Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The Growing Phenomenon &Challenges of Cybercrime in India

Abhishek Srivastav, Irman Ali
M.S. in Cyber Law & Information Security
Indian Institute of Information Technology,
Allahabad, India

Abstract: Now a day's cybercrime in India is no longer an illusion. As technology increases the more people are connected and shared their information through internet. The chances of misusing their information also increases hence here comes a new name to a crime that is cybercrime. Cybercrimes have evaluated from development of computer network. Internet in the present millennium has become all pervasive and omnipresent. Cybercrime being global and a very big threat now a days for all over the world., generally affects the person far away from the place of offence , may it be in the same country or some other country.it therefore require policing at international level as also the active co-operation of the international community. In this paper we are focusing on challenges faced by people, police and government related to cybercrime in India.

Keywords: Cybercrime, challenges of cybercrime, cybercriminal, cyberspace, cyber law.

I. **Introduction**:

Information technology has offered wide scope and opportunities to human beings to identify, disseminate, evaluate and exchange information even to the remotest corner of the world and have become a valuable source development of communication, commerce, industries, environment and adventure. Cybercrime does not recognize national borders. More than 30 countries have separate laws in their statute books to check this menace.

Cyberspace: The word cyberspace was used for the first time by William Gibson in his Science fiction Neuron manicuring 1982. It may be defined as communication over the internet conducted by some kind of technology.it has no physical foundation which can be seen , touched, felt or sensed in the real world, but still one has to accept that translations in cyberspace do take place in the real world and do have real world effects.

Cybercrime: the offenses which take place on or using the medium of the internet are known as cyber crimes, these include a plethora of illegal activities. The term cybercrime is an umbrella term under which many illegal activities may be grouped together. The weapon with which cyber crimes are committed is a technology and therefore the preparations of these crimes are mostly technically skilled persons who have a thorough understanding of the internet and computer applications**.** Cybercrime can be divided into three categories.

- **Against person** : these crimes include various crimes such as harassing anyone with the use of computer that could be via e-mail. Cyber stalking and transmission of child pornography.

- **Against Property:** these crimes include, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information and unauthorized computer trespassing through cyberspace**.**

- **Against government :** a distinct kind of crime in this category is cyber terrorism. This crime manifests itself into terrorism when an individual or a group of people cracks into a government or military –maintained website.
  In our view, there are five main types of cyber attack, each with its own distinct – though sometimes overlapping – methods and objectives

  1. **Economic crime** – this involves criminals, often highly organized and well-funded, hacking into systems and using technology as a tool to commit fraud,

  2. **Espionage** – today, an organization's valuable intellectual property ('IP') includes electronic communications and files as well as traditional IP like research and development ('R&D'). IP theft is a persistent threat, and the victims might not even know it's happened – that is until counterfeit products suddenly appear on the market, or another company registers a patent based on their R&D,

3. **Activism** – the attacks are carried out by supporters of an idealistic cause, most recently the supporters of WikiLeaks,
4. **Terrorism** – terrorist groups might attack either state or private assets, often critical national infrastructure ('CNI') like power, telecoms and financial systems,
5. **Warfare** – this involves states attacking state or private sector organizations[3]

II. Scope of cybercrime:

cybercrime is an ever increasing phenomenon , not only in India but all over the world. The incidence of this crime is directly proportional to the level of progress made by a country in computer technology. Gabriel Weismann, an internet and security expert has studied militants use of websites for nearly a decade, while addressing the internet security personnel said that website and chat rooms used by militant Islamic groups like Al-Qaida are no only used for dissemination of propaganda , but also for terrorist education. He said Al –Qaida has launched a practical website that shows how to use weapons , how to carry out kidnapping and how to use fertilizers to make a bomb. The terrorist attack on India's parliament on December 13, 2001, is yet another glaring instance how computer networks are being misused for destructive activities by the anti-nationals. The computer related crime has already become an area of serious concern for most of the countries of the world and is India no exception to it.the prime factor that has to be taken into consideration while deciding whether a particular computer related activity be reckoned as cybercrime is that a distinction must be drawn between what is unethical and what is illegal.it is when an activity is truly illegal, it should be treated as crime and the prosecution of the offender must be sought. Therefore, criminal law should be implemented with resistant in determination of cases which relate to cyber law.

