

CYBER CRIME-AN OVERVIEW*Abstract*

Crimes are considered as an act against the society. The advent of computer and internet was considered as an important factor for the national and international development. Advancement in computer technology ended in a positive impact on the national economy of India. On the other hand more and more inventions in the computer and internet field ended in new types of crimes committed through computer and internet. The increase in the rate of technology in computers has led to the enactment of Information Technology Act, 2000. Different types of cybercrimes are increasing day by day because they lack of knowledge and poor implementation of laws by the law enforcing authority. The present paper focuses on the meaning and nature of crime, Kinds of Cyber Crimes, analysis of one decade data on cybercrimes. The primary object of the paper is to identify the nature of the cybercrime by examining the past and present and future with the help of the existing primary and secondary data, by adopting doctrinal, analytical and historical method of research.

Key words: Crime, Cyber Crime, Information Technology, Indian Penal Code.

Authors

Madhu Kumar R.N.

Assistant Professor of Computer Science, JSS Law College, Mysore.

Mahesha B.P.

Assistant Professor of Law, JSS Law College, Mysore.

CYBER CRIME- AN OVERVIEW

I. Introduction

Computer is a fast and accurate electronic machine, which processes data and gives us results in the form of correct information. With the invention of computer, life has become easier and more comfortable for man. The history of computer can be understood by looking into the development of computing. The story of computing may be started with the machine abacus. The Abacus machine was used for 5000 years.¹ In 17th Century John Napier invented the Napier's Bones. This was used as multiplication tools.²

Blaise Pascal first developed the adding machine in 1642.³ Charles Babbage invented the difference engine to solve the polynomial equations in 1791 using the grant provided by the British government. But this machine was not working as expected. So he designed another machine called analytical engine by using cogs and wheels. A French textile weaver Joseph Marie Jacquard made the next great contribution to the development of Computer in 1801. He invented the *Jacquard Loom*, used punched card to automate the weaving process. Later, in 1834 *Charles Babbage* designed a calculating machine and called it the *Analytical Engine*. This machine could do all calculations like addition, subtraction, division and multiplication automatically.⁴ In 1888, American inventor *Herman Hollerith* devised a punched card system for tabulating the results of census. To be added Hollerith's machine got widespread success. In 1924, the name was changed to International Business Machines Corporation (IBM). The first electronic digital computer called ENIAC (Electronic Numerical Integrator and Calculator) was developed by the J. Prosper Eckert and J.W. Mauchly of Moore School of Electrical

¹ The Latin word came from Greek ἄβαξ abax it means "board strewn with sand or dust used for drawing geometric figures or calculating. The abacus, also called a counting frame, is a calculating tool used primarily in parts of Asia for performing arithmetic processes. The Abacus was developed in China. It was the first calculating device. It consists of a frame which is divided into two portions by a horizontal bar and vertical threads. Each thread has seven beads. Two beads are shifted on the upper portion and the other five beads are shifted at the lower portion of the frame. These beads are used for mathematical calculations. Today, abaci are often constructed as a bamboo frame with beads sliding on wires, but originally they were beans or stones moved in grooves in sand or on tablets of wood, stone, or metal. The abacus consists of beads strung on wires.

² The Napier's Bones is having a set of 11 rods, each having four faces. These were used as multiplication tools.

³ This machine had a series of numbered wheels and gears. Numbers were entered by rotating these wheels. It helped to add and subtract numbers. This machine was called Pascal's Arithmetic machine or Pascaline.

⁴ Charles Babbage is called the Father of Computers for his contribution to the development of computers.

Engineering, University of Pennsylvania in 1946. The machine was big and it could perform 5000 additions or about 400 multiplications in a second.⁵ The rapid development of the computer electronics can be seen after 1946. The inventions of microprocessor have triggered off revolution in the field of digital technology. Because of the nature of speed, accuracy, efficiency, storage, versatility the computer has now become a part of human life. Life without computer is unimaginable in the modern world.

II. Development of Information Technology(IT) and its impact on National Economy

In the last decades, Information Technology (IT) sector has grown at a great speed. In India it has made a significant impact on setting in priorities and organizational development in different sectors. The growth of IT in India characterized as ‘an island of competitiveness’, this industry’s comparative advantage was drawn from the technical base of India’s higher education as exemplified by the Indian Institutes for Technology(IITs) and Regional Engineering Colleges.⁶

The rise of IT, Software and Hardware services industry during the 1990s represents one of the most spectacular achievements of the Indian economy. The industry has grown at an incredible rate of 50% annum. Over the past few years it is highly export-oriented has established India as an exporter of knowledge-intensive services, and has brought in a number of other spillover benefits such as creating employment and new pool of entrepreneurship. The evolution of India as an exporter of these knowledge-intensive services has also created much interest in the development of community worldwide. Encouraged by the Indian success, a number of other developing countries are trying to emulate it in entering the industry.⁷

The IT sector is a proved engine for global economic growth. The IT sector consists of hardware, software, and IT services consists of 1.1Million IT businesses, supporting 1.4 million high-paying IT jobs who are generating nearly \$900 Billion

⁵ The machine is big and to create these machine 18,500 vacuum tubes, weighed 30 tones, and occupied 1,500 square feet of Flore space.

