RESEARCH PAPER | Commerce | Volume : 3 | Issue : 11 | Nov 2013 | ISSN - 2249-555X

Cyber Crimes: Problems of Investigation and Solution

KEYWORDS

Minny Narang
Assistant Professor, Department of Commerce, Delhi School of Economics, Specialisation- law and finanace, University of Delhi

Gunjan Jain
M.Com, Specialisation- law and finanace, Delhi University.

The 21st century is technology driven era. Advancement in the field of information technology has changed our life. This information technology is still in its age of infancy. Today 93% of all the world data is in digital format. There are about 972, 828, 001 internet users in the world. In India, they are amounted to 39, 200,000. In the next 10 to 20 years, it would be impossible to do any thing without information technology because of its usefulness and consequent dependence upon it. For example, in our Constitution, Article 39 of Directive Principles of State Policy mandates the promotion of justice on the basis of equal opportunity, which implies the concept of justice at the doorstep and of speedy trial. This dream can become a living reality by equipping courts with electronic devices which will make it possible to assist courts through electronic devices with electronic petition filing, video-addressing, video-conferencing and thereby keeping a check on multiplying litigation. It is said that justice delayed is justice denied but with innovation and information technology's application to law it would be possible for the judiciary to speed up the dispensing of justice. India is globalizing its economy. Information services in information technology are starting to have strong effect on the national economy, trade and commerce.

Today, world is undergoing second revolution. Every aspect of human life is being touched by information technology. Every day's activities are affected in form, content and time by the computer. Computerization is replacing human tasks. Computers are used not only extensively to perform the industrial and economic functions of society but are also used to perform many functions upon which survival of human life depends. Computer oversees medical treatment, conducts air traffic control, manages offices, runs businesses, controls defense system of the nations, and regulates the transport system and reservations. Computers are extensively being used for crime detection. Interestingly computers are now even being used to repel mosquitoes.

Every technological development also has got its flip side too. Information Technology is like a double edged weapon. The traits like speed that made the computer, information technology, Internet and World Wide Web popular, are equally responsible for the misuse of the same in the hands of anti-social elements. Criminal minds are quick to harness the fast, easier and cheap medium for their illegal and immoral pursuits. It is a deadliest epidemic face by the world in this millennium. A modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. From software piracy in China to virtual money laundering in the South Pacific, across Asia criminals have been quick to cash on the new opportunities offered by the Internet. This technology has not only given rise to a new wave of 'cyber crimes' but also considerably widened the scope and enhanced the lethal striking capability of the 'traditional crimes'.

One of the greatest lacunae of this field is the absence of a set of comprehensive law anywhere in the world. Further it the growth ratio of Internet and cyber-law is also not proportional. The bottom line is that the internet and the Information Technology are like technological 'tsunami' bound to sweep every woman and man off the floor and no nation in the earth can either ignore or afford to go slow on these. Therefore, it is better to be prepared in advance to utilize the information technology to one's benefit, than to be left on the wrong side of the digital divide.

Investigation of Cyber Crimes

The law enforcement agencies were bound by some ground rules before the evolution of cyber crimes. There were established procedures for investigation and prosecution of all types of crimes. In case of traditional crimes, large number of physical evidence is generally available at the scene of crime. Collection of such physical evidence required at lot of common sense and a little technical knowledge. Forensic help could also be provided since laboratory examination procedures are fully established. The crime scene is also confined to a relatively smaller place.

Today, with the advancement of technology, crimes have become more complex and criminals more sophisticated as their modus operandi is incomparable to the traditional investigation methods. Information technology provides and opportunity to the criminals to commit traditional crimes like cheating, fraud, theft, credit card frauds, embezzlement of bank deposits, industrial and political espionage, cyber terrorism etc. and at the same time it helps in committing non-traditional and information technology related crimes like attacks against the security of critical infrastructures like tale communication, banking and on emergency services. Such crimes may be committed through computer networks across the national borders, affecting not only individuals, but they may instead result in compromising the security and the economy of the nation.

