Available Online at http://www.journalijcir.com

International Journal of Current Innovation Research
Vol. 4, Issue, 12(A), pp. 1416-1422, December, 2018

ISSN: 2395-5775

International Journal of Current Innovation Research

DOI: 10.24327/IJCIR

Research Article

THE CRIMINALS IN A CYBER ENVIRONMENT USING COMPUTER NETWORKS

Jitender K Malik* and Sanjaya Choudhury

Department of Law, Bhagwant University, Ajmer (Raj.)-India

ARTICLE INFO

Article History:

Received 15th September, 2018
Received in revised form
13th October, 2018
Accepted 10th November, 2018
Published online 28th
December, 2018

Key words:

Cyber space, Critical infrastructure, Cyber Crimes, Internet, Netizen.

ABSTRACT

In traditional and online trading environments, consumers are entitled to have their privacy respected. While shopping on the internet; most people typically do not think about what is happening in the background. In the modern era of electronic technology, people want to get their work done quickly with little effort. At times, people forget or ignore the legal and ethical values of their actions. Consequently, cyber wrongs in different forms are increasing day by day: cracking/hacking, e-mail spoofing, spamming/Denial of Services (DOS attacks), carding (making false ATM Debit and Credit cards), cheating and fraud, assault by threat, impersonation, intellectual property rights (IPR) infringements (software piracy, infringement of copyright, trademark, patents, domain names, designs and service mark violation, theft of computer source code, etc.), online gambling and other financial crimes including the use of networking sites and phone networking to attack the victim by sending bogus mails or messages through internet, forgery, URL hijacking or squatting (using the domain name of another person in bad faith), cyber vandalism (destroying or damaging the data when a network service is stopped or disrupted), virus transmission, internet time thefts, pornography, cyber terrorism etc-the list is endless. Customer information has to pass through several hands; and the safety and security of a customer's personal information lies within the hands of the business. Therefore, security and privacy of the information are a major concern. E-commerce has a tremendous impact on copyright and other intellectual property rights (IPRs). The issues related to copyrights on digital content also lie unaddressed. From one perspective, the internet has been described as "the world's biggest copy machine." Generally, a trade mark can be owned by an individual, a company, or any sort of legal entity. When someone else tries to use that trademark without authorization, it could be considered an illegal dilution of the distinctive trademark. If someone uses a trademark in such a way as to dilute the distinctive quality of the mark or trade on the owner's reputation, the trademark owner may seek damages. In the cyberspace, domain name infringements are rampant. The present study primarily intends to address the pitfalls in the present legal system and to evolve a strategy to regulate cyber crimes in India.

INTRODUCTION

The digital technology gives a space to everyone. This space is known as cyberspace, which provides a separate space for their activities. Internet is being used about in all activities of daily life including communication, commerce, advertising, banking, education, research and entertainment. There is hardly any activity that not touched by the internet. In few words, it can be said that the Internet has entered into the blood of the human beings. It has been found that many of the young got addicted to remain online all-time.

Internet has blessed the human species with many gifts associated with the pitfalls. As this space has no boundary and gives a super secure space for all kinds of unlawful activities. The traditional terrorism gets new wings of internet. Now it is very easy to perform the very sophisticated attacks without visiting that targeted place. Now, in this cyber world, it is very difficult to trace the actual culprit. It provides a space for the human activities but without thinking the just and unjust. [1]

Statement of the Problem

The internet age gives a new world to the new types of weapons and target as well to the terrorists. It also gave a new shape to the ways that terrorist group's structure and operates their organizations. Zanini and Edwards, had found, the most infamous terrorist organizations on the path of information technologies, and also using hi-tech machines to organize and coordinate activities[2]. Internet, wireless communications, and other computer networks pose various new challenges for law enforcement agencies throughout the world[3]**.**

The computerization of all sectors invites the vulnerability. As the saying is clear in criminology, - "a crime will happen where and only when the opportunity avails itself." And at the same time, 'once you connected, you are vulnerable' is very much true. So in the same way use of internet provides more chances to the cyber terrorists to accomplish their bad ends.

It cannot be denied that internet technology has given a new speed to the development. At the same time law enforcement agencies started their task but failed and frustrated because of the peculiarity or the nature of the cyber terrorism. They found

Corresponding author:* **Jitender K Malik
Department of Law, Bhagwant University, Ajmer (Raj.)-India

themselves unable to adhere with the fast growing technology. On the other hand, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world's public and private networks. Moreover while investigating cyber crimes, the investigating agencies and law enforcement officials follow the same techniques for collecting, examining and evaluating the evidence as they do in cases of traditional crimes[4].

