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

Cyber Crimes in the Digital World – An Over view

[1] **Dr.Sudarshan Nimma,** *Chairman, Board of Studies, Dept. of Law, Kakatiya University, Telangana, India.*

Advancements in Science and technology, more particularly in the field of information and communication technology made human life very much comfortable and convenient. Generally, scientific development in any sector will be useful to the human beings and the society altogether when used/applied positively for the purpose for which they are intended/made. But the same scientific advancements are presently being misused by certain group of people of deviant behaviour causing lot of inconvenience, personal and financial damages, sometimes causing irreparable losses to the individuals and institutions of the society on large scale. These persons of deviant behaviour are popularly known as 'Cyber Criminals'. These people invented numerous advanced techniques and means by which crimes can be committed better using the developments in Information and communication technology due to internet revolution.

*Interne*t is a product of revolution in information technology. The fastest expansion of the Internet provided new opportunities for the criminals[1] With the help of these developments, using internet today most of the traditional way of committing crimes have been drastically changed and transformed in to *Cyber Crimes* committed by the techno-savvy modern man of 21st century. Most of the crimes happening in present day are cybercrimes. Criminals are constantly on the job of finding new ways to change their pattern of committing crimes. Rapid rise in e-services like online shopping, online banking and Online gaming and the Social apps led to increase in the number of Internet users and are targeted by the cyber criminals.

Cyber Crime

Cyber crime involves a computer with a network/internet connection. These crimes are not just include the ones committed on internet but also include those offences committed in relation to computers or committed with the help of computers systems. Perpetrator of the Cyber crime uses his special knowledge of cyberspace. From the history of cyber attacks on the Internet, it is observed that, trends of attacks are

[1] Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

continuously changing day by day. Cyber Crime is a malicious activity which affects the 3 basic principles of network security[2]

Effects of Cyber Crime

Cyber crimes are causing serious damages to individuals/ institutions of the society Certain basic infrastructure such as energy, transport and communication services.etc are also affected adversely. These Cyber crimes are becoming more sophisticated. The perpetrators are equipping with more technical expertise as such tracking is becoming very much difficult. Consequently, the moral and legal structures, paradigms break down in cyber space. These suggests the failure/inadequacy of the existing legislations and regulations, mechanisms and the urgent need to update and empower the state agencies like legislature, executive and the judiciary to deal with cyber crimes effectively and to put check on the cyber criminals. The situation in India is also not free from the gloom of cyber crimes and the cyber security is at risk.

Before proceeding to know the meaning and scope of ‘Cyber Crime’, it is essential to know the roots of the term ‘Cyber’. The total internet area/jurisdiction in which the crime is committed is known as ‘cyberspace. Technically speaking, Cyber Law means “Internet Law” or Law Governing Cyberspace,[3] Cyber Law deals with the legal issues of Cyber space.[4]

Cyber Crime- Definition[5]

[2] i.e, *confidentiality, integrity, and availability*. The cybercrime includes fraud, stealing, fights, and world war. These terms are also used in real-life crimes, but in the world of Internet, these terms have almost the same meaning but with different techniques.

[3] Cyber law is a term used to describe the legal issues related to the use of communications technology particularly “cyberspace”, i.e., the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet

[4] Dr. K.Nataraj Kumar, Doctoral Thesis “Cyber Crimes in India” Submitted to Acharya Nagarjuna University (2012)

[5] The 10th United Nations Congress on “ Prevention of Crime and Treatment of Offenders,[5] cybercrime was classified into two categories ; Narrow sense of Cyber crime defines it as
Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.where as the Broader sense of Cybercrime defines it as, Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network. Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.

The term ‘Cyber Crime’ is incapable of any precise definition. The word‘ cyber crime’ is not defined in any law, legislation.[6] Generally it can be defined as ‘unlawful acts wherein the computer is either a tool or target or both. [7]

Origin and Evolution of Cyber Crimes

The history and evolution of cybercrime closely linked with the evolution of Internet. ‘Cyber crimes’ were committed much before emergence of Internet i.e, data theft. The initial crimes were just ‘hacks to steak information’ from local networks. The first major wave of cyber crime surfaced with the proliferation of email in the late 80’s, wherein, a host of scams and/or malware delivered to the email inbox.[8]

The next phase in the cyber crime history emerged in 1990’s with the development of ‘*Web Browsers’*. Cyber criminals started adopting new methods and techniques.[9] Now, Cyber crime became a non-stop, round the clock phenomena happening everyday and everywhere across the nations and continents[10] It is very difficult to locate the exact origin or originator of the cyber crime across a computer net work. [11] Cyberspace provided new avenues for the offenders to commit crimes due to its novel features.