In this information technology age, the criminal investigation procedures require radical changes to handle the errant computer users effectively. Today, the crime investigators are faced with the problem of collection of appropriate evidence in computer storage media and data communication system. It requires a cohesive well trained and well equipped force of investigators operating and co-coordinating at national and international level. This change in crime scenario would also necessitate major changes in the related forensic procedures as well as in the outlook of judiciary. Present era of fast changing technologies well soon derail the criminal justice system and make the whole exercise futile, if appropriate steps are not taken urgently.

The law enforcement agencies throughout the world are mainly facing three types of problems in their fight against the cyber crimes.

Volume : 3 | Issue : 11 | Nov 2013 | ISSN - 2249-555X

Jurisdictional Problems

Cyber crimes are crimes truly with have o boundary. Information technology has turned the world into a global village. The advent of Internet has put every one within the reach of other. The cyber criminal have scant regard for national or local jurisdictions. Section 75 of the Information Technology Act is Indian answer to jurisdictional blues. This Section extends the influence of Information Technology Act, 2000 over the entire world keeping in view the nature of cyber crimes.

The salient feature of the provision is that person of any nationality can be booked under this Act provided in the conduct of an offence or in any contravention, any Indian computer, computer system, computer network is in any way involved. So the nationality of criminal, place of perpetration of the crime, the place of effect of crime or nationality of the target or victim is immaterial. Some times a cyber crime is committed from one corner of world against a person in the other corner of world but routed through India. In such circumstances to assume jurisdiction only requirement is the involvement of any Indian computer system, and computer network. It is indeed a revolutionary approach, which is otherwise also a dire necessity if cyber crimes menace is to be tackled.

However, the problem is not as simple as it appears. The difficulty arises in implementing extra-territorial jurisdiction. The problem will arise as to actual conducting of investigation and trail. Internal territorial problems can be solved such problem invariably arises in international arena. The first point is how far the nations are willing to help one another. Police investigations abroad are stifled by a variety of factor, including the desire to protect individual of certain nationalities. The procedure also involves a request by the court of one country to its counterpart in another. Collection of information in cyber matters requires searches and confiscation of delicate material that needs speedy and expert handling. Assistance in such areas is slow and half-hearted despite there being bets relations among countries. An interesting question that arises is how far the police of one country is justified in entering a computer system across the border suo moto to secure information that is available online and is crucial to an investigation. It is very cumbersome, lengthy and expensive. A senior police official is quoted. "The grey areas in the laws apart, we face difficulties when a cyber crime is committed outside the geographical jurisdiction of the country. For instance, we received a complaint from a lady who was receiving absence calls on her cell phone. Since the calls were made from South Africa. We faced difficulties while handling this case."

Also, Section 75 has potential to create problems, as an act that occurred overseas may have no connection in India except the use of some remote computer resource located here, this, which is quite common in internet relations, may be brought within the purview of our laws. How it is justifiable to start criminal proceedings against a foreigner who has not committed any act on Indian territory? It is submitted that jurisdiction of IT Act shall not extend to those cases where the accused and victims are foreigners and the offence is committed outside the territory of India.

Regarding the offences the general provisions of Code of Criminal Procedure, 1973 are applicable. However the tardy procedures of letters- regatory under Section 166A and 166B of the Code of Criminal Procedure enabling investigation of crime in a foreign country would be hopelessly out of tune with the scope of computer crime and swiftness with which the evidence can be destroyed. Similarly, the bar of Section 188 of the Code, requiring prior permission of Central Government to inquire into or try offences committed outside the country, appear to be out of tune with the global nature of computer activity, which has dramatically changed the way we work, communicate and even play.