Cybercriminal :the emerging information and communication technology inevitably has an immense impact on the life of the people in modern time, but the advantages and benefits of global connectivity have brought with them certain dangers emanating from inter connectivity of information networks which provide scope for cyber criminals to carry on their criminal activities in cyberspace. Cybercriminals indulge in criminal activities like electronic fraud, unauthorized access to computer systems , software piracy, cyber stalking, child pornography etc. using their knowledge and skill in computer technology.

Need For Cyber Law : the information technology advanced but computer network undoubtedly pervades every aspect of society and governance in the present new millennium with the increased dependence of e-commerce and e-governance , a wide variety of legal issues related to use of internet as well as other forms of computer or digital processing devices such as violation of intellectual property , piracy, freedom of expression, jurisdiction etc, have emerged which need to be tackled through the instrumentality of law. Since cyber space has no geographical limitations or boundaries nor does it have any physical characteristics such as sex, age etc. it poses a big challenge before the law enforcement agencies for regulating cyberspace transactions of citizen within a country's territorial jurisdiction. Though in practical terms , an internet user is subject to the laws of the state within which he/she goes online but this general rules into conflict where the dispute are international in nature. It is true that time when computer technology was at its developing stage, no one ever contemplated that it can be indiscreetly misused by the internet users for criminal purposes. Because of the anonymity of its character and least possibility of being detected, the cyber criminals are misusing the computer for a variety of crimes which calls for the need for an effective legal framework and regulatory measures to prevent the incidence of this particular type of criminality which is rampant in cyberspace.

INFORMATION TECHNOLGY ACT 2000 :

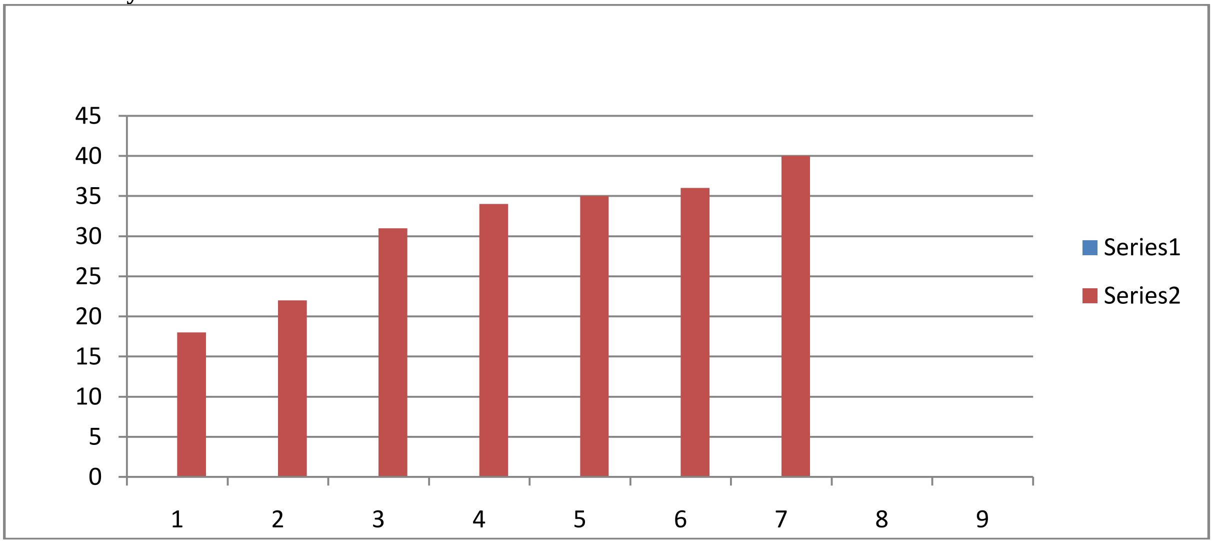
the traditional laws such as Indian penal code , 1860 Evidence act 1872, bankers book Evidence act, Reserve Bank Of India act , Companies act etc where relevant to the socio-economic and cultural scenario existing prior to the advent of information technology and its development through cyberspace and internet. But these laws were found insufficient to cater to the needs of new crimes emerging from internet expansion. Notably some of the international crimes like conspiracy , solicitation , securities, fraud, espionage etc are now being committed via internet which requires a new law to regulate these offences. It was in this background that information technology Act 2000 , was enacted in India primarily for Facilitating e-commerce and prevention of illegal and unlawful activities through computer networks and internet.

