Review of Cyber Crime in India: An Overview

Nidhi Kataria Chawla (Assistant Professor)[1], Aarti Singh (Assistant Professor)[2]
Babu Banarsi Das University
Lucknow (U.P)
India
ernidhikataria@gmail.com[1], aarti.singh18oct@gmail.com[2]

Abstract: **Cybercrimes are the Offences that are committed by individuals or groups of individuals with a criminal motive to intentionally harm the victim using telecommunication networks such as Internet [1]. They are responsible for creating the disturbance in normal computer functioning and create many problems for companies. This research paper aims to discuss following aspects of Cybercrimes: the definition, why they occur, methods of committing cyber crimes, year wise record of cyber crimes and their comparison. Also, this report will display statistical data which will give an idea of how far cybercrimes has increase over the period of five years.**

Keywords: Introduction, Types of crimes, statistics and their comparison**.**

I. INTRODUCTION

With the evolution of the Internet, there is another insurrection of crime where the initiator commits crime and offences on the World Wide Web. Cyber crime is a crime that is committed on the Internet, using the Internet and by means of the Internet like phishing, credit card frauds, bank robbery, illegal downloading, industrial spying, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and distribution of viruses, Spam etc.[2]. The exact definitions of "cybercrime" is "Cybercrimes is defined as any type of illegal activity that makes use of the Internet, a private or public network, or an in-house computer system[3]. Many forms of cybercrime revolve around the unauthorized use of proprietary information. As cyber crimes are a growing day by day around the world, many countries have started to implement laws and other regulatory mechanisms to minimize the incidence of cybercrime.

II. TYPES OF CYBERCRIMES

Cybercrime ranges variety of activities. Cyber crime can be basically divided into three major categories:

A. Cyber crimes against persons like harassment occur in cyberspace or through the use of cyberspace. Harassment can be sexual, racial, religious, or other.
B. Cyber crimes against property like computer wreckage (destruction of others' property), transmission of harmful programs, unauthorized trespassing, unauthorized possession of computer information.
C. Cyber crimes against government like Cyber terrorism [4].

A Crimes against persons are:

- **Cyber-Stalking**: It means to create physical threat that creates fear to use the computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material**: It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- **Defamation:** It is an act of imputing any person to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmes. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is one of the serious cyber crimes known till date .Cracking means that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.
- **E-Mail Spoofing**: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its origin to be different from which actually it originates.
- **SMS Spoofing**: Spoofing is a blocking through spam which means the unwanted uninvited messages. Wrongdoer steals mobile phone number of any person and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.

- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.
- **Cheating & Fraud**: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography**: It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat**: refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones [5].

B Crimes against Property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects person's properties which are as follows:

- **Intellectual Property Crimes**: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting**: It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
- **Cyber Vandalism**: Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System**: Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.
- **Transmitting Virus**: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass**: It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts**: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

C. Cybercrimes against Government

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism**: Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare**: It refers to politically motivated hacking to damage and spying. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software**: It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information**: It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Some other Cybercrimes against Society are An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes: Child Pornography, Cyber Trafficking, Online Gambling, Financial Crimes, and Forgery.

III. STATISTICS AND THEIR COMPARISON

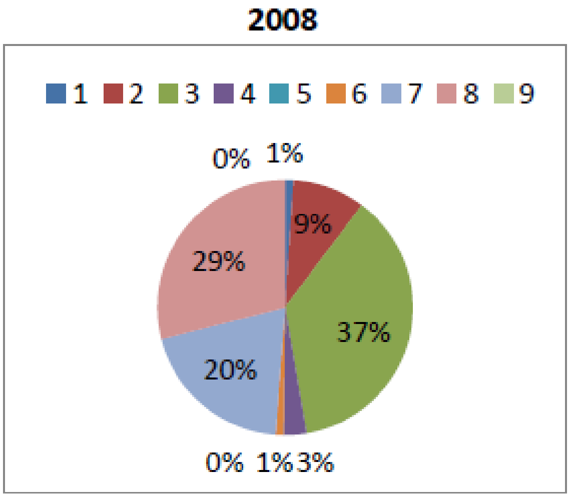
The following table shows the comparison of cybercrime statistics in 2008 to 2012. **[6]**

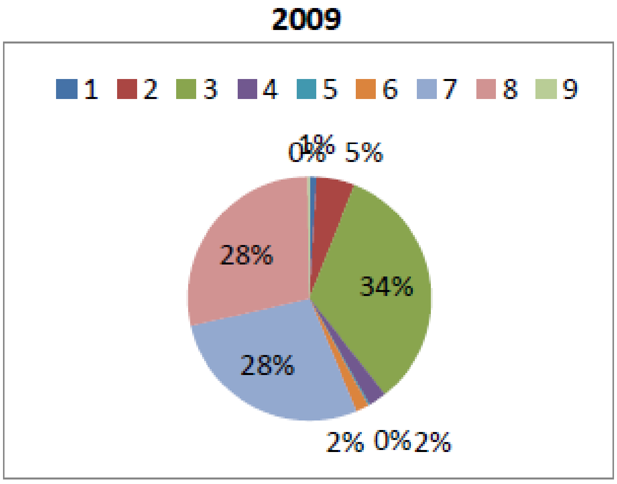
Table 1: Percentage variation of cyber crimes registered and persons arrested in 2008 to 2012