Since cyber terrorism is not a matter of concern of India only. The countries also have framed their rule and statues. Various countries have their domestic cyber laws, but the problem is that most of the books deal with cyber laws of individual nations. In this research work an attempt has been made to do a comparative study of the cyber laws and policies of different countries.

The purpose of this study is to cover the complete scenario of cyber terrorism, their magnitude and nature, and make an insight into the people who are responsible for it. This research work will also take a comprehensive view of the governmental efforts being made in India and abroad to stop such crimes and will look closely on their success and failures. An effort will also be made to vigorously analyze the various perspectives of IT Act, 2000; its inns and outs including its shortcomings and the possible means and ways to overcome them.

Objectives of the Study

1. To understand the basic concepts of the cyber world.
2. To trace the origin and development of the Cyber crimes.
3. To trace the origin and development of the cyber terrorism.
4. To analyze the law and policies of India to curb cyber terrorism in the Indian scenario.
5. To find out the international initiatives to curb cyber menace.
6. To investigate the possible defects and loopholes in the existing laws and policies relating to cyber terrorism.
7. To suggest the reforms and remedial measures for the prevention and control of cyber terrorism.

The basic motto of the study is to analyze the cyber laws at the global level. It is an endeavour to determine all the important facets of cyber terrorism in various countries of the world including UK, USA, Japan and India, etc. The study also is an attempt to find possible implications of the recently cyber attacks.

Rationale of the Study

The significance of the study is to decipher the most critical infrastructure which affects the pulse of any country. Critical infrastructure systems are facilities and assets - such as roads and bridges, telecommunications, water supply, wastewater treatment, flood-reduction structures, and power grids - so vital that their destruction or incapacitation would disrupt the security, economy, safety, health, or welfare of the public. Well functioning infrastructure systems are vital to the nation's prosperity and well-being. Critical infrastructure may cross political boundaries and may be built, natural, or virtual. Therefore, critical infrastructure includes energy, water and waste water treatment, distribution, and collection, transportation, and communications systems. Natural critical infrastructure systems include lakes, rivers, and streams that are used for navigation, water supply, or flood water storage, as well as coastal wetlands that provide a buffer for storm surges. Virtual critical infrastructure includes cyber, electronic, and information systems.

And further an analysis of cyber law as developed in India as well as to do critical comparative analysis of the cyber laws as developed in other countries relating to the cyber terrorism.

The study is important both from the theoretical and practical point of view. On a theoretical level, it reveals the legal and policy appreciation of all the important facets regarding cyber terrorism. On the practical level, it clearly shows the extent to which legal and policy approach meets the requirements of the day by protecting the people against various cyber offences. The result of the study would provide hitherto unknown criteria to evaluate the legislative and judicial philosophy in the research area.

The practical utility of the work lies in the fact that policy making institutions may remove ambiguities surrounding the cyber laws. They may also enact specific cyber legislations pertaining to cyber terrorism.

Hypothesis

The present legal and policy framework for addressing or curbing the cyber menace of cyber terrorism is not robust to achieve the avowed objectives of:

1. Protecting the critical infrastructure.
2. Effective response to the cyber terrorism.
3. Build confidence in cyberspace.

RESEARCH METHODOLOGY

The data and information has been collected from both primary and secondary sources. Constitution, Acts, treaties, subordinate legislation, orders of tribunals and courts, Reports of various committees has been looked into as primary sources. The cases decided by various judicial and quasi-judicial forums have been also analyzed for internal and external consistencies. Internal consistencies here means consistencies vis-a-vis that particular issue amongst various case situations, external consistencies means consistency vis-a-vis statutes, guidelines, rules etc. Proceedings of conferences, both National and International on issues pertaining to response to the cyber terrorism have been relied upon as secondary sources. Also books, articles, journals, reports and monographs discussing the issue has been looked into as secondary sources. E-resources have been extensively referred to. Help has been taken from law firms and institutions also. Moreover the opinions, observations, perceptions and philosophies of the eminent authors, lawyers and jurists in the area have been looked into.

The tool of research which has been applied is descriptive and qualitative ones. Descriptive studies have been undertaken to ascertain anecdotal events, working of institutions and behavioural patterns of groups. It has been employed to understand research problem. The purpose of this study was to enhance predictability under certain circumstances. Qualitative research has been employed to analyze cases, makes a comparative study of the various systems.