⁶ Information Technology and Social Development, C. Ramachandraliah, Economic and Political Weekly March 22-29, 2003, p.1192

⁷ Indian Software Industry development – International and National Perspective, Nagesh Kumar, Economic and Political Weekly, November 10, 2001, p. 4278.

annually in taxes, and adding \$1.7 Trillion per year to global economic prosperity.⁸As there is rapid growth in the international IT trade where business and consumers are increasingly using computers to create, transmit and to store information in the electronic form of rational paper documents. This helps in protecting the environment and it made work easier and time saving. Because of this reason the Government of India announced the 'Digital India Scheme'. In this scheme few government services are going to be provided through online. i.e. LPG direct subsidy deposit Scheme, Digital Documentation etc.

Modern society relies heavily on computer technology. Inventions, discoveries and technologies, widen scientific horizons but also pose new challenges for the legal world. Information technology brought about by computers, internet and cyberspace has also posed new problems in jurisprudence. These problems have arisen in all areas of law. The law (statutory or otherwise) providing answers to these problems or dealing with information technology are sometimes loosely referred to as "computer laws" or "information technology laws" or simply "cyber laws".⁹

III. Meaning of Crime and Cyber Crime

Crime is an act against individual and society. A crime is an act or omission which is prohibited by law as injuries to the public and punished by the state. A crime is an act deemed by law to be harmful to society in general, even though its immediate victim is an individual.¹⁰Crime committed over the internet is called as cybercrime.¹¹Cybercrimes are considered as a highly intelligent crime. Cyber offences are the unlawful acts which are carried in a very sophisticated manner. In cyber offences the physical presence of the criminals in the place of incidence of cybercrime is absent as compared to general kinds of crimes. Criminals are sitting in remote place or without leaving any identity or in fake identity commits the crime.

⁸ Executive summary of expanding the Frontiers of our digital Future: Reducing Software Piracy to Accelerate Global It Benefits, Published by BSA and IDC on December 2005.

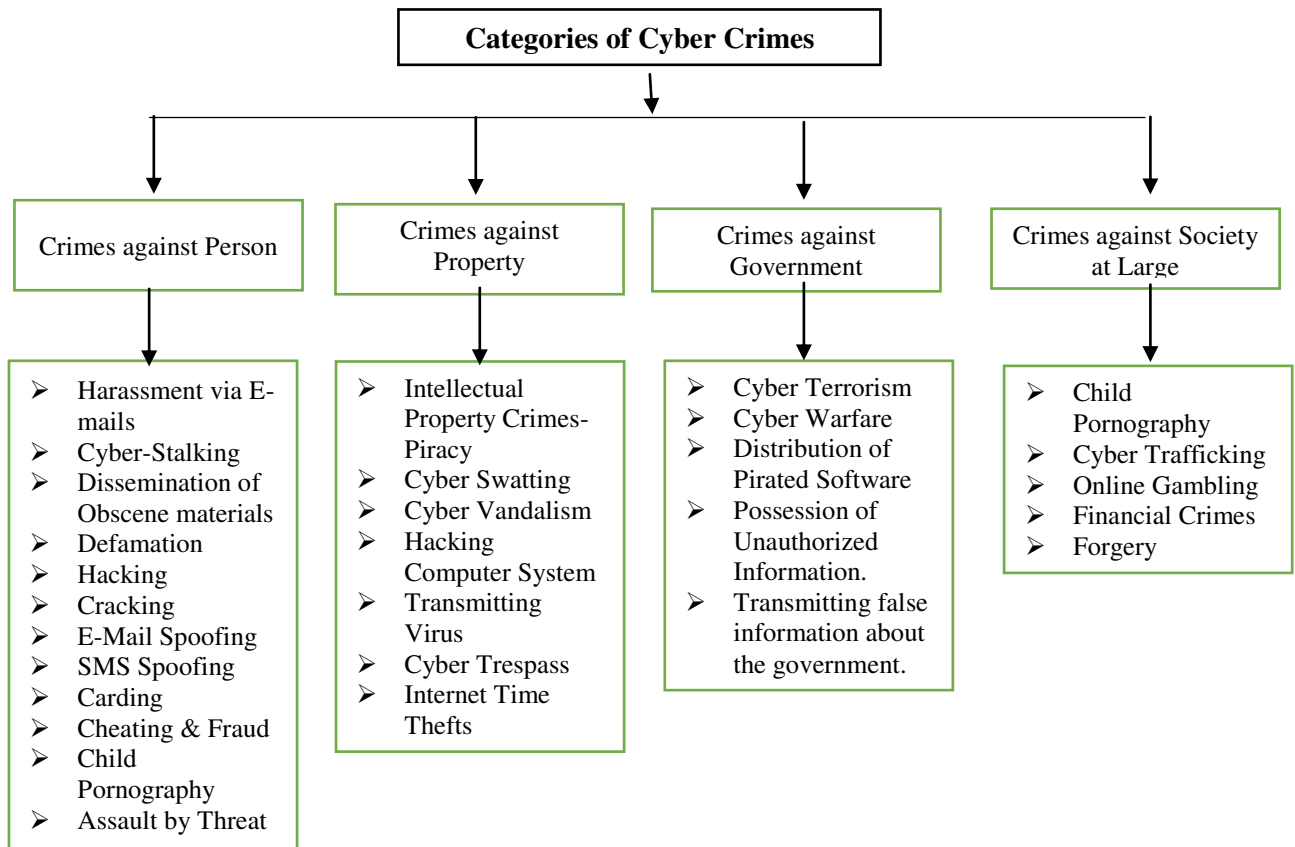
⁹ Open Source software and Intellectual Property rights, By Justice Yatindra Singh, Supreme Court Cases, (2004) 4 SCC(Journal Section) 28.

