International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

Virtual Crimes and Human Disasters Facet of It Revolution in Indian Perspective

K.Srivani
B.Com, LLB,MBA (Fin,Hr), Mphil (Phd)
Associate Professor
St.Josephs Degree &PG College King Kothi Hyd.
Research scholar at Osmania university
Department of Business Management

ABSTARCT

This article is about alarming rise in cybercrimes in recent years ,Impact of information technology on crime and human disasters .Explosion of IT is creating many opportunities and developments in many fields which is catalyzing the growth of human kind to reach new heights of livelihood, comfort levels, earning opportunities bringing smile on many faces. The other side of this reality is it has also encouraged an avenue for crime which is easy, sophisticated and psychopathic. This article focuses on security issues of Internet and its new dimensions of criminal offenses resulting in tampering the privacy of many individuals. This paper has 2 parts first part deals with cyber crimes descriptions and its dimensions. Second part consists of regulatory frame work in India and latest up gradations to meet the changing virtual crimes.

Keywords:

Information Technology Act 2000& the Information Technology Amendment Act 2008,Massive Multiplayer Online Game (MMOG), Psychological warfare, Anti cybercrime groups, United Nations Commission on International Trade Law (UNCITRAL).

Introduction

Crime is both a social and economic phenomenon. It is as old as human society. Many ancient books right from pre-historic days, and mythological stories have spoken about crimes Committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc. Kautilya’s Arthashastra written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it.Akber Birbal stories move around the crimes, cheatings and judgmental tactics to protect the interest of people in administration of state.

Objectives of the study

- To understand the concept of cybercrimes and human disasters resulting from it
- To study about the statistics of growing cybercrimes in India since past 3 years
- To know about the regulatory framework in India
- To understand the concerns of cybercrime Investigations
- To identify the scope of further improvement in cyberlaws

Crime in any form adversely affects all the members of the society. In developing economies, cyber crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitalisation of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile. Snatching some one’s mobile will tantamount to dumping one in solitary confinement!

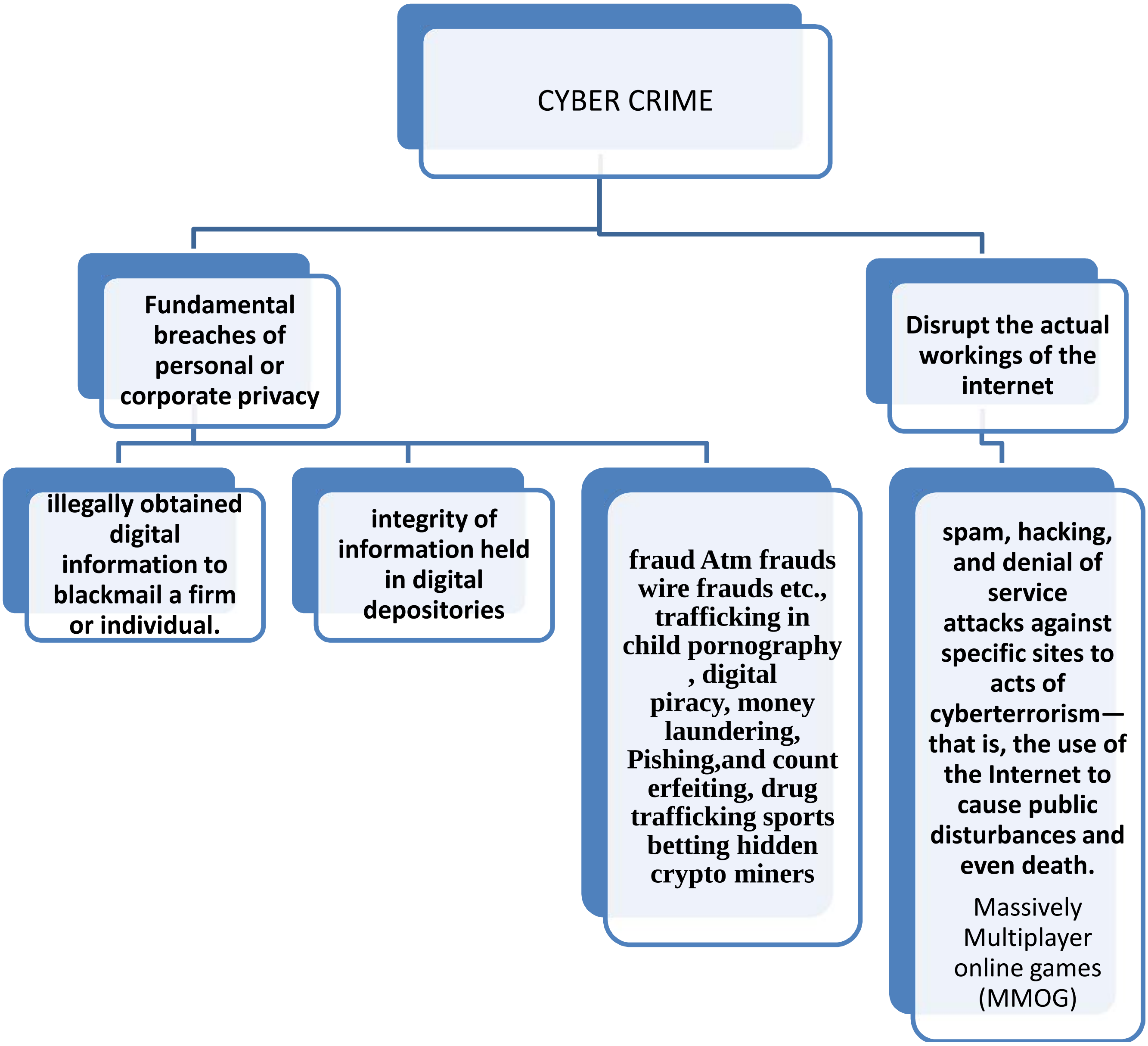
Cyber Crime is not defined in Information Technology Act 2000 nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber crime, we can say, it is just a combination of crime and computer. **To put it in simple terms ‘any offence or crime in which a computer is used is a cyber crime’**. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber crime.

