Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 9, June-2019, ISSN 2230-7540

A Study of Cyber-Crime and Cyber Terrorism in India

Pardeep Malik[1]* Keshav Vimal[2]

[1] Research Scholar

[2] Supervisor

Abstract – Crimes committed on or utilizing the Internet media are known as cyber-crimes. These include an abundance of illicit activity. The word cyber-crime is an umbrella term for the grouping of various unlawful actions. The anonymous nature of the internet allows offenders to engage in many kinds of illegal acts termed cyber-crimes due to numerous unpleasant behaviors taking place in the cyber-space and the study which discussed about, cyber-crime, Cyber-crime perpetrators, Cyber-crime in the world, Different types of cyber-crimes, Cyber-crime and cyber law, Common cyber-crimes, Nature of cyber-crime acts, Application of the cyber-crimes theory, Cyber law in India.

Keyword – Cyber-Crime, Terrorism

----------X----------

INTRODUCTION

Nature has given human beings the strength, the intellect and the brain that differentiates between them and other living things of the world, and makes man superior. Eventually, the development of human civilization led to the discovery and creation of concepts that rose from the necessity to survive to contemporary luxury. Computer and Internet technology legislation is cyber law. Nothing has to be said about the significant transformation of our life styles with modern communication systems and digital technologies. Nearly everyone is impacted in today's increasingly digitalized society. In the way individuals transact, a transformation is seen. Almost every stock transaction is demitting. Virtually all businesses rely heavily on their computer networks to preserve their data in electronic form. For communications most individuals use emails, mobile phones and SMS messaging. Instead of conventional documents, businesses and consumers increasingly use the computer to generate and record information in electronic form. The traditional way of conducting business is replaced by digital signatures and e-contracts. The industry saw a quantum shift in quality, quantity and speed as the computer era approached. The manner of living is modernized. The technology, however, continues to grow and develop. It is the human intellect that creates a drive to know and to understand inside humans which culminates in the development of contemporary science and technology.

Science as a field of knowledge consists of an observation, identification, description, experimentation and methodical examination of natural phenomena and a reasoning impetus for finding truth above and beyond common conceptions. It certainly gave human capacities new dimensions. The evolution of human civilization has had a significant role in science and technology. The use of science or know-how or any means of achieving or applying such know-how to any specific job by utilizing a technological procedure may be described exactly as technology. It is thus human invention in action which includes knowledge creation to expand human capacities or meet the human needs and desires that emerge. It is thus obvious that technology results in changes in the natural environment by applying knowledge scientifically to the material convenience of people. As a result, the globe has uniformly benefitted from the growth of science and technology via all living conveniences. Science has a great deal of effect on human activities in today's world, directly or indirectly. Science and technology progress is basically the result of the creation of radio, telephone, television, supercomputers etc. and all other technical processes. Today, we live in a computer era, which is a major part of our daily lives.

In many areas from cars to household appliances computers and the Internet still permeate human existence. The advent of computers, their growing use and their human dependence on the Internet

have brought numerous bad consequences and drawbacks to mind, although we've gained a great deal from efficiency and administration. Individuals or organizations may now use cyberspace to intimidate or harass nationals of international governments. When a person "cracks" on a government or militarized website, the crime of "cracking" may develop into fear. Cyber terrorism may become a computer system at the hospital and change someone's prescription of medicine into a fatal dose for a vengeance

Activities which are criminal are set out in the Information Technology (IT) Act, 2000. Given that the main purpose of this Act is to establish a commercially useful environment, some omissions and commissions by criminals were not included when utilizing computers. Various cyber-related crimes are also registered, with legal recognition of the Electronic Records and modifications made in several IPC video Act 2000 parts under the relevant sections of the IPC

CYBER CRIME

Crimes committed on or utilizing the Internet media are known as cybercrimes. These include an abundance of illicit activity. The word cybercrime is an umbrella term for the grouping of various unlawful actions. The anonymous nature of the internet allows offenders to engage in many kinds of illegal acts termed cybercrimes due to numerous unpleasant behaviors taking place in the cyber-space.