For trail in India of any foreign national, he can be demanded from has parent country only when the same facts also constitute an offence in that country. For example, pornography is not illegal in Amsterdam (Holland), any person transmitting obscene material in India can not be brought to India and tried under the I.T. Act of 2000 despite the same being an offence here,. Gambling and obscenity laws provide criminal sanctions of individual within their jurisdiction. For example, if the person placing the bet and the bookie is in a country such as the UK where gambling on cricket is legal, and if the bet is placed from a computer in India how can get police department effectively act on this crime in India?

The extradition treaties are not generally there. Even when there is any such extradition treaty, offender can be extradited to India only when the same facts also constituted an offence in other legal system and too after the testing of facts and offence by the legal systems of both the countries. It will be a protracted battle. A number of Kashmiri terrorists are hacking Indian sites from Pakistan. Due to political differences least cooperation is expectable from Pakistan. It has different definitions of crime. Any act of cyber terrorism will be offence in Indian but they are categorized as freedom fighters by Pakistan. So they cannot be brought to book.

A pertinent question arises whether a judgment passed by an Indian court in matter relating to a person/company situated abroad but duly covered under the provisions of the I.T. Act of 2000 would be acceptable to foreign courts. If the judgments delivered by Indian Court can not be enforced then whole exercise of trial and punishments would turn out to be futile if we go by recently U.S. Court approach in Yahoo Inc. France Naxi Memorabilia dot com case. The answer will be disturbing 'no'. U.S. Court approach in Yahoo Inc. France Naxi Memorabilia dot com case has highlighted the legal and practical difficulties in nailing the criminal in a foreign country. Most of the Internet Service Providers are stationed in U.S. A. Hence, this decision is bound to affect the interpretation and implementation of Section 75 of the I.T. Act of 2000. It shows that in the absence of internationally accepted jurisdiction treaty or convention, the desire to bring the cyber criminal book from any corner of the world is just a dream which is far from reality. The problem will be more acute as India is still not the signatory of the International Cyber Crime Treaty, It does not enjoy the privileges accorded to signatory nations in the detection investigation and prosecution of cyber crimes.

Legal Problems

Cyber crimes have become a global menace and is no longer the problem affecting only the developed countries. Therefore, all the nations should treat this menace seriously.

There is no universally accepted definition of cyber crime. The cyber crime in a country may not be termed as a cyber crime in another. There are only 13 countries that have cyber crime laws. This puts enormous pressure on the law enforcement agencies in obtaining international co-operation. The absence of such laws is like shielding the criminals from the legal provisions and providing them safe haven to continue with their evil deeds. Further, the rate at which cyber crimes are increasing in the world, it is necessary for the criminal justice to demonstrate that quick and severe punishment would be awarded to those involved in such criminal activities. What we need is the rule of law at an international level and a universal legal framework which is equal to the worldwide reach of internet. It is therefore, necessary to make appropriate dynamic laws pertaining to cyber crime. It cannot take the usual snail's pace of law making since the technology changes at a very fast rate. The laws made today for yesterday technology might become outdated by the time they are checked. It is submitted that universally accepted definition of cyber crime shall be made and an international treaty on cyber crime shall be made and shall be signed by the entire countries of the world in order to tackle menace of cyber crime.

Volume : 3 | Issue : 11 | Nov 2013 | ISSN - 2249-555X

To effectively combat the cyber crime, it is not sufficient to successfully investigate the crime and nab the criminal, but more important is to prosecute and administer justice, according to the law of land. This requires an effective legal frame work, which fully supports the detection and prosecution of cyber criminals. The traditional techniques for investigation of cyber crime and the prosecution procedures are inadequate. The judiciary must also appreciate the intricacies of the digital evidence that is collected and presented in the courts of law, in spite of the technical and operational hurdles the investigator faces.

(a) Victims and Witnesses' Unawareness

The first impediment that is faced by investigators is of securing the co-operation of complainants and witnesses. It is now well-documented that the victims of crimes of this nature are reluctant to report them to the police. Ernst and Young found in its 8th Global Survey of business fraud, that only one quarter of frauds were reported to the police and only 28% of these respondents were satisfied with the resultant investigation.