¹⁰ P. Ramanath Aiyer, 'Concise Law Dictionary, 3rd Edition 2008, Lexis Nexis Butterworth's Publication, p. 291

¹¹.P.S. R Sadhandham v. Arunachalam, AIR 1980 SC 856.

IV. Categories of Cyber Crimes

Cybercrimes generally be classified into different categories. These categories can be understand in the following Chart.



(Chart .1)

The above indicates the different kinds of crimes committed with the help of or through computer or internet. Cyber Crime is considered as an act against Person, or Property or Government and Society at Large depending upon the impact of the crime. At large computer crimes always affect the companies. The reason being majority of the companies are using computer in all sectors. This led the companies to be the victim of Cyber Crimes. In modern cyber technology world it is very much necessary to regulate cybercrimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers. The United Nations Commission on International Trade Law adopted the Model law on electronic Commerce in 1996. The General Assembly of United Nation’s mandate the member’s country to enact uniform Model law for equal legal treatment of users of electronic communication and paper based communication. This made the Indian parliament to enact a law called Information Technology Act, 2000(IT Act, 2000).

This was enacted with an objective to give a fillip to the growth of electronic based transactions, to provide legal recognition for e-commerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology. This Act came into force on 17th October 2000. The Act comprises of XIII Chapter which contains 94 sections with 2 Schedules. This Act was amended in 2008 to address new issues in the cyber Crimes.¹²Till today there are 22 Rules, 3 Regulations and 6 Important Notifications notified for the better enforcement of the IT Act, 2000.

V. Kinds of Cyber Crime

According to Indian Bureau Crimes (IBC) Cybercrimes are new classes of crimes to India rapidly expanding due to extensive use of Internet and IT. The statistics on Cyber Crimes can be divided into two.

1. **Offences under the Information Technology Act, 2000:** Offences which are punishable under the IT Act 2000. Crimes punishable under this Act are, Tampering with the computer source documents, Hacking, Publishing of information which is obscene in electronic form, Contravention of the direction of the Controller, Misrepresentation, Breach of confidentiality & Privacy, and Publishing False Digital Signature Certificate.

2. **Offences under the Indian Penal Code:** Crimes committed with the use of computers can be punishable under IPC. Those crimes are, Obscenity, Forgery for purpose of the cheating or harming reputation, Sale, etc., of obscene objects to young person, Obscene acts and songs, Sending defamatory messages by e-mail, Theft of Computer Hardware and Software, Sending threatening messages by E-mail & criminal Intimidation, Bogus websites, Cyber Frauds, Criminal intimidation by an anonymous communication, E-mail Spoofing(Forgery) and Word, gesture or act intended to insult the modesty of women.

The following table shows the offences which are punishable under Information Technology Act, 2000 and Indian Penal Code, 1860 and other laws along with the punishment.

¹² Section 43A was inserted. According to this provision, 'Were a body corporate in marinating and protecting the data's of the person as provided by the central government, if there is any negligent act or failure in protecting the data/ information then a body corporate shall be liable to pay compensation to person so affected.

OFFENCES PUNISHABLE UNDER INFORMATION TECHNOLOGY ACT, 2000			
Nature of the Crime	Section & Punishment	Nature of the Crime	IPC Section & Punishment
Tampering with computer source Documents	Sec. 65 – Imprisonment upto 3 Years or with fine which may extend upto 2 Lakh or with both	Un-authorized access to protected system	Sec. 70 – Imprisonment extend to 10 years and with fine
Hacking with computer systems, Data Alteration	Sec. 66 – Extend to 3 Years or with fine extend upto 5 Lakh or with both	Failed to provide information as requested by Indian Computer Emergency Response Team	Sec. 70B – Imprisonment extend to 1 year or with fine extend to 1 lakh or with both
Sending offensive messages through communication service, etc	Sec. 66A – Extend to 3 Years and with fine	Penalty for misrepresentation	Sec. 71 – Imprisonment extend to 2 years or with fine extend to 1 lakh or with both
Dishonestly receiving stolen computer resource or communication device	Sec. 66B – Extend to 3 Years or with fine which may extend upto 1 Lakh or with both	Breach of Confidentiality and privacy	Sec. 72 – Imprisonment extend to 2 years or with fine extend to 1 lakh or with both
Identity theft	Sec. 66C – Extend to 3 Years and with fine extend upto 1 Lakh	Punishment for disclosure of information in breach of lawful contract	Sec. 73 – imprisonment extend to 3 years or with fine extend to 5 lakh or with both
Cheating by personation by using computer resource	Sec. 66D - Imprisonment upto 3 Years and with fine which may extend upto 1 Lakh	Publishing False digital signature certificates	Sec. 73 – Imprisonment extend to 2 years or with fine extend to 1 lakh or with both
Violation of privacy	Sec. 66E - Imprisonment upto 3 Years or with fine which may extend upto 2 Lakh or with both	Publication for fraudulent purpose	Sec. 74 – Imprisonment extend to 2 years or with fine extend to 1 lakh or with both
Cyber terrorism	Sec. 66F – Imprisonment for Life	Act to apply for offence or contraventions committed outside India	Sec. 75 – Same punishment as like the crime committed in India.
Publishing or transmitting obscene material in electronic form	Sec. 67 - Imprisonment extend to 3 Years and with fine which may extend upto 1 Lakh or with both	Compensation, penalties or confiscation not to interfere with other punishment	Sec. 77 – Punishment also can be given under any other law
Publishing or transmitting of material containing sexually explicit act, etc, in electronic form	Sec. 67A – 1 st time offence - Imprisonment extend to 5 Years and with fine; Subsequent conviction- imprisonment extend to 7 Years and fine extend to 10 Lakh	Other than the offences for which the punishment for life or imprisonment for term exceeding 3 years are compounding of offences	Sec.77A
Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Sec. 67B – 1 st time - Imprisonment extend to 5 Years and with fine which may extend to 10 Lakh or with both; Subsequent conviction – imprisonment extend to 7 years and with fine extend to 10 Lakh	Offences with three years and above imprisonment to be cognizable and the offence punishable with imprisonment of three years shall be bailable.	Sec. 77B
Preservation and Retention of information by Intermediaries	Sec.67C - Imprisonment extend to 3 years and fine.	Exemption from liability of intermediary in certain cases	Sec. 79