Technology is the weapon with which cybercrimes are conducted and therefore, mainly competent technicians who have a comprehensive knowledge of the internet and computer applications are involved. Cyber crime, cyber terrorist attacks, email spoophing, bombing, cyber pornography, cyber defamation, polymorphic virus, worms, etc. are some of the most recent cyber crimes that occur. Certain traditional crimes may also constitute cybercrimes if performed on or via the Internet. The examples here include robbery, malice, trickery, fraud, deception, pornography, bullied acts, threats, etc.

As for the accurate definition of cybercrime, no legislation or law has yet defined it. There is no definition of cybercrime, including in the Information Technology Act, 2000. Nevertheless, cybercrimes may be considered to be exactly those criminal species, in which computers are either an object or a topic of behaviour that constitutes or may be both. Any action that uses computers as a tool, goal or method to commit further crimes is thus part of cybercrime.

The above definition of cybercrime clearly shows that the divide between traditional crime and cybercrime is extremely narrow. The prerequisite for cybercrime is that a virtual cyber medium, i.e. a computer, should be involved at all stages. A basic but robust definition of cybercrime is 'illegal actions in which the computer is either an instrument or a goal, or both.' Cybercrimes are crimes against a computer, a computer system or a network of computers.

CYBER-CRIME PERPETRATORS

Due to the emergence and easy availability of malware toolkits, cybercrime offenders no longer need sophisticated skills and methods. It is believed that up to 80 percent of cybercrime is based on some organized activity, with black cybercrime marketplaces being built up via malware generation, computer infection, botnets administration, personal and financial data collection, data selling, and financial information cashing. Often a high degree of structure is required in cybercrime, which may leverage its resources to tiny criminal gangs, loose ad hoc networks or bigger organized crime (United Nations Office on Drugs and Crime, 2013). The typology of criminals and active criminal organizations reflects mostly trends in the conventional world. In the context of developing countries in particular, there have been subculture groups of young males involved in computer-related financial fraud who, in their late teenage years, often begin to participate in cybercrime. In the fact that young men are the majority, their demographic composition reflects traditional crime, but the age profile increasingly reflects older (male) persons, especially those involved with child pornography. Although some criminals, particularly in the area of computer technology, have gone through advanced training, many recognized offenders don't have any specific training. There is a dearth of comprehensive investigation of the nature of organizing crime operating in cyberspace, and more study on the linkages between child pornography offenders online and off-line. There are numerous aspects to the complete representation of a cybercrime offender. The main factors are probably age, sex, socio-economic background, country and motivation. Moreover, the degree to which people behave with others constitutes a defining characteristic of the aspect of human connection underlying criminal behaviour. Understanding the usage of cybercrime as a “social-techanism” phenomenon is a more general approach to prevention than the understanding of the characteristics of those who perpetrate such crimes.

CYBER-CRIME IN THE WORLD

The list of cyber assaults' most hazardous nations is based on 2012 statistics. "When it comes to cyber attacks Chinese and U.S. may dominate the news, but poor world nations are more susceptible to internet attacks... Cyber thieves are likely to resort to fewer defenses when they target consumers. Markets are being developed, with millions of additional Internet users and less

security resources every year," the agency said. The US has also been featured on the list, however, with 45% of those who suffered cyber assaults last year in 19th position. About 78 percent of the population of the U.S. was online last year or an estimated 245 million individuals. In Russia, 59% of internet users were attacked online last year, the most dangerous scenario in cyber attacks. Last year only approximately 48% (68 million people) of Russia's population were online.

DIFFERENT TYPES OF CYBER-CRIMES

We may classify different cyber crimes in different ways. We may split them into two extremely large groups: one, violent or possibly violent crimes and two non-violent. Cyber-terrorism; threatening assault; cyber-stalking and child pornography constitute serious or possibly violent cyber-crime, Three major offending patterns are part of cybercrimes. The offending may concentrate either on the integrity of the system or on the computer, or the content of the computer itself may be the target of the offence.

Child exploitation: In 2005, The Virtual Global Task Force described child sex abuse online as the sharing and download of pictures of children who are mistreated physically and sexually and contact children online to establish a 'real-world' sexual connection. The exploitation of children is by no means a creation of the Internet era. However, for consumers of child pornography and for those who supply them, the Internet has become the new playground.

