International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013
ISSN No.: 2250-0758
Pages: 13-18
www.ijemr.net

A Study on Cyber Crime and Security Scenario in INDIA

Yougal Joshi[1], Anand Singh[2]
[1]Information Scientist, Kumaun University, Nainital,Uttarakhand, INDIA.
[2]Assistant Professor, Department of IT, Institute of Management Studies, Dehradun, INDIA.

ABSTRACT

Cybercrime is evolving at an astounding pace, following the same dynamic as the inevitable penetration of computer technology and communication into all walks of life. Whilst society is inventing and evolving, at the same time, criminals are deploying a remarkable adaptability in order to derive the greatest benefit from it. To avoid giving cybercriminals the initiative, it is important for those involved in the fight against cybercrime to try to anticipate qualitative and quantitative changes in its underlying elements so that they can adjust their methods appropriately.

I. INTRODUCTION

"Cybercrime" combines the term "crime" with the root "cyber" from the word "cybernetic", from the Greek, "kubernân", which means to lead or govern. The "cyber" environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "computer crime" to encompass crimes committed using the Internet, all digital crimes, and crimes involving telecommunications networks. This more recent terminology covers a wide variety of facets, leading to different approaches, depending on the dominant culture of the experts, making it appear either reduced or expanded, in different dimensions, dealing with emerging issues that also reflect its diversity.

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment.” The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin “the criminal quality of an act cannot be discovered by reference to any standard but one: *is the* act prohibited with penal consequences”.

A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences. The expanding reach of computers and the internet has made it easier for people to keep in touch across long distances and collaborate for purposes related to business, education and culture among others. However, the means that enable the free flow of information across borders also give rise to a worryingly high incidence of irresponsible behavior. Any technology is capable of beneficial uses as well as misuse. It is the job of the legal system and regulatory agencies to keep pace with the same and ensure that newer technologies do not become tools of exploitation and harassment.

However, substantial legal questions have arisen in many contexts. The World Wide Web allows users to circulate content in the form of text, images, videos and sounds. Websites are created and updated for many useful purposes, but they can also be used to circulate offensive content such as pornography, hate speech and defamatory materials. In many cases, the intellectual property rights of authors and artists are violated through the unauthorized circulation of their works. There has also been an upsurge in instances of financial fraud and cheating in relation to commercial transactions conducted online.

The digital medium provides the convenient shield of anonymity and fake identities. Errant persons become more emboldened in their offensive behavior if they think that they will not face any consequences. In recent years, there have been numerous reports of internet users receiving unsolicited e-mails which often contains obscene language and amounts to harassment. Those who post personal information about themselves on job and marriage to websites or social networking websites are often at the receiving end of ‘cyber-stalking’. Women and minors who post their contact details become especially vulnerable since lumpen elements such as sex-offenders can use this information to target potential victims

II. ASPECTS OF CYBER CRIMES

2.1 Technological Aspect of Cybercrime

From a technological dimension, other experts point out the need for a comprehensive term, such as *"electronic crime"* or *"e-crime"*, thanks to the convergence of ICT, including mobile technology, telephony, memory, surveillance systems, and other technologies, including nanotechnology and robotics, which must be taken into account from now on. These electronic media will be targeted increasingly more often and will also be used to conceal, commit, or support crimes and offenses. Only the positive actions for which one or more means were used to commit one of the elements of the offense can be included.

2.2 Anthropological Aspect of Cybercrime

From an anthropological aspect, cybercrime originates from various populations and exhibits socio-educational, socio-economic, and techno-ideological factors and their expressions, including pathological expressions like addiction. The maladjustment of the education system may contribute to the development of new forms of cybercrime or deviant practices and behaviour with various levels of severity, including cheating and reputational damage, which can be related to frustrations and the redefinition of material and citizen values, inconsistent with what is expected when approaching and leading an adult life. Difficult socio-economic conditions also include the Internet as a place for expressing psychological troubles with socio-economic origins, including theft, child pornography, and calls for uprisings, violence, and hatred. With regard to techno-ideological factors, one must consider sites and networks aimed at propaganda, destabilisation, and individual and mass psychological manipulation using methods that involve the digital processing of images, videos, and audio.