The materials collected from primary and secondary sources have been presented in descriptive manner and wherever required critical inputs have been provided. Although empirical data from both primary and secondary sources have been used in the study. However, neither a field study nor data collection through questionnaires of formal interview was under taken. Even though there were many informal meetings with many experts in the field, they have not been cited in the work because all arguments are based on published materials. For the purpose of interpretation of legislations secondary sources were relied upon.

REVIEW OF THE LITERATURE

They say books are the quietest and most constant of friends, they are the most accessible and wisest of counselors, and the most patient of teachers. No thesis can be written without consulting good books and articles. One of the steps for starting the work on the problem is to review the existing literature on the subject. After identifying a problem, it is imperative to consult literature on the subject as the answers you get from literature depends on the questions you pose. The review of the existing literature not only provides clarity of concept and understanding of different aspects of the subject but also helps avoid repetition. It helps in identifying problem zones. It also helps in formulating research methodology. A number of books, monographs, reports, research papers and articles deal with the subject of prevention and control of cyber crimes and of cyber terrorism.

The review of existing literature on the topic has its limitations, so the available and approachable number of books, monographs, reports, research papers and articles has reviewed for the better understanding of concept.

Books

Justice Yatindra Singh in his book “Cyber Laws”[5] provides a comprehensive guide to the various legal issues which have arisen as a result of the unprecedented growth of the internet. It covers both academic and practical information regarding technology related issues and the underlying legal principles which have been applied in these areas. The book provides an overview of the cyber law scenario in India. In the book many aspects have been discussed very nicely.

The book covers all the important changes introduced by the IT (Amendment Act) of 2008. The book also incorporates several important provisions of the Communication Convergence Bill of 2001. As far as the infringement of IPRs in cyberspace is concerned he has critically analyzed the judgments of Napster Case,[6] Sony Play Station Case[7] and Grokster Case[8]. The cyber terrorism has been discussed but in brief, even though the book is a nice work on the issues of cyber space and intellectual property rights.

Vivek Sood in his book “Cyber Crimes, Electronic Evidence and Investigation: Legal Issues”[9] has suggested various strategies to curb cyber crimes. He says that since cyber crimes are technology based, so the best answer to these crimes is security technology[10]. Fire-walls, anti-virus software and anti-intrusion systems are some of the effectively used security technologies. He concluded that “protect yourself” is the best mantra against cyber crimes[11]. The book inter-alia deals with various strategies to effectively counter these new-age crimes, explains the stepwise process of leading electronic evidence in the Court, analyses the various provisions of the I.T. Act, 2000 & IT Amendment Act, 2008 & other related statutes, takes a firm view on challenging legal issues on the subject and also answers the question whether India should sign the Convention on Cyber crime.

Dr. Vishwanath Paranjape in his book “Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India”[12] has pointed out that with the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue[13]. The book suggested the need for international cooperation to combat cyber crimes and cyber terrorism. The book also comprehensively discuss various national and international conventions, conferences, summits etc. relating to cyber crimes along with the municipal cyber legislations of different countries like UK, USA, India, Canada, China, Japan, Germany, Australia, and France etc.

Nandan Kamath in his book “Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000”[14] has commented on the emerging field of ‘electronic evidence’ in the cases of cyber crimes. He has made an in-depth study about the admissibility and authenticity of electronic records, burden of proof in cyber offences, and of certain other concepts like production and effect of such evidences, video-conferencing, forensic computing and best evidence rules, etc.[15]. The book also discusses the latest trends and crimes in the cyber space.

Dr. M. Dasgupta in his book “Cyber Crime in India: A Comparative Study”[16] has succinctly defined the meaning, nature, scope, characteristics and elements of cyber crimes. Commenting on the scope of cyber crimes he has stated that “it is very essential to emphasize that the world is not run by weapons anymore, or energy, or money. It is run by ones and zeros….little bits of data ….it is all electrons. There’s a war out here, a world war. It is not about who has the most bullets. It is about who controls the information – what we see and hear, how we work, what we think etc. it’s all about information.”[17] Further, he has critically analyzed the modus operandi of some important cyber crimes like cyber hacking, cyber terrorism, cyber pornography, cyber fraud etc. and also stated the national and international initiatives to prevent and control such cyber crimes.

S.K. Verma and Raman Mittal in their book “Legal Dimensions of Cyber Space”[18] have explained the basic concepts of cyber world like meaning, types, features and major components of computers; history and development of internet; merits and limitations of internet; various computer contaminants like virus, worms, Trojans etc. Emphasizing on the importance of computers and internet in day-to-day chores they have opined that “today it touches and influences almost every aspect of our lives. We are in the information age and computers are the driving force. We hardly do any activity that is not in some way dependent on computers.”[19] They further suggest that not only do we need to be computer-literate, but we also need to understand the myriad issues that surround our extensive and necessary dependence on computers. Commenting on the interlink of human-conflicts-law, they state that where humans are, crime and conflict of interests cannot be far behind, further, where crime and conflict of interests are, law must necessarily march in order to take control and regulate[20]. Thus, they have made a detailed study on the indispensable role of computer and internet, and the resultant cyber crimes.