Harassment: This is usually employed in order to harass another individual via the Internet, e-mails and other electronic communication instruments.

Digital Piracy: The development of the personal computer has led to a widespread usage of the Internet, allowing information sharing and crime-including behaviour. Digital piracy is one kind of crime on the Internet. Gunter, Higgins and Gealt (2010) described digital piracy, for any purpose other than to save the copyright holder without express consent or remuneration using computer technology, as an act of copying digital products which includes software, documents and audio (including speech and music).

Hacking: Unauthorized access may occur both on home computers of people and at business. 'Hacking is one of the most important forms of unauthorized access. Hacking means illegal access to a computer system or to a network and unauthorized use of such access in certain cases.

Intention Damage: The communication networks of the company may be affected by zapping, destroying or deleting information and data, and this causes both the company and the consumer difficulties.

Spam: E-mail Spam may be one of the most common crime since virtually every user of e-mail certainly has at some point received at least a couple of unwanted commercial e-mails. Spam mail is defined as a mass e-mail distribution offering subscribers goods or services according Kunz and Patrick (2004).

CYBER-CRIME AND CYBER LAW

Cybercrime reflects our over dependence on the internet or cyber space. Computer crimes are criminal acts that make a computer a tool or target or both. Computer crimes are illegal behaviors. Crimes involving computers are prohibited. The first computer crime in the 1820s was documented. The enormous growth in e-commerce and online stock exchanges has led to a spectacular cybercrime epidemic. It constitutes a step towards the changing and improving dimensions of the criminal world in the legal field. The IT Act 2000 is the main legislation on rules and regulations in the cyber globe. The law primarily seeks to provide e-commerce legal legitimacy and make it simpler for the government to submit electronic registration. Computer law criminalizes numerous computer offences and imposes severe penalties (prison sentences of up to 10 years and compensation of up to 1 rupee).

COMMON CYBER-CRIMES

The different types of computer crimes are:

Unauthorized access and piracy: Unauthorized access implies any kind of access to the computer, computer system or computer network without authorization from any authority or responsibility. Hacking is unlawful entry into a computer and/or network system. Piracy is every act committed to entering a computer and/or network. To attack the target machine, hackers create or utilize computer ready for use applications. They want to demolish this devastation and to enjoy the thrill of it. Some hackers are jeopardizing personal monetary gains such as obtaining credit card data, transfer of money from bank accounts to their account, and withdrawal. The most particular websites for hackers are government websites.

Web hijacking implies a strong control over the website of another person; in this situation, the website owner loses control over his websites and their contents.

Pornography: Pornography implies that sexual activities are shown to generate sexual excitement. The term pornography also encompasses pornographic websites; computer-

generated pornographic periodicals and Internet pornography delivered via mobile telephones.

Child pornography: Pedophiles lure minors via pornography distributors and then attempt to meet them for sex or to capture nude pictures, including their sexual involvement. Pedophiles abuse minors sexually, use them as sexual items or take their pornographic pictures for sale on the internet.

Denial of Service attack: The attack causes the criminal to flood the bandwidth of the victim's network or to fill up his spam box which deprives him of the services he has the right to access or provide. Such an attack is planned with excessive traffic with view to block the network.

Virus attacks: Viruses are programmes that may infect copy and distribute other programmes to other programmes. Viruses usually influence computer data when they are modified or deleted. Trojan horse has something like a programme.

Software piracy: Software piracy refers to the unlawful copying or falsification and distribution of original programmes and goods to which the original should be referred. Crimes of this kind include infringement of copyright, trademark violations, computer source code robbery, patent offences etc.

Salami attacks: These kinds of assaults are utilized for financial crime commission. The reason for this is because the changes will be so small that they will be totally unknown in one instance. If a bank server staff sets a programme for an illustration, a little sum (for example 5 a month) is deducted from the customer's bank account. No account holder may detect the unauthorized debt, yet every month the bank worker will get a substantial sum.