2.3 Strategic Aspect of Cybercrime

From a strategic aspect, cybercrime is seen as an offense to cyber-security, namely attacks to digital networks for the purpose of seizing control, paralysing them, or even destroying infrastructures that are vital to governments and sectors of vital importance.

III. IMPACT OF CYBER CRIME

This section presents the results concerning the impact of technological change and breakthroughs of dominance – or rather, of the increase – of cybercrime during the 2010 to 2020 decade.

3.1 Perception of the Impact of Cybercrime

The impact of cybercrime is hard to identify. Yet, there is an increase in the development of information technology and the exploitation of vulnerabilities among cybercriminals, a gap between lawful and corrupt countries, and a paradox related to technological developments and breakthroughs. It is always worthwhile to remember that technology itself is neutral. However, its use can be described as negative or positive. This is especially true in cryptography, used for securing transactions and data interchange as well as to secure communications covering illegal activities and the establishment of evidence. History shows that new technologies, rarely regulated and not fully complete, are both used for good and bad. The next ten years will be marked by mobility, with the need for availability, real-time communication, connectivity, and a dependence on digital identity equipment and risk. This decade will also include monitoring automata systems and increasingly new risks.

3.2 Negative Developments with regard to Cybercrime

Expected developments, which may have a negative impact on cybercrime, render little distinction between work life and private life, using for example the difficulty of locating information for a company and Web applications with cloud computing, targeted stealth malware, and more generally, the massive use of new technologies, including mobile and wireless technologies, and a careless exposure to social engineering, social networks, and mobile downloads carried out less securely than in the past. We must emphasize the volatile nature of finding data as evidence and the difficulty of reporting offenses to the sources, with no legal means, because cybercriminals are adapting alongside new technologies.

3.3 Positive Developments with regard to Cybercrime

Security measures based on these same technologies could have a positive impact. Security is central to the problem and must be based on policies and be strictly enforced. It will be a major challenge with cloud computing, due to the complexity of where data is stored and the numerous jurisdictions involved, major risks associated with governance and territoriality. The effective level of quality security will be a key factor in the acceptance of these new services.

IV. CYBER CRIMES AGAINST INDIVIDUALS

Against Individuals: –

□ Harassment via e-mails

a) Email spoofing

(Online a method of sending e-mail using a false name or e-mail address to make it appear that the e-mail comes from somebody other than the true sender.)

b) Cyber pornography (exm.MMS)

□ Cyber-stalking.

□ Dissemination of obscene material.

□ Defamation.

□ Unauthorized control/access over computer system.

□ Indecent exposure

□ Email spoofing

□ Cheating & Fraud Breach of Confidentiality

4.1 Computers as target of crimes

Due to the Home PC the use of computers has grown widely, such computers can become target of crime either in the physical or in the virtual manner, i.e. parts of the computer can be stolen example the hard disk thus leading to physical break-ins. Unauthorized access to the computer leading to confidential data loss will amount to virtual targeting of the computer, this will amount to a crime of data theft, which is termed as hacking in the ordinary parlance. Other forms of crimes in which the computer is the target include offences such as – Blackmail based on the information stolen in the form of medical information, personal data etc. this category can also include offences like the theft of Intellectual property, or important data of corporations like the marketing information etc. Further these crimes could also be committed with a mean intent by causing impediments in the business operation. Gaining access to the government records and making false passports, driver's licenses, manipulating the tax record, land record, accessing the intelligence files etc.

The type of victim's targeted also helps in establishing the typology of the Cyber crimes Individuals: Most of the cyber crimes fall under this type, cyber staking is an example of an individual being affected through internet, or an individual may be affected even though he may have nothing to do with the cyberspace but still be victimized for instance online baking transaction frauds committed by hackers who gain entry into the computer systems of the banks.