Power to issue directions for interception or monitoring or decryption of any information through any computer resource	Sec. 69 - Imprisonment extend to 7 Years and with fine	Punishment for abetment of offences	Sec. 84B
Power to issue directions for blocking or public access of any information through any computer resource	Sec. 69A - Imprisonment extend to 7 Years and with fine	Punishment for attempt to commit offences	Sec. 84C
Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security	Sec. 69B – Imprisonment extend to 3 years, shall also be liable to fine.	Offences by Companies	Sec. 85
OFFENCES UNDER INDIAN PENAL CODE			
Nature of the Crime	Section & Punishment	Nature of the Crime	IPC Section & Punishment
Obscenity	Sec. 292 - 1 st time imprisonment extend to 2 years and with fine extend to 2,000; 2 nd and subsequent conviction, imprisonment extend to 5 years and with fine extend to 5,000 rupees	Forgery for purpose of cheating	Sec.468 - Imprisonment extend to 7 years and shall also be liable to fine
Sale, etc., of obscene objects to young person	Sec. 293 - 1 st time imprisonment for extend to 3 years and with fine extend to 2,000; 2 nd and subsequent conviction, 7 years and with fine extend to 5,000.	Forgery for purpose of harming reputation	Sec. 469 – Imprisonment extend to 3 years and shall also liable for fine
Obscene acts and songs	Sec. 294 - Imprisonment extend to 3 months or with fine or with both	Sending defamatory messages by e-mail	Sec. 500 – Imprisonment extend to 2 years or with fine or with both
Theft of Computer Hardware and Punishment	Sec. 378 & 380 – imprisonment extend to 7 years and shall also be liable to fine.	Sending threatening messages by E-mail & Punishment for criminal Intimidation	Sec. 503 & 506 – Imprisonment extend to 2 years or with fine, or with both; If threat be to cause death or grievous hurt- imprisonment extend to 7 years; To impute, unchastity to woman – 7 years or with fine or with both.
Bogus websites, Cyber Frauds	Sec. 420 - Imprisonment extend to 7 years and shall also be liable to fine	Criminal intimidation by an anonymous communication	Sec. 507 – Imprisonment extend to 2 years in addition to the punishment provided for the offence by the punishment under Sec. 506
E-mail Spoofing(Forgery)	Sec.463 to 465 – Imprisonment extend to 2 years or with fine, or with both	Word, gesture or act intended to insult the modest of women	Sec. 509 – Imprisonment extend 3 years and also with fine.
PUNISHMENT UNDER OTHER LAWS			
Online sale of Drugs	NDPS Act	Online Sale of Arms	Arms Act.

(Table – 1)

Crimes committed under IT Act, 2000 and IPC are increasing year by year. Cyber Crimes/Cases registered and person arrested under IT Act, 2000 and IPC during 2003 to 2013 can be seen in the following table 2 and 3.