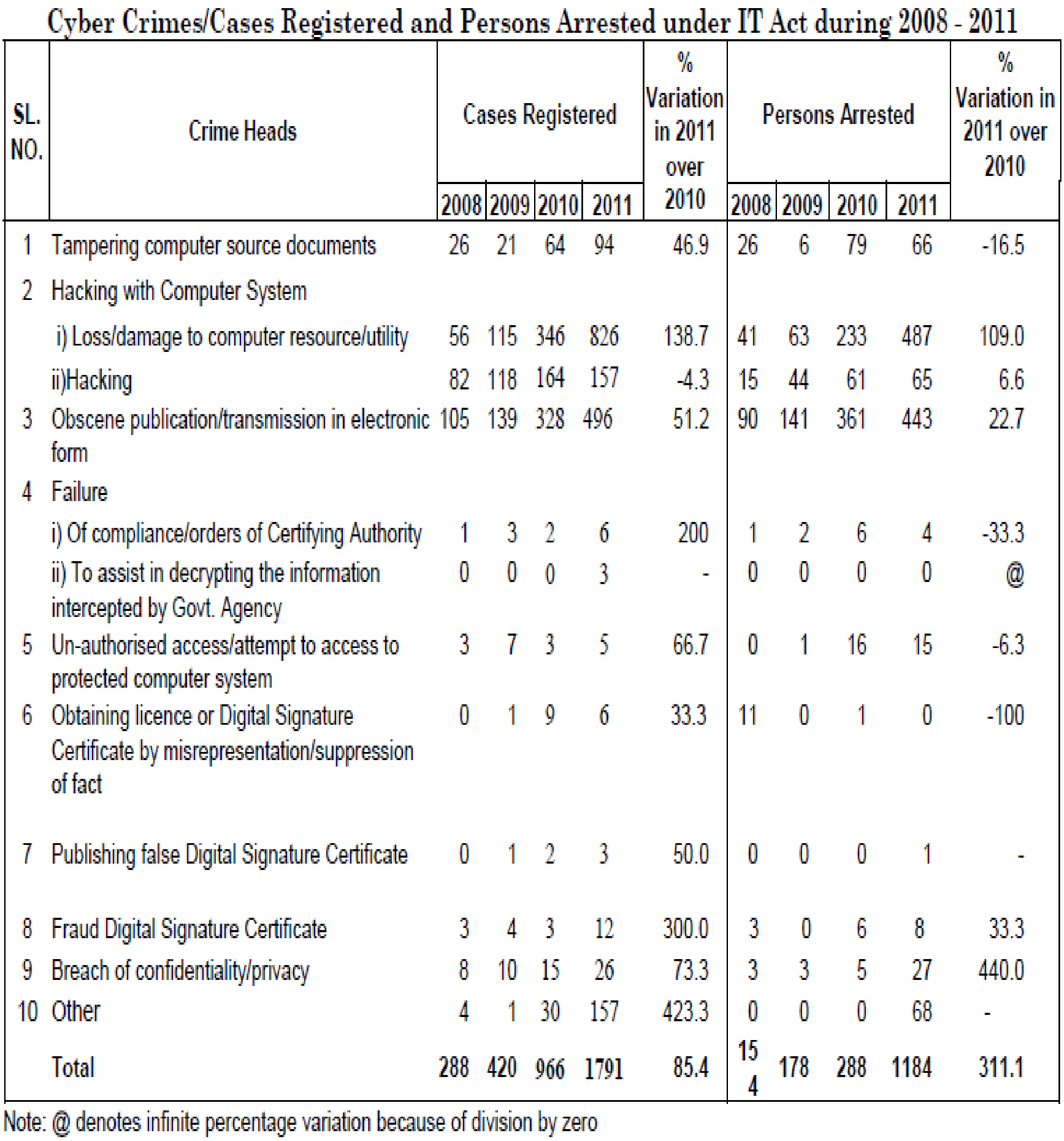
III. Challenges faced by Governments :

Although governments are actively focused on fighting and preventing cyber criminals from damaging infrastructure, the very nature of cyberspace poses a number of challenges to the implementation of cyber regulations in any country. Within cyberspace it is often difficult to determine political borders and culprits. Furthermore, the cyber criminal community and their techniques are continuously evolving, making it more challenging for governments and companies to keep up with ever-changing techniques.