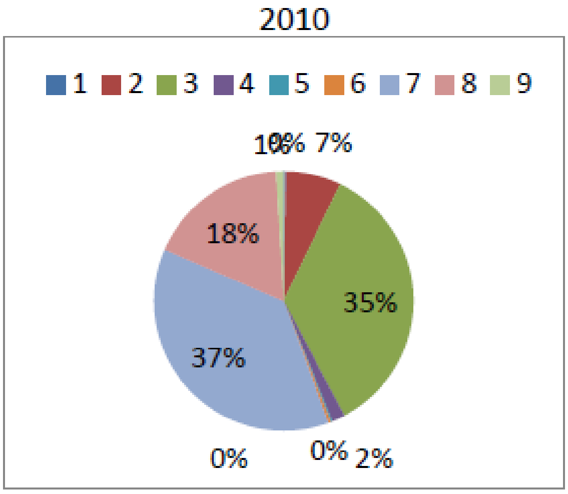
S.No	**Crimes**	**Case Registered**					**% Variation in 2012 over 2011**	**Persons Arrested**					**% Variation in 2012 over 2011**
		2008	2009	2010	2011	2012		2008	2009	2010	2011	2012	
1	Fraud Digital Signature Certificate	3	4	3	157	176	12.1	3	0	6	8	134	97.1
2	Tampering computer source documents	26	21	64	94	161	71.3	26	6	79	66	104	57.6
3	Obscene publication/transmission in electronic form	105	139	328	496	589	18.8	90	141	361	443	497	12.2
4	Breach of confidentiality/privacy	8	10	15	26	46	76.9	3	3	5	27	22	-18.5
5	Publishing false Digital Signature Certificate	0	1	2	3	1	-66.7	0	0	0	1	0	-100.0
6	Un-authorized access/attempt to access to protected computer system	3	7	3	5	3	-40.0	0	1	16	15	1	-93.3
7	Loss/damage to computer resource/utility	56	115	346	826	1440	74.3	41	63	233	487	612	25.7
8	Hacking	82	118	164	157	435	177.1	15	44	61	65	137	110.8
9	Obtaining licence or Digital Signature Certificate by misrepresentation/suppre	0	1	9	6	6	0.0	11	0	1	0	5	-

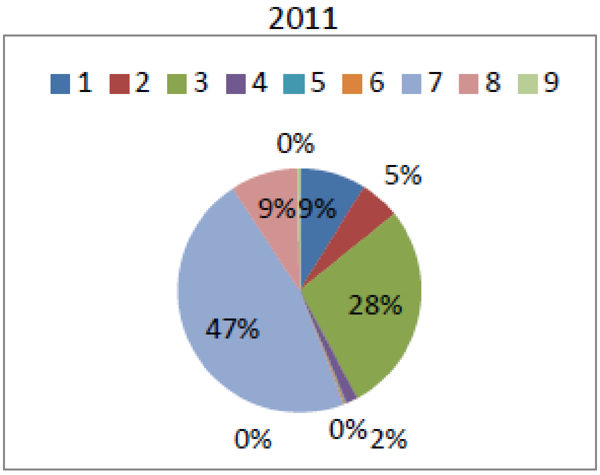
	ssion of fact												
	Total	283	416	934	1770	2857		189	258	1020	1112	1512	

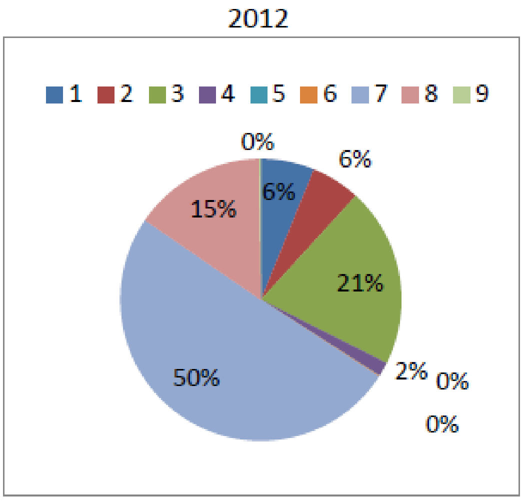
Pie Charts to show the variation of case registered from 2008-2012:











IV. CONCLUSION:

From above table we can conclude that from 2008 to 2012 the cyber crimes are continuously increasing but except publishing false Digital Signature Certificate, this crime was decreased in 2012 in comparison of 2012. There is highly increase in loss /damage to computer resource /utility and hacking crimes in 2012.On the other side we see the person arrested against their crimes are also increased. This is the good sign that our government is quite attentive now in respect of cyber crimes. There are number of laws against cyber crimes.

REFERENCES

[1] https://en.wikipedia.org/wiki/Cybercrime
[2] http://www.cyberlawsindia.net/internet-crime.html
[3] http://www.legalindia.in/cyber-crimes-and-the-law
[4] http://www.slideshare.net/likanpatra/cyber-crime-25646273
[5] http://www.wisegeek.com/what-is-cybercrime.htm
[6] Rupinder Pal Kaur, IJECS Volume 2 Issue 8 August, 2013 Page No.2555-2559