CYBER CRIMES/CASES REGISTERED AND PERSONS ARRESTED UNDER IT ACT 2000 DURING 2003 TO 2013

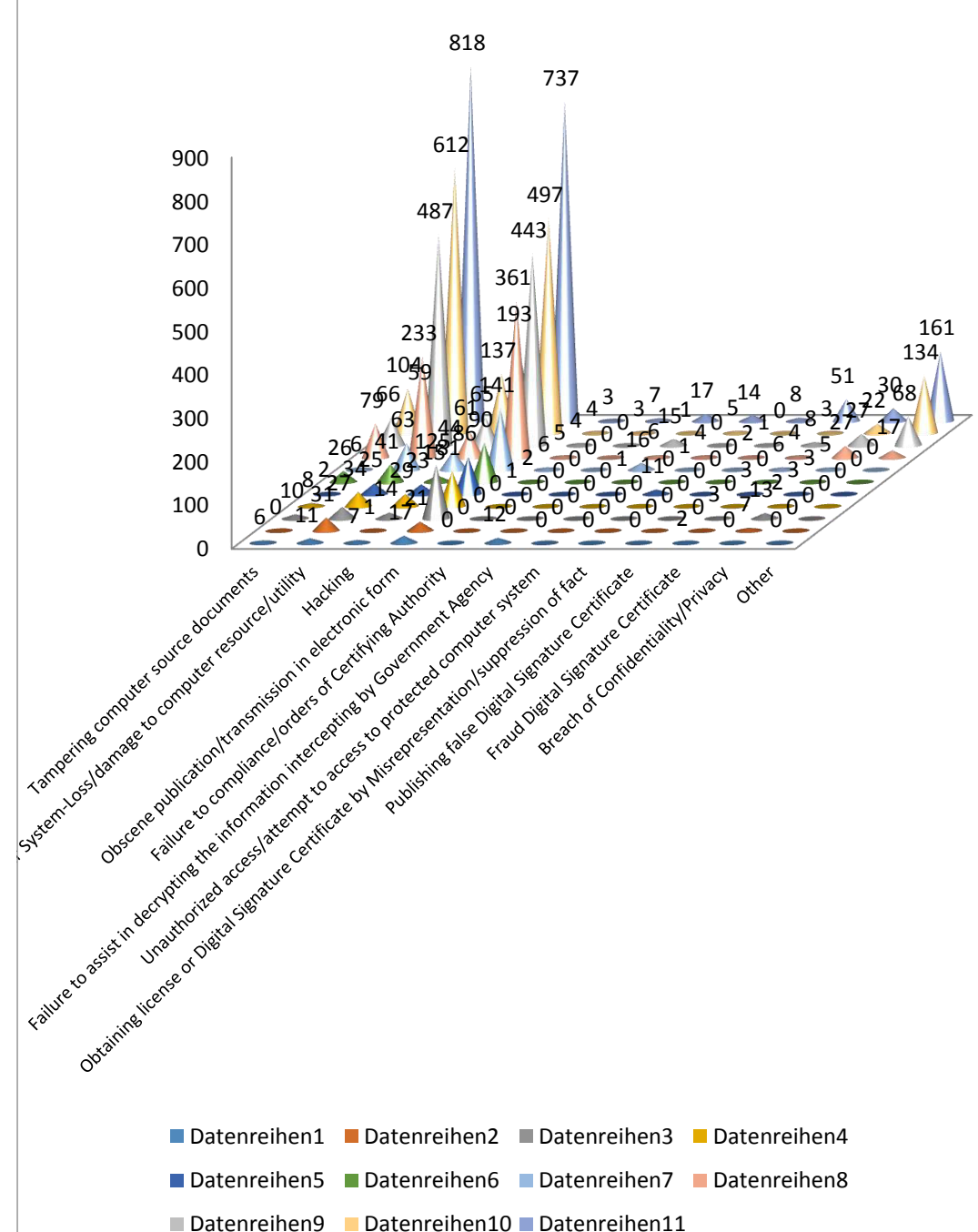
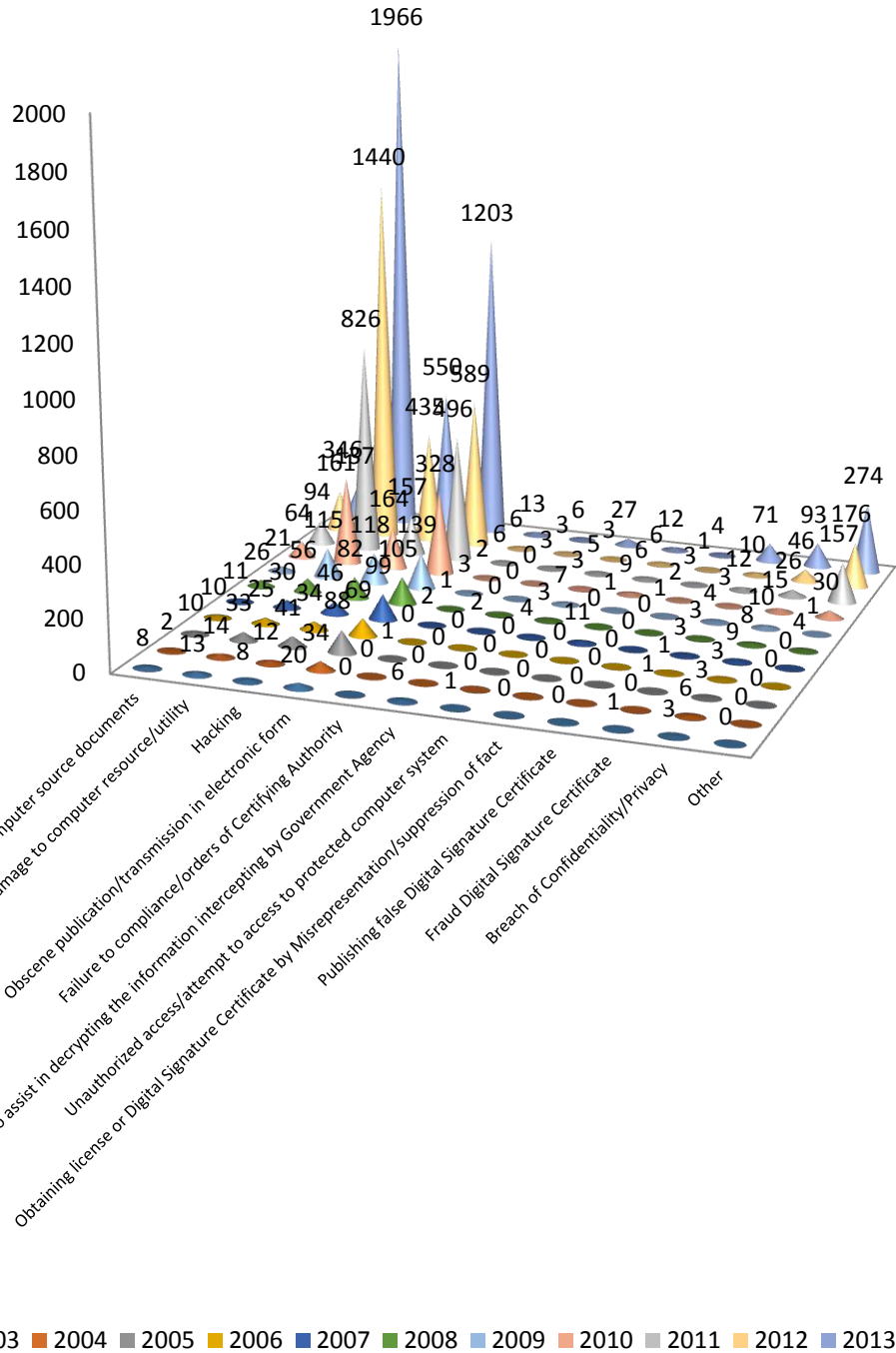
Crimes	Cases Registered From 2003 to 2013											Total	Person Arrested From 2003 to 2013											Total
	03	04	05	06	07	08	09	10	11	12	13		03	04	05	06	07	08	09	10	11	12	13	
Tampering computer source documents	8	2	10	10	11	26	21	64	94	161	137	544	6	0	10	8	2	26	6	79	66	104	59	366
Hacking with Computer System- Loss/damage to computer resource/utility	13	14	33	25	30	56	115	346	826	1440	1966	4864	11	31	27	34	25	41	63	233	487	612	818	2382
Hacking	8	12	41	34	46	82	118	164	157	435	550	1647	7	1	14	29	23	15	44	61	65	137	193	589
Obscene publication/transmission in electronic form	20	34	88	69	99	105	139	328	496	589	1203	3170	17	21	125	81	86	90	141	361	443	497	737	2599
Failure to compliance/orders of Certifying Authority	0	0	1	0	2	1	3	2	6	6	13	34	0	0	0	0	1	2	6	5	4	4	3	25