Some of the reasons given by the respondents of an Australian survey conducted by Deakin University in Melbourne on fraud incidents against businesses in Victoria for not reporting fraud to the police included a belief that the matter was not serious enough to warrant police attention, a fear of consumer backlash, bad publicity, inadequate proof and a reluctance to devote time and resources to prosecuting the matter. In the case of cyber crime, this last explanation is of great significance. As the time and resources needed to prosecute an offender in another jurisdiction can be considerably very high. The result is that investigators may face considerable barriers in securing cooperation from victims and witnesses especially those located in other countries. Unless and until the people are not made aware of this epidemic it is impossible to tackle this problem.

(b) Identifying Suspects

Another problem faced by cyber crime investigators is the identification of suspects. Occasionally, this can lead to considerable problems when the wrong person is arrested.

Digital technologies enable people to disguise their identity in a wide range of ways making it difficult to know with certainty as to who was using a computer from which illegal communications came. This problem is more prevalent in business environment where multiple people may have access to a personal computer and where passwords are known or shared, than in private home where it can often be assumed who the person was and who was using the computer because of circumstantial evidence.

On-line technologies make it relatively simple to disguise one's true identity, to misrepresent one's identity or to make use of some one else's identity, e-mailing services can be used to disguise one's identity when sending e-mail by stripping them to identifying information and allocating an anonymous identifier, sometime encrypted for added security. By using several Emailing services users can make their communications almost impossible to follow.

Anonymity can also be achieved in cyberspace using less technologically complex means simply purchasing a pre-paid Internet Service Provider and renting a telephone line from a carrier, each in a false name provides an easy means of achieving anonymity.

This problem of identifying suspects may be resolved by traditional investigative techniques, such as the use of video surveillance or gathering indirect circumstantial evidence that locates accused at the terminal at a particular time and day. However the use of intrusive surveillance is not always successful with attention having to be paid to human rights issues and legal privileges.

This problem may be also solved by the use of biometric means of identification. At present few computers have biometric user authentication systems such as fingerprint scanner when logging on. When they become more widespread, problems of identification may be reduced.

DNA samples which can be gathered from keyboards may be used to identity an individual with a particular computer in some cases.

Technical Problems

Technical challenges thwarting the efforts of law enforcement agencies ability to catch and prosecute on line offenders. Investigating the Internet crimes, e.g., hacking of a website, staling data stored in computers, exchanges of pornographic material, espionage, blackmailing e-mails etc, involves identification of the person who initiated the communication.

Locating and Securing Relevant Material

Considerable difficulties arise in locating and securing electronic evidence as the mere act of switching on or off a computer may alter critical evidence and associated time and date records. It is also necessary to search through vast quantities of data in order to locate the information being sought.

Today's cyber investigators are faced with many problems because digital evidence is highly fragile, bits are easier to temper than paper, can easily be altered, manipulated and destroyed. So chain of custody of these needs is to be maintained and all digital evidence need to be authenticated.

Difficult problems arise in obtaining digital evidence in cyber crime cases, although in some ways computers have made the process easier through the ability to conduct searches of hard drives remotely via the Internet. Some of the main difficulties, however, relate to obtaining permission to conduct such a search, securing the relevant access device such as a password, decrypting data that have been encrypted, and imaging a hard drive without interfering with the evidence. There is also the practical problem of conducting searches quickly so that data cannot be removed.

Problems of Encryption

A difficult problem faced by cyber crime investigators is concerning the data that have been encrypted by accused who refuse to provide the decryption key or password.

An illustration of the use of strong encryption by a criminal organization was discovered during 'Operation Cathedral' by police in 1998, which led to the largest ever global seizure of pedophile material. This involved police in 15 countries who uncovered the activities of the Wonderland (sic) Club, an international network with members in Europe, North America, and Australia who used the Internet to download and exchange child pornography including real time video images. The Club used a secure network with regularly changed passwords and encrypted content. In Europe alone, over 750, 000 images were recovered from computers, along, with over 750 CDs and 1,300 videos and 3,400 floppy disks. The encryption used was able to be overcome because one member of the club cooperated with police and provided access to the files. This led to approximately 100 arrests around the world in September 1998.

