North Asian International Research Journal of Social Science & Humanities

ISSN: 2454-9827 Vol. 5, Issue-5 May-2019

IRJIF: 3.015

Index Copernicus Value: 57.07 Thomson Reuters ID: S-8304-2016

A Peer Reviewed Refereed Journal

CYBER CRIME: LAW AND SOCIETY

***DR.DEEPIKA BHATNAGAR**

****Associate Professor, SVIL, Indore***

ABSTRACT:

The Cyber use is very fast and now it is becoming the life of everyone. It is as parallel as our life. Few years back nobody can imagine about the cyber crime. But today it is a emerging a serious threat. Worldwide it is spreading like a disease. The government, Police department, Intelligence units have started to react on this. There are many types of cyber crimes. Indian Police has initiated to curb across the country.

Key words: ***Cyber Terrorism, Hacking, Identity Theft, Pornography, Vandalism.***

INTRODUCTION:

We are living in the modern era of Technology. We are depending on the technology of an extent that without it we don't even think to move a single step. Use of Internet is very common. This name is a common to everyone. Computer and Internet are becoming the part of our life. With the help of these two our life is becoming easier. Cyber crime is a criminal act related to computers and networks.

The history of computers and networks came into the year of 1990's.In that era hacking was the job to get more information about the systems on competition basis and win the tag of best hackers award. The result of this was much malicious software becoming ubiquitous during the same period. Right from the military to commercial organizations all were affected by the Hacking, result was that network and system slow. Cyber criminals like Hackers they are became more skillful, they always gain benefit to explore and using their started using their knowledge and expertise to gain benefit by exploiting and victimizing others.

In the current modern society the usage of internet is increasing day by day. It makes the world small and people coming closer. Fast rapid growth of technology has provided the big area of new opportunity and efficient sources for the organizations. It is nation asset because the nation security is depending on it.

Cybercrime which is a crime in which the object of the crime is a computer. Cyber crime is any criminal act related to computers and networks it is an unlawful act where the computer is used as a tool or target or both. We know about all type of cyber crime which is also known as computer crime e-crime, hi-tech crime or electronic crime which is nothing but an activity done with a criminal intention in cyber space. Persons those indulging in cyber crimes are not driven by ego or expertise but they want to gain profit quickly by using their knowledge. Fast gain is main aim for these criminals. They expertise to steal, deceive and exploit people to earn money. Cyber crimes is very different from old days crime like robbing, mugging, stealing. It is now a real threat for everyone Cyber crime can be handled single and no need to present criminal physically. It can be committing from the remote area also.

Computer crime and Cyber crime are distinguished from each other but cyber crime is using as a umbrella term for various crime committed by WWW that is world wide web.

DIVISION OF CYBER CRIME: MAINLY CYBER CRIME IS DIVIDED INTO THREE DIVISIONS NAMELY

Government: Whenever any crime committed against the government it is considered as cyber terrorism. In this type of crime cyber criminals hack government websites, confidential documents, Military documents and many more important documents. After success they will create havoc and panic situation for civilian population.

Property: This type of division is very dangerous to the individual because it will create problem financially, resort to stealing and robbing. In this type criminal can take out money from his credit card ,bank details, numerous purchase from online, use malicious software to gain access to the organization's website, it will damage software and hardware to. This type of division is high profile division.

Individual: This type of cyber crime is different from the other two divisions. It can be in can be in the many form like cyber stalking, distributing pornography, trafficking and "grooming". Law enforcement agencies are taking this crime very seriously.

TYPES OF CYBER CRIMES:

Hacking: Hacking is a crime in which deals with sending illegal instruction to any other computer or network. In this crime a person's computer is broken into so that his personal or sensitive information can be accessed. Ethical hacking is different from Hacking In hacking, if the person's computer is hacked so that his personal and sensitive information can be accessed. In this crime person may not be aware that his computer has been hacked. Hackers use many type of software for hacking.

Theft or Piracy: This type of cyber crime related to the violation of the copyright for like violation of the copyright of the music, violation of the Copyright of the movie, violation of the copyright on the games also the violation of the copyright on the any type of software. Nowadays there are many websites which encourage piracy, these illegal websites targeted by FBI and our justice system is addressing this crime with the help of many Laws,

Cyber Stalking: In this kind of Cyber Crime the victim is subjected to a barrage of online messages and emails called online harassment. In this type usually the stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Cyber Terrorism: This type of cyber crime attacks on individuals, government, and organizations. It is also known as information wars. This can be defined as an act of the internet terrorism which includes deliberate and large scale attacks. In these disruptions of computer networks using computer viruses, or physical attacks using malware, the goal of terrorism is to create a feeling of terror in the minds of the victims. .

Identity Theft: This is related to cash transaction by using internet and using banking transactions. It now a very big and major problem with those persons who are doing every transaction by using internet, Criminals accesses data of a person's bank account, details and buy many things by his name. The result of this crime is major financial loss.