Failure to assist in decrypting the information intercepting by Government Agency	6	0	0	0	2	0	0	0	3	3	6	20	12	0	0	0	0	0	0	0	0	3	7	22
Unauthorized access/attempt to access to protected computer system	1	0	0	0	4	3	7	3	5	3	27	53	0	0	0	0	0	1	16	6	15	1	17	56
Obtaining license or Digital Signature Certificate by Misrepresentation/suppression of fact	0	0	0	0	11	0	1	9	6	6	12	45	0	0	0	0	11	0	1	4	0	5	14	35
Publishing false Digital Signature Certificate	0	0	0	0	0	0	1	2	3	1	4	11	0	0	0	0	0	0	0	2	1	0	8	11
Fraud Digital Signature Certificate	1	0	1	1	3	3	4	3	12	10	71	109	2	0	3	0	3	0	6	4	8	3	51	80
Breach of Confidentiality/Privacy	3	6	3	3	9	8	10	15	26	46	93	222	0	7	13	2	3	3	5	27	27	22	30	139
Other	0	0	0	0	0	4	1	30	157	176	274	642	0	0	0	0	0	0	0	17	68	134	161	380
Total	60	68	177	142	217	288	420	966	1791	2876	4356	11361	55	60	192	154	154	178	288	779	1184	1522	2098	6684