In a cyber crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come

under the broader definition of cyber crime.crime is defined as an action that causes unjustified harm, and must be prosecuted and punished by a legal authority .a crime that happened in a virtual world can cause harm in the real world is not an issue that can be instantly solved. Following the same definition, a crime in a virtual world would be able to cause real psychological harm often amounting to a trauma given the remarkably realistic nature of the virtual environment. Although today’s virtual worlds give the impression that they are not real, in the future virtual worlds are likely to become more immersive, contributing to the sense that the victim was exposed to a real harm. But when it comes to gauging the amount of harm inflicted by a virtual crime, the issue would become much more complicated because of arguments considering different degrees of reality.

Although virtual crimes are happening now and are likely to become a serious issue in the future, discussions about virtual crimes are largely speculative since the first “real” virtual reality headset came out only a recent origin There are still multiple nontrivial technological hurdles to overcome to deliver a perfectly immersive virtual experience. But we would need to begin discussing ways to regulate criminal activities in virtual environments before criminals could act without restraint in a different world causing realistic harm to everyone else

TYPES OF CYBER-CRIME


CYBER CRIME
Fundamental breaches of personal or corporate privacy
Disrupt the actual workings of the internet
illegally obtained digital information to blackmail a firm or individual.
integrity of information held in digital depositories
fraud Atm frauds wire frauds etc., trafficking in child pornography , digital piracy, money laundering, Pishing,and count erfeiting, drug trafficking sports betting hidden crypto miners
spam, hacking, and denial of service attacks against specific sites to acts of cyberterrorism—that is, the use of the Internet to cause public disturbances and even death.
Massively Multiplayer online games (MMOG)

FACTS & FACETS

Cyber terrorism focuses upon the use of the Internet by nonstate actors to affect a nation's economic and technological infrastructure. Since the September 11 attacks of 2001, public awareness of the threat of cyber terrorism has grown dramatically.

The Blue Whale suicide game is believed to be a social media group which is encouraging people to kill themselves .The horrific tasks include self-harming, watching horror movies and waking up at unusual hours, but these gradually get more extreme. On the 50th day, the controlling manipulators behind the game reportedly instruct the youngsters to commit suicide

STATISTICS OF CYBER CRIME IN RECENT YEARS IN INDIA ---PTI SOURCES

The government told the Rajya Sabha last week that cyber crimes cases in the country have grown in the last three years, with the number rising from 9,622 and 11,592 to 12,317 during 2014, 2015 and 2016 respectively.

Minister of electronics and information technology Ravi Shankar Prasad told the Upper House that according to CERT-In, 79 phishing incidents affecting 22 financial organisations, 13 incidents affecting ATMs, Point of Sales (POS) systems and Unified Payments Interface (UPI) were reported.

The Reserve Bank of India has registered 13,083, 16,468, 13,653 and 12,520 cases of frauds involving credit cards in 2014-15, 2015-16, 2016-17 and between April-September 2017 respectively, he added.

Prime Minister Narendra Modi and National Security Adviser Ajit Doval are also taking part in the conference that is being attended by officers of DGP and IGP rank from all the states and central police organisations.

Union home minister Rajnath Singh has told heads of state police that the rising rate of cybercrime in India is among the latest challenge for law enforcement agencies and both state and central authorities in India must be prepared to deal with the issue effectively.Singh made the comments during the three-day conference of the country’s top police officials at the Border Security Force (BSF) Academy in Madhya Pradesh’s Tekanpur.

Singh cited the data by the Indian Computer Emergency Response Team (CERT-In), which says there cybercrime has increased by 21% every year, during his speech at the Annual Conference of Director Generals of Police (DGPs) and Inspector Generals of Police (IGPs).

.REGULATORY FRAME WORK OF CYBER CRIME IN INDIA

The Genesis of IT legislation in India: Mid 90’s saw an impetus in globalization and computerisation,with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records ie the data what is stored in a computer or an external storage attached thereto.