- *Globalization*, facilitating the criminals to cross the traditional borders.
- *Distributed networks,* created new opportunities for victimization.
- *Synopticism and panopticism*, empowered surveillance capability on victims from remote
- *Data trails*, facilitated the criminal to commit ‘identity theft.

[6] The *Oxford Reference Online* defines ‘Cyber Crime’ as crime committed over the Internet. The *Encyclopaedia Britannica* defines ‘cyber crime’ as any crime that is committed by means of special knowledge or expert use of computer technology. The *CBI Manual* defines cyber crime as, crimes committed by using computers as a means, including conventional crimes and Crimes in which computers are targets. Justice K.N.BASHA,Judge, Madras High Court, Paper presented at Seminar & Workshop on Detection of Cyber Crime and Investigation, at S.V.P. National Police Academy, Hyderabad on 28/29 June 2010@https://documents.site/cyber-crime-by-knbj.html

[7] ‘Cyber Crime’ may be defined as an ‘Offence committed against individuals or groups of individuals with a criminal motive to intentionally harm reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet.

[8]The first Nigerian Prince scam read as “Greetings, I am a down-and-out prince from Nigeria. I need help getting millions out of my country and all you have to do is send me some money first to set-up the transfer. Once done I’ll share my millions with you” yeah right.https://www.le-vpn.com/history-cyber-crime-origin-evolution/

[9]Cyber crime really began to take off in the early 2000, when social media came to light. These criminals operate in gangs, use well-established methods and target everything and everyone with a presence on the web

[10]It is estimated that cyber criminals make an astounding income of nearly $450 billion per annum, and the number of records stolen last year is also quite high, over 2 billion, including at least 100 million health insurance files, mostly US.

[11] One can find out the first major attack on a digital network and use it as a source or reference point of event in evolution of the cyber crimes.

Objectives of Cyber Criminals[12]

Every individual works towards his objectives. The objective may be to gain money, respect, revenge etc. Cyber attackers also have their own objectives for which they resort to cyber attacks/cybercrimes. All Cyber criminals are not expected to be equally gifted with skill or talents or same degree of motive and fun. There exist certain variations in terms of accomplishment on the basis of age, attitude, purpose and proficiency.[13] The mindset of a cyber criminal is unpredictable more particularly in white collar crimes.[14] Passion for high quality life styles motivates and drives a computer literate to become cyber criminal.

1) *Entertainment*

Few cyber criminals make cyber attack to test their hacking talents. They feel great and enjoy for their successes. They desire to become famous.

2) Hacktivists

Few cyber attackers are motivated by political, religious, and social ends. They want to spread their religion/politics to popularise among the masses.[15]

3) *Financial gains*

Most of the criminals commit it for financial gains. They strongly desire to be rich. They generally target the banking sector, big companies, organizations, rich individuals/countries. Some of these cyber attackers are generally engaged by individual/country/organization/company etc.

4) Spying

These cyber criminals attack the networks to steal the individual/institutional confidential information.[16]

[12] Cybercrimes: A Proposed Taxonomy and Challenges- Harmandeep Singh Brar and Gulshan Kumar; *Journal of Computer Networks and Communications* ; volume 2018 |Article ID 1798659

[13] A pre-adolescent downloads illegal songs without realising it as a crime; a desperate white collar worker in dire financial straits may download company secrets and sell to rival competitor for money to pay her family medical bills knowing well that she is committing a serious wrong, and a cold hearted sociopath may use the network to get whatever he wants, whenever he wants it believing that there is no such thing as right or wrong.

[14] White collar criminals often use computers to commit offenses because it's easy to manipulate electronic databases to misappropriate money or other things of value. Some white collar criminals are highly organized and meticulous about details, stealing only limited amounts from any one source and may go on for years or decades without being caught. Others do it on impulse; for instance, they may be angry about a bad evaluation or being passed over for promotion and "strike" back at the company by taking money they believe they deserve.

[15]The current trend of 2016 and 2017 shows that, hacktivists are exposing the individuals having secret affairs through social websites. The latest example is '*Ashley Madison* dating users list' was exposed by attackers in public domain. Their motive is to preach their political and religious mottos and discourage people of other sets.

[16] Spy hackers use similar tactics like those of hacktivists, but their only agenda is to serve their client's goals and get paid in return.