Phishing: Phishing is an email sent to a person who false claims to be a genuine business established in order to disappoint the user in supplying sensitive information needed for ID theft.

Sale of illegal items: This area of cyber crime covers the sales of narcotics, firearms, wild animals etc. through posting information on websites and auction boards.

Online game: Millions of websites are available; all are on servers overseas that provide online gambling. In fact, many of these websites are considered to be fronts of money laundering. Online reported cases of healing transactions and money laundering

Email spoofing: Email representation refers to email from a source which seems to have been sent from a source. E-mail representation may also cause financial harm.

Cyber Defamation: If an individual poses a defamatory inquiry about someone on a website or sends e-mails with defamatory material to their acquaintances, this is known as cyber defamation.

Falsification: Invoices, postal and entry tags, brand papers, etc. are counterfeited using computers, printers and scanners. They are made using high-quality computers and scanners.

Theft of information in electronic format: This involves robbery on computer hard discs, portable media, etc.

Bombardment by email: Email Bombardment is about sending a lot of emails to the victim who block the email account of the victim (in the event of a person) or email server (in the case of a company or an email service provider).

Data distribution: This type of attack requires changing the raw data before it is processed by the computer and changing it after it has been processed.

Theft of time on the Internet: Internet time refers to the usage of Internet hours paid by another person by an unauthorized individual.

Theft of the computer system: The theft of a computer, certain computer components or a device linked to the computer constitutes this offence.

Physical damage to a computer system: The physical damage to computers or its devices is caused by this crime.

Violation of privacy and confidentiality: Data protection refers to the right of an individual to decide whether, how and how much his or her personal information is disclosed. Violation of privacy means that personal data may be used or illegal dissemination or disclosure.

Data distribution: Data deletion requires data to be modified before or during computer entry. Information changes on how a person entering data, the data must be entered by a virus that modifies the data, the database or the application programmer or any individual involved in the data stocking process. It also involves the automated exchange and restoration of financial information for a period before processing.

Investment fraud: Securities fraud is a misleading activity in stock or market commodities markets, also known as equity fraud and equity fraud, which leads investors to make purchasing and selling choices based on incorrect information, frequently in breach of the Securities Act. Securities fraud is a deceptive method in stock or commodities markets causing investors to

make buying or selling decisions on the basis of false information, often leading to the loss of equity fraud in breach of securities laws.

Cyber terrorism: The primary objectives were attacks on military installations, power plants, air traffic controllers, banks and networks for traffic management. Others, for example police, doctors, fire and rescue systems etc. For many reasons, cyber terrorism is an attractive alternative for contemporary terrorists

NATURE OF CYBER-CRIME ACTS

Cybercrime actions may be financially driven, computer content acts or computer systems' secrecy, integrity and accessibility. The proportional risk and danger between governments and enterprises may be different. In particular in nations with lower levels of development, individual cyber crime victims are considerably higher than 'conventional' crimes, emphasizing the need to enhance preventive measures in these countries. In Europe, private sector firms report victims of actions such as data violation due to Intrusion or Phishing at between 2 and 16 percent These activities, like as botnets, are deemed criminal instruments of choice worldwide. More than 1 million distinct IP addresses worked as command and control servers for caps worldwide in 2011. (United Nations Office on Drugs and Crime, 2013)

The Internet material the government removals includes pornography for children and hate speech, but also defamation and public criticism, which in certain instances raises issue about human rights legislation

APPLICATION OF THE CYBER-CRIMES THEORY

The Routine Activity Theory (RAT) is used for this research, based on child exploitation as one of cyber crimes. The idea centered on 'crime opportunities' for the environment. The action occurs essentially at a crossroads between a mobilized offender and an appropriate objective for victimization when a possible criminal opportunity emerges. At the end, this crime takes place in a location that does not have a competent custodian to safeguard the "appropriate target," which is regarded either a vulnerable person or uncontrolled property. Therefore, the potential failure to commit a crime would the lack of any of the three circumstantial conditions. As a consequence, the theory of routine action is regarded a macro theory for many kinds of crime in order to expound the process of criminal victimization rather than the particular motives of criminal behaviour. In the absence of a competent guardian, which might possibly prevent the offender from committing a crime, the idea says that a crime occurs if a motivated crime is in touch. Ngo and Paternoster (2011) said that the idea is that variances in criminal rates may be explained by the provision of appropriate goals and competent caregivers, but we recognize that the notion of the function of motivated criminals is somewhat agnostic.