Source: Indian Bureau of Crimes Record.

(Table – 2)

Cases Registered From 2003 to 2013

Person Arrested From 2003 to 2013



- Datenreihen1 Datenreihen2 Datenreihen3 Datenreihen4
- Datenreihen5 Datenreihen6 Datenreihen7 Datenreihen8
- Datenreihen9 Datenreihen10 Datenreihen11

**CYBER CRIMES/CASES REGISTERED AND PERSONS ARRESTED UNDER IT INDIAN PENAL CODE 1860
DURING 2003 TO 2013**

Crimes	Cases Registered From 2003 to 2013											Total	Person Arrested From 2003 to 2013											Total
	03	04	05	06	07	08	09	10	11	12	13		03	04	05	06	07	08	09	10	11	12	13	
Offences by/Against Public Servant	0	0	0	0	0	0	0	2	7	2	1	12	0	0	0	0	0	0	0	3	3	4	2	12
False electronic evidence	0	0	0	0	0	1	0	3	1	4	6	15	0	0	0	0	0	0	0	4	1	2	7	14
Destruction of electronic evidence	0	0	0	0	0	0	3	1	9	9	6	28	0	0	0	0	0	0	0	0	10	16	4	30
Forgery	89	77	48	160	217	55	158	188	259	259	747	2257	102	81	71	194	264	61	161	257	277	263	626	2357
Criminal Breach of Trust/Fraud	269	173	186	90	73	79	90	146	118	282	518	2024	255	181	215	121	85	96	79	100	129	215	471	1947
Counterfeiting-Property/mark	4	12	0	13	8	17	1	1	6	21	10	93	10	8	0	7	23	20	3	2	8	13	34	128
Counterfeiting-Tampering	8	7	9	0	5	3	3	8	5	19	8	75	33	16	0	0	8	0	0	12	7	26	10	112
Counterfeiting-Currency/Stamps	41	10	59	48	36	21	21	7	17	5	41	306	75	43	82	89	49	18	20	16	11	10	49	462
Total	411	279	302	311	339	176	276	356	422	601	1337	4810	475	329	368	411	429	195	263	394	446	549	1203	5062

Source: Indian Crime Bureau of Records.

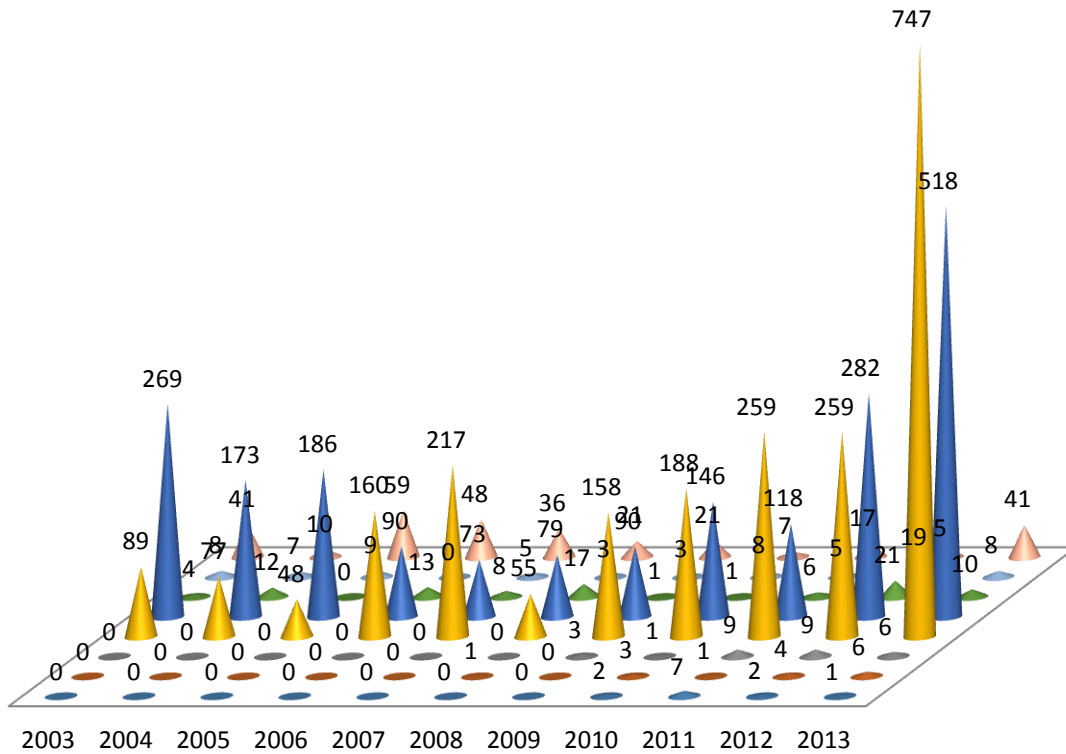
(Table – 3)

It is evident from the above table that a total number 1,337 cases were registered under various sections of IPC during the Year 2013. It was 601 in 2012 and it raised to 1337 2013. Compared to crimes during 2013 to 2012 there is 122.5% increasing. A total of 1,203 persons were arrested in the country for cybercrimes under IPC during 2013. 52.0% (626 persons) of these offenders were arrested for offences under ‘cyber forgery’, 39.2%(471 persons) for criminal breach of trust/fraud during 2013.Incidence of cybercrimes (IT Act + IPC sections) has increased by 63.7% in2013 as compared to 2012 (from 3,477 cases in 2012 to 5873 cases in 2013).

Cyber Forgery accounted for 55.9%(747 out of total 1,337 IPC cases) and cyber fraud accounted for 38.7% (518 out of 1,337 IPC cases) were the major cases reported under IPC category for cybercrimes.