5) Revenge

These category of cyber criminals include the humiliated employees, who are expelled from their organization/office. They aware of the policies, secrets of the institution/nation. They resort to cyber attacks under certain emotions of hate and feel satisfy by causing financial loss, tarnishing, damage to their reputation etc.,

Characteristic Features of Cyber Crime

1. High-speed with low-cost Offence
2. High-tech Offence:
3. Complex Nature [17] :- Cybercrime acts are resorted to damage reputation of the governments by creating their own terrorism websites, enter false data into the key systems of the governments, destroying key systems, disabling their functioning.[18]

4. *Transnational in nature*

Uniqueness of Cybercrime is that, it can be committed from any place with much ease, the accessibility of Internet is just enough to the criminal. Since the computer equipment and online services are available, accessible to every body.

Ex:- Cyber crime can be committed on individuals/institutions of any country/continent of the world on this internet made global village, cutting across the territorial barriers.

5. *Structurally Unique*

They are technologically more advanced and latest ones, when compared to the traditional crimes.

6. *Victims not revealing their Identity/Victimization*

Most of the victims of internet crime remain anonymous till discovery of some pictures or images by the law enforcing authorities during an investigation.

7. *Rarely Reported*

[17] Apart from obtaining financial gain or other material benefits from committing cyber crime offences, perpetrators also misuse computer technologies and information and communication networks driven by socio-psychological motivations.

[18] Wojciech Filipkowsk, Cyber laundering: an analysis of typology and techniques International Journal of Criminal Justice Sciences, Vol. 3. Issue 1. 2008

Many cases of cyber crimes are not reported. Most of the victims does not show interest in reporting, as they feel that, reporting would not serve any useful purpose, instead may damage them further..[19]

8. *Low rates of Arrest*

9. *Low rates of Conviction*

The fundamental principal of criminal law i.e, *proof beyond reasonable doubt*, makes it very difficult to ensure convictions in these cyber crime cases. Direct evidence is not available in majority of these cases.

Classification of Cyber Crimes on the Basis of 'Victim'

There are 4 major categories of cybercrimes.

1.Cyber Crime affecting the Persons and properties

These type of crimes include those directly affects persons or their properties. Malicious software is used to gain access to a web page containing confidential information

a) *Affecting Person*

These crimes affect the individual persons

Ex:-Cyber stalking and distributing pornography and trafficking.

b) *Affecting Property*

The hacker steals a person's bank/credit card details to gain access to funds, make purchases online run phishing scams to get information from the people

2. *Cyber Crimes against the Companies/ Organizations*

This includes hacking of a company's products of known as cyber extortion and data breaches etc.,which is very often takes place.

[19] According to the Computer Crime and Security Survey, 70 percent of those not reporting cyber crimes cited negative publicity as a reason.

3. *Cyber Crimes against the Society*

These crimes affects the entire society, which include,

- Economic offences affecting public institutions,
- Prohibited products Sale, trafficking,
- Forgery and internet gambling.

4. *Cyber Crimes against the Government*

This is one of the worst and the least common type of cybercrime in the world, but the most serious offence. It's also known as *cyber terrorism*. These crimes consists of forced trespassing into the government network systems, defacing the military websites and to spread false propaganda, executed by generally by the terrorists/enemy countries.

a. Financial Crimes' in Cyberspace

Today's internet plays a vital role in a vast number of money-making enterprises, including those of the criminal kind. Illegal activities that existed long before the internet, such as theft and swindling, now flourish on the World Wide Web. The internet allows criminals to hide their real identities and easily, cheaply obtain specialised software tools, such as malware, for stealing sensitive data from anywhere. Internet crime is borderless and requires coordination among national authorities.[20] White collar offenders belong to the top management in the organisation and a whistle-blower is at the risk of employment.[21]

'Dark Web'[22] is found to be promoting/boosting the Financial Crimes[23] on Internet on account of which these are risen very fast. The Most Popular Financial Crimes in Cyber Space include, Phishing/ Spoofing, Malware , Identity Theft and Carding

[20] Just in the past few years, startling data has revealed the rise of financial digital frauds.

[21] Deb Shinder, Profiling and categorizing cybercriminals, https://www.techrepublic.com/blog/it-security/profiling-and-categorizing cybercriminals/

[22] the portion of the internet unavailable through traditional browsers and only accessible via specific protocols and encrypted networks. Cyber Money laundering takes places online because the *Dark Web* allows illicit funds to be transferred to and from multiple anonymous accounts, assisting the launderers get illegally acquired money.

[23] The Evolution of Financial Crime in the Dark Web- Fraud Watch International; Nov 02, 2018