Cyber Law in India

Before the IT Act372000 was passed, there was no independent and distinct cyber law in India, and all computer-based offences were prosecuted according to the conventional criminal law, i.e. the Indian Penal Code, 1860. However, computer-based information technology began to influence every area of society and government in the new century. Different legal issues related to computer usage and Internet or digital processing systems, such as infringement of IPRs, piracy, freedoms of expression, jurisdiction etc. arose as a result of increased dependence on the electronic trade and electronic governance, which cannot be addressed under current laws, since cyberspace has no geographical limitations or physical characteristics such as This raised real difficulties, both inside the nation and in the countries outside, before law enforcement authorities in controlling internet transactions. In practice, however, an internet user is subject to the laws of the State in which he/she works, but when the issues are international, this general norm conflicts.

CONCLUSION

Change is inevitable and cannot be avoided by the challenges posed by technological progress. In fact, the criminals have altered their tactics and begun using sophisticated technology and to cope with them they will also have to modify their mechanisms for combating society, law and enforcement agencies, private businesses and organizations. Such specialists must not only be informed, but must also have the technological equipment and software needs to combat cyber thieves effectively, Since computer system users and internet users grow globally every day. Within a few seconds you may readily obtain information utilizing the web that is the medium for big-scale information and a broad base of worldwide communications. Netizens should take some cautious steps when utilizing the Internet to challenge this important danger of cybercrime, Multilateral issues with many aspects and dimensions are at issue with cyber terrorism. It needs a rigorous use of energy and resources for its solution. Law is usually seven steps behind technology, The application of these rights demands a "qualitative effort" rather than a "quantitative effort." Therefore we must not be timid and reluctant to utilize existing laws before a law is explicitly established to deal with cyber terrorism.

REFERENCE

1. Animesh Sarmahand and Amlan Jyoti Baruah (2017), volume 04, issue 06, pp. 1633-1640.

2. Anuraj Singh (2007), volume 05, issue 06, pp. 11273- 11279.

3. Saurabh Mittal (2019) on “a study of cyber-crime and perpetration of cyber-crime in india” doi:10.4018/978-1-5225-8897-9.ch050 in book: cyber law, privacy, and security (pp.1080-1096.

4. Rupa CH, Thippa Reddy Gadekallu (2018) on “computational system to classify cyber-crime offenses using machine learning” sustainability 2018, 12, 4087; doi:10.3390/su12104087 www.mdpi.com/journal/sustainability.

5. J.a. Mshana (2017) on “cybercrime: an empirical study of its impact in the society- a case study of tanzania” institute of judicial administration lushoto, box 20 lushoto e-mail: jumamshana@gmail.com; jamshana@ija.ac.tz.

6. Mathiha Nehla Hani and Aaswathy Rajan (2018) on “a critical study on cyber terrorism with reference with 26/11 mumbai attack” international journal of pure and applied mathematics volume 119 no. 17 2018, 1617-1636 issn: 1314-3395 (on-line version) url: http://www.acadpubl.eu/hub/ special issue.

7. Vijay Raghavan (2015) on “the indian criminal justice system: voices from field”the indian police journal january - march, 2015 l vol. l, XII l no. 1.

8. Shivani Verma, Siddharth Nayak, Deepak Kumar Deshmukh (2018). A survey of emerging cyber-crimes and their probable solutions. Research j. Engineering and tech. 2018);11(2): pp. 82-88. DOI: 10.5958/2321-581x.2018.00015.x

9. Animesh Sarmah, Roshmi Sarmah (2017) on “a brief study on cyber-crime and cyber laws of India” international research journal of engineering and technology (IRJET) E-ISSN: 2395-0056 volume: 04 issue: 06 | June-2017 www.irjet.net P-ISSN: 2395-0072

Corresponding Author

Pardeep Malik*

Research Scholar