Child pornography and Abuse: The type of crime against the children. In this crime Child used to abuse sexually. In this criminals solicit via chat rooms for the purpose of child pornography. Cyber Security department doing regularly monitoring these chat rooms to control and reducing the child abuse.

Computer Vandalism: This type of crime is considered as a malicious behavior that involves damages computers and data in various ways and potentially disrupting business. Viruses attach themselves to the existing programs and they are different from Computer vandalism.

Malicious Software: In Malicious software there are internet based software or programmed for using disrupt a network. This software always access to the computer system to steal sensitive information or data. This causes the damage to software.

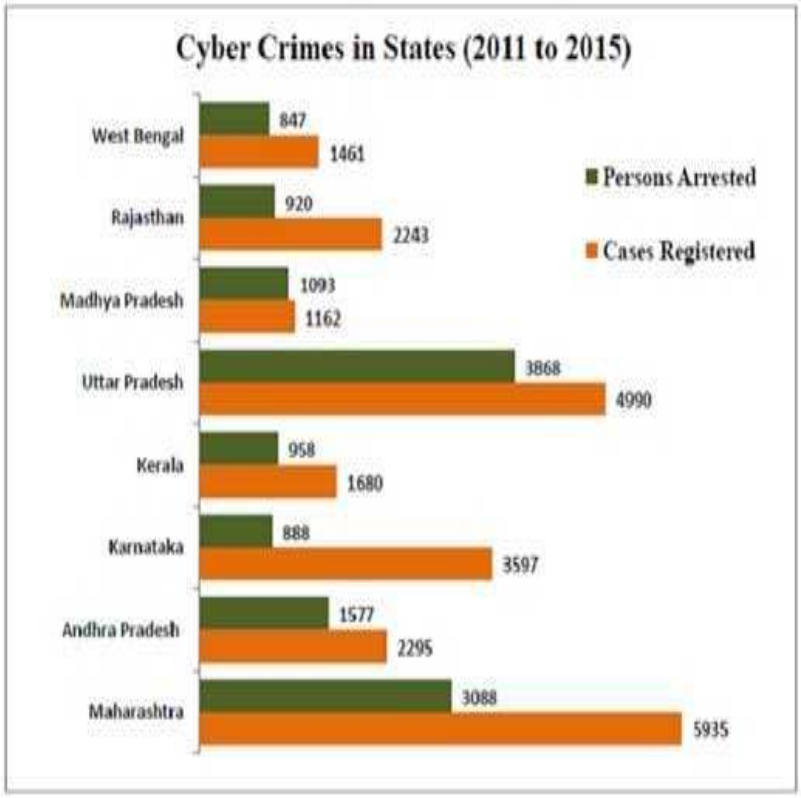
CAUSES OF CYBERCRIME:

Cyber crime is a very easy way to earn huge amount in a very short period of time. Cyber criminals always attack like Banks, Big industries, Casinos, big financial Institutions, Hotels and many other big Money stockers. These criminals have simple cause behind it that attack on that place where huge amount of money flows and sensitive information can catch. Catching of these criminals are very difficult because they can operate their target from huge miles away. Computers are vulnerable that why the cyber criminals are increasing day by day. The causes behind the cyber crime are as follows:

- **Small space for storing Data:**– The computer does not have big space to store data and this is very good opportunity for the cyber criminals to steel data from the computer and earn profit.
- **Complex in Nature** – The nature of computer is very complex because it does not run without computers millions of codes. Human mind is not a machine ,it is imperfect in front of the computer because it always does mistake at any stage and that is the time of criminals to act on their own benefit
- **Human Negligence** – Human Negligence is one of the basic characteristics of human conduct. This negligence give opportunity to the criminals the access and control over the computer system.
- **Loss of evidence** – The data related to the crime can be easily destroyed. Evidence is very important step to investigate any type of crime but when the evidence is missed which is very common and obvious problem, that will paralyzes the system.
- **Access is very easy** – The computer is having many coding and complexity but decoding is also very easy to the criminals. So may Hackers are having the techniques to hack or steel data from any computer. Hackers are very intelligent they know how to decode any data, open the ratina image, how to open advanced voice recorder and that can fool biometric system very easily. Bypass firewalls can be use to get past security system.

IMPACTS OF CYBER CRIME:

The impacts of cyber crimes are very bad because if any cyber crime successful it will impact the large number of loss. Damages like damages on confidentiality, theft on intellectual property, loss of consumer confidence and faith, all cyber criminals' focuses on their attacks on large and small business. In 5 years more than 5900 cases are registered in Maharashtra and became at the top, Uttar Pradesh around 5000 cases at 2nd position and Karnataka at 3rd with more than 3500 cases.



Source:www.faclty.in.com

CYBER CRIME AFFECTS TO THE SOCIETY IN BOTH THE WAYS LIKE ONLINE AND OFFLINE.