4.2 National Security

E–mail as its is popularly referred to started becoming utilized for military applications. With the development of the World Wide Web this technology was inducted in the public domain. This is the starting point where the virtual medium started being utilized for criminal activities, and with the growth of terrorism, the terrorists also have adopted this technology. The terrorist's organizations all over the world have started using the internet to spread their ideology, and also for bringing in ability to their nefarious activities against any state or society at large. Further there are attempts done by terrorist organizations to disrupt the communications hubs of the states, so that their activities could be carried with greater effect causing larger damage. In the context of national security, especially viz. military applications information plays a major role, on the basis of which military victories become decisive. This game of intelligence and counter-intelligence is carried out in the virtual medium as most of the military activities and the information management of most of the advanced nations is based on the use of computers and the internet. Thus disrupting the information's network of the advanced nations through the virtual medium has become a cost-effective technique resorted by the nation who do not have the military supremacy.

4.3 Economic crimes

This is one of the most widely committed crimes and with the society with every passing day more and more members of the society accepting e-commerce as a means to do commerce, crime through the virtual medium will be the one of the major dilemma which will necessarily be required to be contained through the agency of law. Major economic crimes under this classification are: Hacking, Virus, Cyber frauds, Software piracy and violation of copyrights, Industrial espionages by rival corporations Forgery and counterfeiting etc.

The content of the information also forms the basis for classification in deciding the typology of the Cyber Crimes – The quantum of information being exchanged on the internet is beyond imagination. Not all the information being exchanged on the net has remained within the limits of public morality, thus the net has become a fertile ground for exchange of immoral information further leading to misuse of the right of freedom of speech and expression.

4.4 Society is dynamic

However due to rapid technological advancements in communications and the computer technology have left the law trailing behind to such an extent that it is facing the complex challenges posed by the criminals of the new generation, who commit modern crimes with the help of technology. The focal use of the net is to transfer files, exchange mails, for video conferencing, and the latest to add to these various purposes of communications is voice interface, these above mentioned forms of communications are carried out between the computer and a distantly accessible host computer, this form of communications becomes all the more important in the age where E–commerce has become a inevitable means of doing business.

4.5 Jurisdiction

Territorial limitation on the internet becomes of peripheral nature in the virtual medium as the web pages on the net can reach almost every province in the nation and conceivably almost every nation on the globe. This is where the point of friction between the cyber world and the territorial world begins as in the territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world.

A judicial system can function effectively if it is well regulated; it is these regulations that identify every functional aspect of the judicial system including the jurisdiction of the courts. A court in order to deliver effective judgments must have proper and well defined jurisdiction, as without a jurisdiction the court's judgments would be ineffective Jurisdictions are of two types namely, Personal and Subject Matter jurisdiction, and for a judgment to be effective both these types must exist contemporaneously. Further the conventional requirement as to a party can sue another is at the place where the defendant resides or where the cause of action arises. This itself is the problem with Internet jurisdiction as on the net it is difficult to establish the above two criteria's with certainty. Issues of this nature have contributed to the complete confusion and contradiction that plague judicial decisions in the area of Internet jurisdiction.

The IT Act 2000 passed in India is a perfect example of the ambiguous law in the area of jurisdiction in the context of the Internet. Section 1(2) provides that the act shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention there under committed outside India by any person. Similarly Section 75(2) provided that this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. Such a provision appears to against the principle of justice. Going to the next level, let’s say even if the Indian court successfully assert jurisdiction and pass a judgment as per the above provisions of the IT Act 2000, the other question that arises will the foreign courts implement such a judgment? In case of the above predicament the only way to resolve such a dispute is by means of having an extradition treaty with the host nation and India, further it has been suggested by that the Indian court develop justifiable ground on which the extra-territorial jurisdiction may validly exercised as done by the American Judiciary1. From the above it becomes necessary to appreciate the complexities involved and thus it becomes indispensable to understand the nature of the Cyber crime, and whether the existing penal laws are sufficient.

When Macaulay came up with the Indian penal code in 1860 the notion of Cyber Crimes was completely unknown. Further until the IT Act 2000 was enacted there was no legal provision viz. Cyber Crimes; this was the sole rationale along with recognizing transactions carried on by means of electronic communications to augment the e-commerce, with which the IT Act 2000 was enacted. Further a blanket provision was made under section 77 of the IT Act 2000 which provides that the penalties or confiscations provided under the IT Act 2000 will not release an offender from liability under any other law, in short the substantive provisions of the IPC are still applicable to Cyber Crimes committed in India.