In order to decrypt data, one method is to install a key logging program onto a computer that will capture the password used for decryption. The installation of such a program of course must be done without the knowledge of the accused. This may cause legal complication such as it amounts to interference with right to privacy, and a special warrant needs to be obtained for this. In one famous case in the United States, evidence obtained in this way was challenged on the grounds that the key logger involved the illegal interception of wire communications that requires a special warrant. It was held, however that the key logger only operated when

Volume : 3 | Issue : 11 | Nov 2013 | ISSN - 2249-555X

the computer's modem was not connected thus excluding any interception of telecommunications.

If all else fails, investigators may seek to break encryption codes, although this is difficult, time consuming and costly and would be inappropriate in all the cases.

The Australian Federal Police, for example, has seen an exponential increase in the size of data storage system that the required to be analyzed during investigations. Where a law enforcement examination of a computer hard drive in 1990 involved 50,000 pages of text, a contemporary examination of the same would involve approximately 5 to 50 million pages of text. This increase in investigative capacity has created considerable resources implications for police that will no doubt increase in the years to come.

Conclusion and Suggestions

The increasing popularly and dependency upon internet, www and information technology and the vulnerability of personal data to criminal access makes everyone the easiest target for a range of culpable crimes. According to Justice Yatindra Singh "regulating cyber space is daunting task of corpus juries of any country. Computer, internet and cyberspace-together known as Information Technology has posed new problems in jurisprudence. I have shown inadequacy of law while dealing with the information technology, changes induced by the information technology in the way we live, perceive and do business". The existing laws were designed, having geographical location, tangible medium and physical environment in view. These laws are not suited to faceless, borderless and paperless cyberspace. This required for a new legal regime which would provide solutions to the issues generated y this new technology. So it is submitted that after identifying the cyber crime universally accepted definitions of these shall be made and cyber penal code shall be enacted which incorporate all these offences and an international treaty on cyber crime shall be made and shall be signed by the entire nations of the world in order to tackle the menace of cyber crime.

Section 75 of the Information Technology Act extends the influence of this Act over the entire world keeping in view the nature of cyber crimes. As we have discussed earlier, difficulties arise in implementing extra-territorial jurisdiction. So, it is submitted that jurisdiction of IT Act shall not extend to those cases where the accused and victims are foreigners and the offence is committed outside the territory of India.

It is submitted that the jurisdictional problems shall be resolved through the international cooperation taking in view the global impact of cyber crimes. It is an urgent need that the tardy procedures of letter-regatory under Sections 166-A, 166B and 188 of the Code of Criminal Procedure shall be removed by making suitable amendment in the Code of Criminal Procedure.

It is evident from number of studies conducted by various agencies that victims of cyber crime are reluctant to report them to the police and the witnesses are non cooperative. So it is suggested that people shall be made aware about the gravity of these crimes so that the people (victim) shall inform the matter to the police as soon as the crime is committed. It is submitted that for the identification of suspects the computers (at least computer owned by institutions and companies) shall be lodged with biometric use authentication system.

REFERENCE (i) Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. ITU Telecommunication Development Bureau. | (ii) Smith, G. R. (2003). Investigating Cybercrime: Barriers and Solutions. Retrieved Oct. 01, 2013 from | a. http://www.aic.gov.au/media_library/conferences/other/smith_russell/2003-09-cybercrime.pdf | (iii) Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future, International Journal of Cyber Criminology, 1(1), 1-26. | (iv) Singh, T. Cyber Law & Information Technology. Retrieved Oct. 01, 2013 from http://delhidistrictcourts.nic.in/CYBER%20LAW.pdf | (v) Information Technology Act 2000 (Delhi) (Ind.).