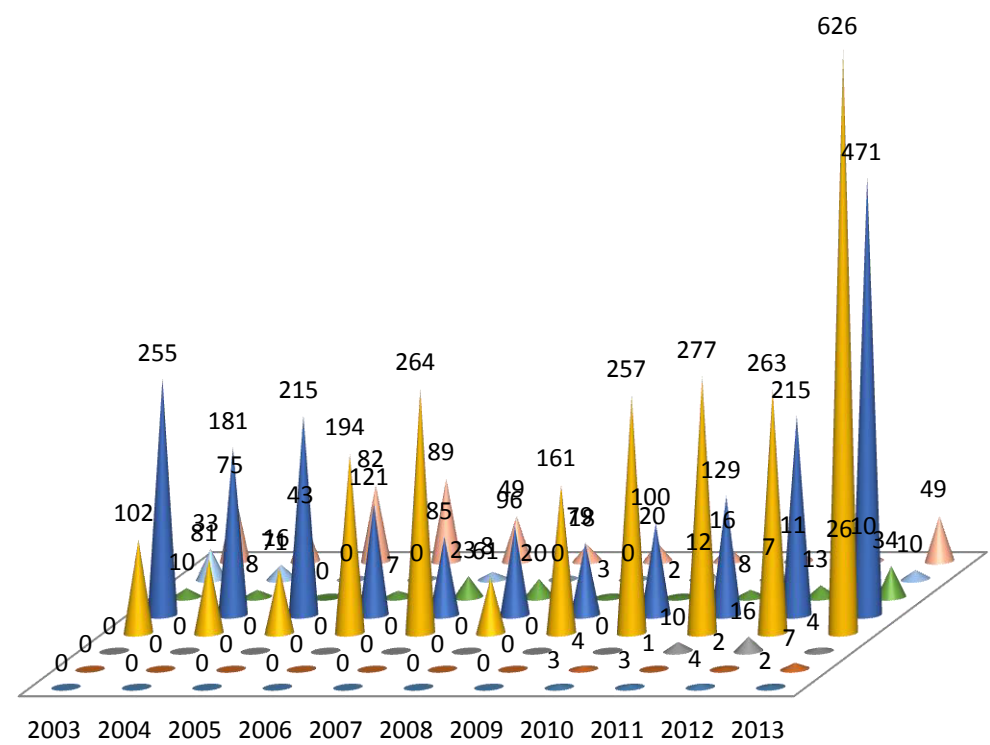
Cases Registered From 2003 to 2013

- Offences by/Against Public Servant
- False electronic evidence
- Destruction of electronic evidence
- Forgery
- Criminal Breach of Trust/Fraud
- Counterfeiting- Property/mark
- Counterfeiting- Tampering
- Counterfeiting- Currency/Stamps



Person Arrested From 2003 to 2013

- Offences by/Against Public Servant
- False electronic evidence
- Destruction of electronic evidence
- Forgery
- Criminal Breach of Trust/Fraud
- Counterfeiting- Property/mark
- Counterfeiting- Tampering
- Counterfeiting- Currency/Stamps



It is also reported that,¹³ 56.7% of the offenders under IT Act were in the age group 18-30 years (1,190 out of 2,098 persons) and 50.1% of the offenders under IPC Sections were in the age group 30-45 years (603 out of 1,203 persons). During 2013, 21.8% of cybercrimes were reported for fraud/ illegal gain (1,240 out of 5,693 cases) followed by eve-teasing/ sexual-harassment with 19.6% (1,116 cases) and greed/ money with 14.4% (821 cases).

VI. Conclusion

After careful observation of data on cybercrime, Researchers are of the view that the Cyber Crime is a new challenge before India. If we don't take it very seriously it is very difficult to survive in this digital millennium. Particularly in India, Indians are very fascinated towards purchasing computer, internet connection and computer related materials such as Desktop, Laptop, Advanced Mobile, Tab and Digital watch etc. Day by day new inventions in the field of computer technology has made the people to depend more and more on computer and mobile.

The main problem in controlling of cybercrimes is the lack of knowledge about rights and liabilities among the person who are using Computer and Internet. Majority of them are unaware of the laws on cyber space. It is needed that to educate the computer users well in advance before they are using computer or Internet. On the same it is required to give legal and technical training to the person who are already using computer and internet. In the same way it is required to train Indian law enforcement officials including the judicial officers. For effective enforcement of law.

Another problem in preventing Cybercrime is the lack of infrastructure and well equipped cyber police station. In India, Cyber police station are few in number. So there shall be at least 2 or 3 Cyber Crime Cells or police stations in a District for effective investigation of Cybercrime cases.

In India, there is only one forensic laboratory. (Hyderabad Forensic Laboratory) to prepare forensic report on Cybercrime cases. This is one of the impediment in providing speedy justice to the victims of cybercrimes. So in India there is a need for more well equipped forensic laboratory with technically trained personals in the laboratory.

Another problem in preventing the Cybercrime is the lack of international cooperation among world countries. The Cybercrime may be committed by the foreign

¹³ Crimes in India – 2013 Published by Indian Bureau of Crime.

nationals or citizen. If there is no cooperation or treaty or agreement between the countries it is very difficult to conduct investigation, collection of evidence, prosecute and enforce the Indian courts decisions. So it is needed that there shall be an International Cyber Cases enforcing agency which involves the multinational experts or investigative team and enforcement team. If these kind of agencies are established it is very easy to prevent trans-border Cybercrimes.

It is also necessary to have an International Cyber Code which is applicable to member countries of UNO or other international organizations working for world peace and security. If it is not possible, there can be a separate wing or department or branch in the international agencies for monitoring and enforcement of cyber code or laws on Information Technology.