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

It is against this background the Government of India enacted its Information Technology Act 2000.The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000.

The Act essentially deals with the following issues:

_ Legal Recognition of Electronic Documents

_ Legal Recognition of Digital Signatures

_ Offenses and Contraventions

_ Justice Dispensation Systems for cyber crimes.

The need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003-04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations, **the Information Technology Amendment Act 2008** was made effective from 27 October 2009.

Some of the notable features of the ITAA are as follows:

_ Focusing on data privacy

_ Focusing on Information Security

_ Defining cyber café

_ Making digital signature technology neutral
_ Defining reasonable security practices to be followed by corporate
_ Redefining the role of intermediaries
_ Recognising the role of Indian Computer Emergency Response Team
_ Inclusion of some additional cyber crimes like child pornography and cyber terrorism
_ authorizing an Inspector to investigate cyber offences (as against the DSP earlier),

Applicability: The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person.

Other Acts amended by the ITA

- The Indian Penal Code, 1860
- The Indian Evidence Act 1872
- The Bankers' Books Evidence(BBE) Act 1891
- The Reserve Bank of India Act, 1934.
- Prevention of Money Laundering Act:

Observations And Issues in ITA & ITAA

Some of the broader areas of omissions and commissions in the Act and the general criticism the Acts have faced over the years.

Awareness: There is no serious provision for creating awareness and putting such initiatives in place in the Act. which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large.

Jurisdiction: This is a major issue which is not satisfactorily addressed in the ITA or ITAA.

Some fundamental issues like if the mail of someone is hacked and the accused is a resident of a city in some state coming to know of it in a different city, which police station does he go to? If he is an employee of a Multi National Company with branches throughout the world and in many metros in India and is often on tour in India and he suspects another individual say an employee of the same firm in his branch or headquarters office and informs the police that evidence could lie in the suspect's computer system itself, where does he go to file he complaint. Often, the investigators do not accept such complaints on the grounds of jurisdiction and there are occasions that the judicial officers too have hesitated to deal with such cases. The knowledge that cyber crime is geography-agnostic, borderless, territory-free and sans all jurisdiction and frontiers and happens in 'cloud' or the 'space', has to be spread and proper training is to be given to all concerned players in the field.

Evidences: Evidences are a major concern in cyber crimes. Pat of evidences is the 'crime scene' issues.. We cannot mark a place nor a computer nor a network,nor seize the hard-disk immediately and keep it under lock and key keep it as an exhibit taken from the crime scene.

Non coverage of many crimes:

Many cyber crimes like cyber squatting with an evil attention to extort money. Spam mails, ISP's liability in copyright infringement, data privacy issues have not been given adequate coverage.

Soft On Cyber Criminals

To quote the noted cyber law expert in the nation and Supreme Court advocate Shri Pavan Duggal, "While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyberlaw and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyberlaw a cyber crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart;

Conclusion

In order to curb computer crimes, the police alone cannot make all the difference. Awareness regarding these cyber laws must be created. Private and Non Government organizations must play an active role in communicating this message to the masses. Moreover, the judiciary will also have to play a proactive role in adjudicating cyber trials. A large part of the judiciary is probably unaware of cyber laws and their implications. They must themselves study the laws carefully and effectively enforce them. Co-ordination amongst the organizations, police and judiciary will definitely create some impact and minimize the crime rate. However, the working and implementation of this law will depend greatly on the rules and regulations that will be formed by the the Government and other authorities constituted under the Act.

References:

1)"IT" Security of IIBF Published by M/s TaxMann Publishers

2) A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom By divijoshi *http://books.sipri.org/files/books/SIPRI04BaiFro/SIPRI04BaiFro17.pdf* 2*http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities studies/pdfs/CIIP-HB-2006-2-27-53.pdf*

3) Report: Expect more website ads to contain hidden cryptominers By Bradley Barth January 04, 2018 .

4) Cyber Crime And Law - Indian PerspectiveWritten by: Author 1: Akanksha Malhotra, (5th year); B.A, LL.B (Hons.)Afilliation: NALSAR, University of Law,Hyberabad. Author 2: Akshay Kumar, 4th year, B.A, LL.BAffiliation: Jamia Millia University, New Delhi.

5) New adware found in fake flashlight apps with dark intentions. By bradley barth january 05, 2018 Lawmaker seeks police-social media tie-up vs terrorism August 22, 2017 BY: Pathricia Ann V. Roxas Security and privacy in the internet of things,Carsten Maple. Pages 155-184 | Received 20 Apr 2017, Accepted 08 Jul 2017, Published online: 24 Aug 2017

6) Lawmaker seeks police-social media tie-up vs terrorism August 22, 2017 BY: Pathricia Ann V. Roxas

7) 7 fall in cybersex den raid in Gingoog City.July 12, 2017 BY: Jigger J. Jerusalem

8) PNP anti-cybercrime group sees rise in internet offenses.June 28, 2017 BY: Jeannette I. Andrade.