V. TYPE OF ATTACKS

5.1 Attacks to Electronic Identity

Electronic identity theft, resulting from acts of interception and data theft, will increase, particularly through social engineering, currently carried out in cybercrime using malware tools and powerful methods, such as phishing and spamming. Personal data will continue to be intercepted from personal systems, businesses, and communities over time, given their increasingly high tech nature, for financial gain and other motivations.

5.2 Attacks on Minors

Child pornography is expected to remain steady in terms of physical concurrent acts. This form of crime relies on "*human material*", with children victimised by acts of paedophilia or made to participate in carrying out offenses. This is still risky for criminals due to legal enforcement. What will change in this area is the way in which images and videos will be exchanged, with greater availability and concealment. *Child pornographers often argue that they are not doing anything wrong, instead believing themselves to be merely "voyeurs".*

5.3 Attacks on Infrastructures

Critical infrastructures will be targeted by cyberterrorism for various reasons. Power distribution networks, transportation networks, and communication networks are expected to undergo attacks intended to paralyse a nation by depriving it of its vital services. Such attacks could cause unprecedented crises on many levels, including *the economy, safety, health, sanitation, civil peace, and more*. In addition, hackers and other cybercriminals (even governments themselves) could further target their opponents. They may include attempts to attack informational sites, with a growing number of counterattacks by some governments or resistance groups.

VI. CYBER CRIMES AND THE NATURE OF EVIDENCE

The nature of evidence in the real world and the virtual world is different. This disparity is conspicuous in all the stages of evidence detection, gathering, storage and exhibition before the court. The critical part is that all the investigation authorities that are responsible right from the stage of collection of the evidence to the presentation of the evidence before the court must understand the distinguishing attributes of the evidence so that they can preserve the evidence collected by them. In this regard the role of the judiciary also becomes vital as the judiciary must also be in the position to appreciate the computer evidence presented before them. Contrary to the real world crimes where any tangible evidence in the form of finger prints, weapon of crime, blood stain marks etc can be traced, in the virtual world such traces become very difficult to find. The science of computer forensics is gaining significance in the investigation departments, corporate world, government departments etc. Let us understand some of the challenges that are involved in the process of cyber evidence detection, gathering, storage and exhibition before the court.

It is considered difficult to expunge the information from the computer system than what is generally contemplated. This can be done with the help of computer forensics who are able to gather evidence or even recover information which may have been deleted intentionally. It is vital that the victim report the law enforcement agencies about the crime as early as possible. The process of preservation of cyber crime evidence lies within the understanding of an efficient and knowledgeable computer forensics expert because any carelessness in the process can lead to diminutive value of the evidence. The most often faced impediment is that the victim–companies are more concerned with restoration of their systems to full operational status rather than allowing proper evidence collection. Thus the timely assistance of the computer forensics expert can help collect evidence from the system within shortest time possible.

Cyber evidence is of physical or logical nature. It is the physical evidence that can be traced easily as the investigator just has to visit the scene of crime and search for and take into his custody computer hardware, which may constitute main frame computers to pocket sized personal assistants, floppy diskettes, electronic chips etc. The facets of the logical component of the cyber evidence are of different nature. This entails a process described as Information Discovery' wherein the investigator scrutinizes through the log files, and tries to salvage the data from a computer system which has been affected.

Once the required evidence is identified, then the investigator must ensure that the same is collected by adhering to the legal requirements, such as evidence is collected only after the requisite warrant for it is issued or if the information appears to be outside the scope of the warrant then additional warrant be issued. The evidence collected becomes valid in the courts of law only if the evidence is collected by legal means16. At the moment only officers not below the rank of a Deputy Superintendent of Police and officers deputed by the central government can be authorized to enter public places and collects evidence and carry out search operations and arrest17. This authority has been given to higher grade officers at the moment keeping in view the misuse of this power viz. right to privacy and ensuring the validity of the cyber evidence As of now in India the concept of 'Reasonable expectation of Privacy' has not be developed. The issues involved in this are that whether an 'individual's demeanor reflects subjective expectation of privacy' or 'the individual's subjective expectation of privacy is such that the society is ready to recognize it as reasonable.