The impact of cyber crime is immense. As per the report of Symantec, more than 1.5 million people fall victim to some sort of cyber crime every day, ranging from simple password theft to extensive. Another cyber crime like Piracy also affects the society. It effects on entertainment, music, films and also on software industries. Claims of damages are hard to estimate and even harder to verify, with estimates ranging widely from hundreds of millions to hundreds of billions of dollars per year. Social impact of the cyber crime also ranges very high. It involves bonnets, computer viruses, cyber bullying, cyber stalking, cyber terrorism, cyber pornography, identity theft and malware. Despite of lot of damaging impacts still people are not changing their behavior if they became victim or not taking precautions. In the current time Cyber Crime is a very big business opportunity driven by profit and also personal gain.

CYBER LAWS IN INDIA:

In India, to control Cyber Crime three important legislations are made. They are Information Technology Act, Indian Penal Code and State Level Legislation. These legislations having many sections which are related to cyber safety and Cyber crime. They are as follows:

According to Information Technology Act:

Section 65: Tampering with computer source documents
Section 66: Hacking with Computer systems, Data alteration
Section 67: Publishing obscene information
Section 70: Un-authorized access to protected systems
Section 72: Breach of Confidentiality and Privacy
Section 73: Publishing false digital signature certificates

In Indian Penal Code some sections related to cyber crime are as under:

Section 505: Sending threatening messages by email
Section 499: Sending defamatory messages by email
Section 463: Forgery of Electronic records
Section 420: Bogus websites, Cyber Frauds
Section463: Email Spoofing
Section 383: Web- Jacking
Section 500: Email abuse

Cyber Crime under special cells:

- Online sale of Arms Act
- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act

GOVERNMENT STEPS TO CURB THE CYBER CRIME:

1. The step should be taken by the state government to curb the cyber crime like new technique buildup, establishment of cyber police stations, new technical infrastructure and skilled manpower for registration, investigation, detection and prosecution of cyber crime.
2. Providing advanced and basic training to Law Enforcement Agencies, Forensic Labs and Judiciary regarding procedures and methods to collect analyze and present digital evidence by Indian Computer Emergency Response Team (CERT-In)
3. Centre for Development of Advanced Computing (CDAC).
4. At the Central Bureau of Investigation (CBI), training of Forensic Lab has been set up to give training to Cyber Crime Police Officers. And also, in the states of Kerala, Assam, Mizoram, Nagaland, Arunachal

Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir government have set up training forensic labs.

5. NASSCOM, DSCI (Data Security Council of India) have been set up at Mumbai, Bangalore, Pune and Kolkata for creating awareness regarding Cyber Crime.
6. CERT-In has published guidelines for securing the websites which are available on www.cert-in.org.in and also conduct regular training programs to make system administrators aware regarding cyber attacks.
7. Through Crime and Criminal Tracking Network and Systems (CCTNS) Government has decided to provide a centralized citizen portal for registering online cyber complaints.
8. For fighting the against the cyber crime it is the duty of the Ministry of home affairs to set up the Indian Cyber Crime Coordination Center and also generate the open platform to raise complaints by the victims.

PRECAUTIONS:

As we are using regularly computer, Net, all transactions related to cyber it our duty to take all the precautions so that we can save us.

1.Awareness among the people who do not know about the cyber crime.

2.Training for using internet, computer, credit card, debit card etc

3.Awareness about Government Initiatives, all laws related to cyber crime and safety.

4.Unique password, run always anti-virus software, watches suspicious emails.

5.Avoid sending any photographs online particularly strangers.

6. Avoid disclosing any information pertaining to one.

7.Always use latest and update antivirus.

8..Never send your credit card number to any site.

9..Keep backup files.

10.Using Firewalls may be beneficial

EMERGING TRENDS OF CYBER LAW:

In the recent years many cyber crimes are reported. The trends of cyber attacks are changing their mode. Organizations should strength their data supply chains with better inspection methods. Cloud computing is a major new trend in cyber crime. The growth of Bit coins and another virtual currency is another crime which is likely to grow in near future. Unauthorized access to network are increasing very fast, growing privacy is another major call in emerging trends.

CONCLUSION:

Controlling cyber crime is a very big task in front of the government. Much legislation has been passed but still the growth of cyber crime is increasing day by day. It is very difficult to eliminate cyber crime from the cyber space. People should aware about their rights and duties and more stringent to check crime. There is a need to bring changes in the Information Technology Act so that it will combat cyber crime. Then only our country will be safe from cyber crime.

REFERENCES:

1. Cyber Crime Today &Tomorrow
2. Crime in India, 2012 statistics, Report on Cyber Crime-chapter 18"- NCRB report
3. Crime in India, 2013 statistics, Report on Cyber Crime-chapter 18"- NCRB report
4. *Wikipedia-Cyber crime, Google.*