabotage" or "Cyber Sabotage" refers to a relatively new development in the ever-evolving dangers posed by cyberspace. Contaminated hardware or software is now a worry, and it does not matter if it was transmitted over the internet or whether it was purposely installed during the manufacturing process. The term "sabotage" refers to any intentional and malevolent act that has the purpose of causing disruption to normally occurring processes and functions, as well as the destruction of, or damage to, equipment or information[8].

3. Access Crime

(a) Unauthorized Access

[5] Oracle® Security Overview 10g Release 1 (10.1) Part Number B10777-01, available at https://docs.oracle.com/cd/B13789_01/network.101/b10777/toc.htm accessed on 09th February 2019

[6] Xing, Liudong; Levitin, Gregory, "Balancing theft and corruption threats by data partition in cloud system with independent server protection", November (2017), Reliability Engineering & System Safety. 167: 248–254

[7] e-study guide for: Digital Terrestrial Broadcasting Networks, Wolfgang Beutler, Cram101, 2012, C.T. Reviews

[8] Kevin Coleman, Defensetech, Cyber Sabotage. Available at https://www.military.com/defensetech/2008/02/06/cyber-sabotage

When a person gains access to a system without permission, it's because they used someone else's login information or some other way to bypass security measures. To acquire unauthorised access, a user might, for instance, repeatedly try a variety of credentials to enter a system that does not belong to them, eventually succeeding. It is also possible for unauthorised access to occur if a user tries to enter a restricted area of the system. Another case where unlawful entry is possible. They wouldn't be let in if they attempted, and they might even see a sign saying they didn't have authorization to be there[9].

(b) Malware Dissemination

Malware is an abbreviation for "malicious software," which refers to software that is designed to secretly infiltrate computers that are part of a network without the knowledge or permission of the user. Malware is a wide spectrum that refers to a wide number of different forms of destructive software. The terms "Worm," "Botnet," "virus," "Trojan horse," "Backdoor," "Rootkit," "Logic bomb," "Rabbit," and "Spyware" are all examples of "Malware." Botnets and worms are the most frequent and dangerous forms of malware, and they are responsible for the majority of today's cyber attacks. There are many different kinds of malware[10].

In the broadest sense, the term "cyber crimes" refers to any and all activities carried out in cyberspace with the purpose to commit a crime. They can be organised into the following four classes:

1. Cyber Crime against human:

The transfer of pornography involving children, harassing any person sexually by using computer as a means, including electronic mail and e-stalking, are all examples of the first category of cyber crimes perpetrated in against of persons and fall under the umbrella of "cyber stalking." Any unwanted contact between two people that conveys a threat to the victim or causes the victim to feel fearful is considered stalking. Today, pornography, indecent exposure, and child pornography distribution, publication, and circulation are some of the most serious forms of cybercrime that can be committed. The distribution of such material is also considered a form of cybercrime. It is difficult to overstate the potential damage that a crime of this nature could cause to humankind[11].

2. Cyber Crime against property

The subsequent category of online criminal activity is comprised of offences committed against any and all forms of property. These offences comprise hacking, which refers to the unauthorised use of computer system and network resources, as well as cracking, which involves breaking through the computer system of another person, most frequently while they are connected to a network, or purposefully breaching computer security[12]. A computer programme that is capable of reproducing itself and inflicting damage to data as well as the contamination of creative or artistic works that have copy-right protection is known as a virus. Copying a work that is protected by intellectual property rights should only be done with the owner's permission. A state grants an inventor or their assign exclusive rights for a set period in exchange for the inventor disclosing their innovation[13]. In the context of the Internet, "cyber squatting" is to register, deal in, or use a domain name for the purpose of capitalising on the reputation associated with another party's trademark. As far as cybercrime goes, hacking and cracking are among the worst examples we have. Having your computer systems hacked

[9] Unauthorized access, Computer Hope. Available at https://www.computerhope.com/jargon/u/unauacce.htm

[10] Rouhani Zeidanloo, Hossein & Tabatabaei, Farzaneh&VahdaniAmoli, Payam &Tajpour, Atefeh. (2010). All About Malwares (Malicious Codes).. 342-348.

[11] D. Halder and K. Jaishankar, Cybercrimes Against Women in India, SAGE Publications, 2016

[12] L. Freeman and A.G. Peace, Information ethics: Privacy and intellectual property, IGI Global research collection, Idea Group Publishing, 2005. Page 9

[13] WIPO Intellectual Property Handbook: Policy, Law and Use. Chapter 2: Fields of Intellectual Property Protection Archived 2013-05-20 at the Wayback Machine WIPO 2008

into without your knowledge or consent and having sensitive and valuable data and information changed with is a bad feeling. This holds truer if you know for a fact that this person has done this. Furthermore, there is no computer system in the world that is completely safe from being hacked. Every system can be hacked; this is a fact that has been proven beyond a shadow of a doubt.