Another quarter which needs to be tested under cyber evidence and which is inevitable is the appreciation of the computer generated evidence by all the authorities associated with the process of administration of justice. Thus not just the judiciary19 but also the prosecutors, the defence lawyers must become familiar with the technicalities, this is so because till now these authorities were dealing with evidence in the tangible form but the nature of evidence undergoes complete change under the virtual medium, they will have to adjust themselves to appreciate the evidence in logical format.

VII. PREVENTIVE MEASURES TO AVOID CYBER CRIMES

□ Cyber Forensics can be use to detect cyber Evidence

□ To make necessary amendments in Indian laws to control on Cyber Crimes

□ There is strong need to harmonize some sections of IT act 2000 to curb cyber crimes and Individuals to prevent cyber stalking avoid disclosing any information pertaining to one. This is as good as disclosing your identity to strangers in public place

□ Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

□ Always use latest and up date anti virus software to guard against virus attacks.

□ always keep back up volumes so that one may not suffer data loss in case of virus contamination

□ Never send your credit card number to any site that is not secured, to guard against frauds.

□ Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.

□ It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.

□ Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.

□ web servers running public sites must be physically separate protected from internal corporate network

VIII. CONCLUSION

Change is inevitable and the dilemmas that advancement in technology poses cannot be avoided, the truth is that the criminals have changed their method and have started relying of the advanced technology, and in order to deal with them the society the legal and law enforcement authorities, the private corporations and organizations will also have to change. Further such experts must not only be knowledgeable but must also be provided with necessary technical hardware and software so that they can efficiently fight the cyber criminals. Thus necessary facilities must be established in various parts of the country so that crime in the virtual world can be contained20. Another aspect which needs to be highlighted is that a culture of continuous education and learning needs to be inculcated amongst the legal and the law enforcement authorities because the Information Technology field is a very dynamic field as the knowledge of today becomes obsolete in a very short time. Lastly the preamble of the Information Technology Act 2000 provides that the act was passed with the objective to give legal recognition for transactions carried out by means of electronic data interchange and other means of e-commerce, further the act has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act 1934 for facilitating legal recognition and regulation of the commercial activities. Though this objective of the act is not to suppress the criminal activity, this act has defined certain offences and penalties to smother such omissions, which is understood to come within the characterization of cyber crimes. From this it can be inferred that the law cannot afford to be static, it has to change with the changing times and viz. cyber space this is all the more required, as there many application of the technology that can be used for the betterment of the mankind, similarly it equally true that such application can also be used for the detriment of the mankind as has been demonstrated by the Spy–cam case. The bottom–line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development. 20 Cyber cell of the law enforcement agencies have started operating in metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc.

REFERENCES

[1] www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov guidelines_provisional2_3April2008_fr.pdf

[2] www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf

[3] http://userpage.fu-berlin.de/~jmueller/its/conf/Madrid02/abstracts/Ghernaouti-Helie.pdf

[4] www.met.police.uk/pceu/documents/ACPOecrimestrategy.pdf

[5] Guinier D, Dispositif de gestion de continuité – PRA/PCA: une obligation légale pour certains et un impératif pour tous (Continuity Planning – BRP/BCP: a legal requirement for some and a vital necessity for all). Expertises, no. 308, Nov. 2006, pp. 390-396.

[6] CSIS: Securing Cyberspace for the 44th Presidency, CSIS Commission on Cybersecurity, US Center for Strategic and International Studies (CSIS), Washington DC, December 2008.

[7] Verizon (2011): 2010 Data Breach Investigations Report, Verizon/US Secret Services, 2011.

[8] Crimes in Cyber Space (Scams & Frauds) – By V D. Dudheja.

[9] Intellectual Property - Cornish 3rd Volume

[10] Computer & Cyber Laws - Nandan Kamath

[11] Laws relating to Computers - Rahul Matthan

[12] Indian Copyright Laws - Narayan

[13] “Cyber Crimes against Individuals in India and IT Act.