International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 22-02-2023, Accepted: 11-03-2023, Published: 25-03-2023
Volume 9, Issue 2, 2023, Page No. 44-45

Cyber crime and classification

Pardeep Kaur[1], Dr. Simranjeet Kaur[2]
[1] Research Scholar, CT University, Ludhiana, Punjab, India
[2] Principal, School of Law, CT University, Ludhiana, Punjab, India

Abstract
Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation's security and financial health.

Keywords: cybercrime, commerce, breaching privacy

Introduction
Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which take place an over the medium of computers or internet or other technology recognised by the I.T act. Cyber crime is the most prerialent crime playing a devastating role in modern India. There are number of Illegal activities which are committed over the internet by technology skilled criminals.

Characteristics of cyber crime
The concept of cyber crime is very different from the traditional crime. Also due to growth of internet technology, this crime has gained serious and infettered attention as compared to the traditional crime. So it is necessary to examine the peculiar characteristics of cyber crime.

People with specialised knowledge
Cyber crimes can only be committed through the technology thus to commit this kind of crime one has to be very skilled in internet and computers and internet to commit such a crime. the people who have committed cyber crime and well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to take the perpetrators of cyber crime.

Geographical challenges
In cyberspace the geographical boundaries reduce to zero. A cyber criminal in no time sitting in any part of the world commit crime in other corner of the world For example a hacker sitting in India hack in the system placed in U.S.

Virtual world
The act of cyber crime takes place in the cyber space and the criminal who is committing this act is physically outside the cyber space. Every activity of the criminal while commuting that crime is done over the virtual world.

Collection of evidence
It is very difficult to Collect evidence of cyber crime and prove of cyber crime The criminal in cyber crime invoke jurisdiction of several countries while committing the cyber crime and at the same time he is sitting same place safe where in net traceable.

Magnitude of crime unimaginable
The cyber crime has the potential of causing injury and lass of eye to an extent which cannot be imagined. The offenses like cyber terrorism,cyber pornography etc has wide reach and it can destroy the websites, steal data of the companies in no time.

Classification of cyber crimes
Cyber crimes can be classified in to 4 major categories as the following:

1. Cyber crime against Individual
2. Cyber crime Against Property
3. Cyber crime Against Organization
4. Cyber crime Against Society

Against Individuals
Email spoofing
A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.

Spamming
Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

Cyber defamation
This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

Harassment & cyber stalking
Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

Against Property
Credit card fraud
As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

Intellectual Property crimes
These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

Internet time theft
This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

Against organisations
Unauthorized accessing of computer
Accessing the computer/network without permission from the owner. It can be of 2 forms:

(1) Changing/deleting data: Unauthorized changing of data.
(2) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

Denial of service
When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

Computer contamination / Virus attack
A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

Email bombing
Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

Salami attack
When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

Logic Bomb
It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

Trojan Horse
This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Data diddling
This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Against Society
Forgery
Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

Cyber terrorism
Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.

Web Jacking
Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

Conclusion
The Internet has become a tool of evil deeds that are exploited by intelligent people for evil motives and sometimes for financial gain. Thus, at this point in time, cyber laws come into the picture and are important for every citizen. Due to the fact that cyberspace is an extremely difficult territory to deal with, some activities are classified as grey activities that cannot be governed by law.It can be prevented if lawmakers, internet providers, banks, shopping websites and other intercessors work together.
However, ultimately, it is up to the users to participate in the fight against cyber crime. The only way for the growth of online safety and resilience to take place is through the consideration of the actions of these stakeholders, ensuring they stay within the confines of the law of cyberspace

References
1. https://wwwgreeksforgreek.org. https://wwwbhatandjoshiassociation.com
2. https://blog.ipleader.in.
3. https://www.lawyersclubindia.com/amp/articles/classification-of-cybercrimes--1484.asp#amp_tf=From%20%251%24s&aoh=16774053754302&referrer=https%3A%2F%2Fwww.google.com.