- Tracking the origin of crime
- Growth of the underground cyber crime economy
- Shortage of skilled cyber crime fighters
- Widespread use of pirated software

Statistics of Cybercrime in INDIA:





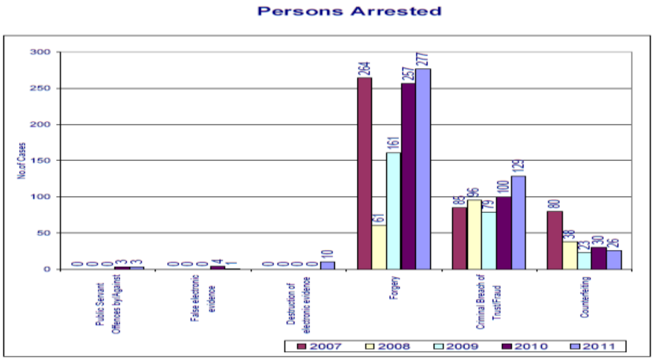
Cyber Crimes/Cases Registered and Persons Arrested under IT Act during 2008 - 2011

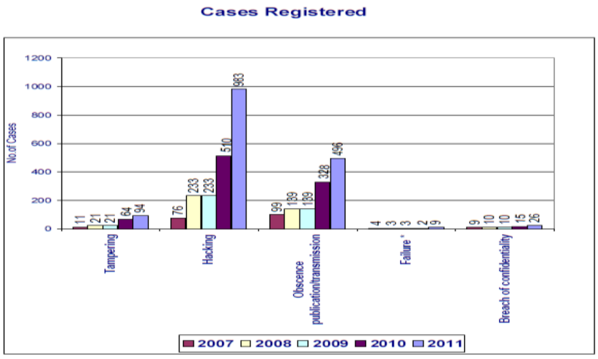
SL. NO.	Crime Heads	Cases Registered				% Variation in 2011 over 2010	Persons Arrested				% Variation in 2011 over 2010
		2008	2009	2010	2011		2008	2009	2010	2011	
1	Tampering computer source documents	26	21	64	94	46.9	26	6	79	66	-16.5
2	Hacking with Computer System										
	i) Loss/damage to computer resource/utility	56	115	346	826	138.7	41	63	233	487	109.0
	ii)Hacking	82	118	164	157	-4.3	15	44	61	65	6.6
3	Obscene publication/transmission in electronic form	105	139	328	496	51.2	90	141	361	443	22.7
4	Failure										
	i) Of compliance/orders of Certifying Authority	1	3	2	6	200	1	2	6	4	-33.3
	ii) To assist in decrypting the information intercepted by Govt. Agency	0	0	0	3	-	0	0	0	0	@
5	Un-authorised access/attempt to access to protected computer system	3	7	3	5	66.7	0	1	16	15	-6.3
6	Obtaining licence or Digital Signature Certificate by misrepresentation/suppression of fact	0	1	9	6	33.3	11	0	1	0	-100
7	Publishing false Digital Signature Certificate	0	1	2	3	50.0	0	0	0	1	-
8	Fraud Digital Signature Certificate	3	4	3	12	300.0	3	0	6	8	33.3
9	Breach of confidentiality/privacy	8	10	15	26	73.3	3	3	5	27	440.0
10	Other	4	1	30	157	423.3	0	0	0	68	-
	Total	288	420	966	1791	85.4	154	178	288	1184	311.1

Note: @ denotes infinite percentage variation because of division by zero

Person Arrested under IT ACT during 2007-2011:

Cyber crime/Cases Registerd under IT ACT during 2007-2011:





IV. Conclusion :

Cybercrime means any criminal activity in which computer or network is the source , tool or target or place of crime. Cybercrime comes in many forms, but most of these crimes deal with stolen information. The most common type of cybercrime include identity theft , phishing , scams and fraud.it is crime committed with the use of computer or relating to computers, especially through internet. Crime involves use of information or usage of electronic means. It can be classified in to four major categories. Cybercrime against person , cyber crime against government , cyber crime against property, cyber crime against organization. Advances in technology are fast-paced,

as are fraudsters, however organizations are often far behind. It is now essential to ensure that cyber and information security issues have the standing they warrant on an organization's risk register. Those organizations ready to understand and embrace the risks and opportunities of the cyber world, will be the ones to gain competitive advantage in today's technology driven environment. Establishing the right "tone at the top" is key in the fight against economic crime. It's time for everyone to rise to the challenge .

References:

1. http://shodhganga.inflibnet.ac.in/bitstream/10603/7829/12/12_chapter%203.pdf, data accessed, jan 26 2014.
2. http://www.pwc.in/assets/pdfs/publications-2011/economic-crime-survey-2011-india-report.pdf data accessed, jan 26, 2014.
3. http://www.slideshare.net/PWC/gecs-global-report data accessed , data accessed jan 26, 2014.