Cybersquatting: It includes two different parties making competing claims for ownership of the same domain name, with each party claiming prior right to use the name through registration or prior use of a name that is confusingly similar to the one at issue. Consider the websites www.yahoo.com and www.yahhoo.com, which seem very similar.

Cyber Vandalism: Vandalism refers to the intentional destruction of the property of other person. Therefore, the destruction or damage of data or information held in a computer is considered to be an act of cyber vandalism. This might occur when a network service is terminated or disrupted. Any form of physical damage that was done to the computer of any person could fall under its purview. Stealing a computer system, a component of a computer, a circumferential device, or some other equipment that is connected to the computer can be considered one form of these illegal activities.

Hacking Computer System: Hackers attack several online platforms, including Famous Twitter and blogging platforms, by gaining unauthorised access to or control of them. As a direct result of the hacking actions, data and the computer system would be lost. And research shows that the attacks weren't just about making money; they were also meant to ruin the victim's or the company's reputation.

Transmitting Virus: Viruses are malicious programmes that infect one computer or file before replicating themselves and spreading to others through a network. These programmes are created by programmers and are known as "worms." They mostly change or delete the data that is stored on a computer, but they can also corrupt it. Attacks by worms play a significant part in the way in which individuals' computer systems are impacted[14].

3. Cyber Crime against Government

One possible definition of cyber terrorism is the prepared act. An attack on a target's system, of information, computer programmes, and data that is intended to damage the socio-political or physical infrastructural base of the prey in order to cause vehemence towards the general people[15]. The concept of cyber terrorism is fraught with debate. Some authors choose fora definition that is extremely narrow in scope. The term "cyberterrorism" pertains to the utilisation of disabling assaults on computer networks by established terrorist groups with the primary objective of inducing fear, chaos, or physical disruption. Some academics favour a more inclusive definition that takes into account online criminal activity. Participation in a cyber attack has an effect on the impression of the threat posed by terrorism, even if the attack is not carried out in a violent manner[16]. According to certain definitions, it may be difficult to differentiate between acts of cyber terrorism and acts of cybercrime when referring to activities that take place online[17]. During the year 1998, the Liberation Tigers of Tamil Eelam (LTTE) targeted a huge number of Sri Lankan embassies' computer systems all over the world. They did this by sending 800 emails to each embassy daily for a period of two weeks, with

[14] Er. Harpreet Singh Dalla, Ms. Geeta, Cyber Crime – A Threat to Persons, Property, Government and Societies, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 Available online at: http://ijarcsse.com/Before_August_2017/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf accessed on 09th February 2019

[15] Col. Prasad, R.S, Cyber Crime - An Introduction. Hyderabad, ICFAI Univ. Press, ed. First 2004, p.8

[16] Canetti, Daphna; Gross, Michael; Waismel-Manor, Israel; Levanon, Asaf; Cohen, Hagit (2017-02-01). "How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks". Cyberpsychology, Behavior, and Social Networking. 20 (2): 72–77.

[17] Hower, Sara; Uradnik, Kathleen (2011). Cyberterrorism (1st ed.). Santa Barbara, CA: Greenwood. pp. 140–149

the subject line reading "we are internet black tigers and we are using this to disrupt your communications."It is the first attack seen to have been carried out by terrorists on the computer system of a nation.

4. Cyber Crime and Organized Crime

The change brought about by the internet has had a profound effect on society as a whole and the business world in particular. Despite the fact that business management is common on the internet due to its ability to approach people at a global level in cost efficient manner. Therefore, organised crime has also discovered fresh chances and advantages on the internet, which are highly valuable for promoting the commotion of crime organisations. The traditional illegal activities of organised crime organisations are slowly being replaced by the more lucrative and less dangerous operations that can be carried out through cyberspace. There are now new kinds of criminal networks that deal specifically with e-crime, and traditional criminal organisations are actively seeking the help of e-criminals who possess the necessary technological expertise[18].

Conclusion:

Users must take the necessary precautions to avoid cybercrime, for example by setting passwords and encrypting them. A large number of companies are victims of cybercrime and need to be protected by implementing interference detection techniques, confirmation check tools or irregularity control systems if they wish not to become victims. Cybercrimes exist in nearly all States and territories of India, and relevant governments have taken measures to prevent them. Everyone, from babies to elders, has been reliant on digital technology since 2020 due to the COVID19 pandemic. And during this period there has been an increase in cybercrimes. Cyber bullying, defamation and cyber fraud are some of the most frequent crimes. The easy access to the devices, in some cases user negligence, is a cause of cybercrime. Many people in India don't know about such crimes, and when they're hacked, they lose money, but they don't know what's going on. It is therefore vital to inform them about those crimes and their rights in the Digital World first. The Indian government's taken steps to prevent cybercrime in the country but there is still a long way to go. The government will ensure compensation and justice for the victims.

[18] Dr.Tropina, Tatiana, Cyber Crime and Organized Crime, available at; http://www.freedorafromfearmagazine.org, accessed on 9th February 2019