Vakul Sharma in his book “Information Technology; Law and Practice”[21] has evaluated the issue of jurisdiction in cyber space. While discussing the role of international law in deciding jurisdiction of cyber offences he has made references to various principles like territorial principle, nationality principle, protective principle, passive personality principle, effects principle and universality principle[22]. Further, he has made deep insight into the controversial issue regarding extradition of cyber criminals[23]. Moreover, he has examined the US, European and Indian approaches towards personal jurisdiction at a greater length.[24]

Rodney D. Ryder in his book "Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet)[25] has exhaustively dealt with the provisions of the Information Technology Act, 2000 as amended in the year 2008. He has pointed out some grey areas of the Act and has also suggested the remedial reforms in order to provide more teeth and nail to the Act[26].

Articles

S.C. Agarwal in his article "Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements",[27] has stated that the law enforcement officials throughout the world are severely handicapped in tackling the new wave of cyber crimes. He has gone to the extent of saying that you "either have to take a cop and make him a computer expert or take a computer specialist and make him a cop."[28] He has suggested that we have to set up a Cyber Crime Investigation and Training Cell in all the States for imparting training to the police personnel, public prosecutors and judicial officers[29].

Abhimanyu Behra in his article "Cyber Crime and Law in India",[30] has discussed various types of cyber crimes and also suggested strategies to curb them.

A.S. Dalal "Jurisdiction in Cyberspace",[31] has elaborately examined the jurisdictional issue in trans-border cyber crimes and calls for an effective international regime to tackle the recently evolved cyber menace.

Miscellaneous

Websites

A number of standard websites such as those of Internet Corporation for Assigned Names and Numbers,[32] Indian Ministry of Information Technology,[33] World Intellectual Property Organization52 etc. were visited and consulted for information on various issues. A detailed list of the websites is given in the internet reference section of the bibliography.

Newspapers

Some national dailies like The Hindu, The Times of India, The Indian Express, The Tribune, The Hindustan Times etc. were also read for latest news regarding cyber crimes. Some other dailies of United States, UK and other countries, available online, also read for the latest updates on the research topic. A list of these dailies is given in the newspaper section of the bibliography.

Operationalization of Terms/Expressions

There are certain terms which have been used in the study. These terms have also been defined and explained in greater detail at the appropriate places. Unless specified otherwise, for the purposes of studies the terms described refers to the following.

Cyber Space

The term 'cyber space' was first used by William Gibson in his science fiction 'Neuromancer' in 1982, which he later described as "an evocative and essentially meaningless buzzword that could serve as a cipher for all of his cybernetic musings. Now it is used to describe anything associated with computers, information technology, the internet and the diverse internet culture. Thus, "cyberspace' is the electronic medium of computer networks, in which online communication takes place and where individuals can interact, exchange ideas, share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussions etc.

Netizen

Persons in cyberspace are called netizens i.e. anyone who is associated with computers, information technology and the Internet. Thus, a netizen is a person who becomes part of and participates in the larger internet society, which recognizes few boundaries save language. The term 'netizen' comes from the combination of two words 'Internet' and 'citizen'[34]. The number of netizens had jumped to 700 million in 2001 from a mere 143 million in 1998 and according to a UN report, world will have 2.7 billion netizens by the end of 2015 which is about 39 per cent of the global population were connected to internet and this number is increasing at a very fast speed every year. The report said that in the developing world, 31 per cent of the population are online, compared to 77 per cent in the developed world. Sub-Saharan Africa, where less than 20 per cent of the population is using the internet, remains the region with the lowest penetration rate. Further there are over one billion websites online[35].

Computer

The term 'computer' is derived from the word 'compute' which means to calculate. A computer is an electronic machine devised for performing calculations and controlling operations that can be expressed either in logical or numerical terms. It performs various operations with the help of instructions to process the information in order to achieve desired results. Further endless complex calculations can be done in mere fraction of time. Huge data can be stored without any space problem. Communication has become cheaper, faster and easier. Similarly difficult decisions can be made with unerring accuracy at comparatively little cost.

Today computers are widely seen as instruments for future progress and as a tool to achieve sustainability by way of improved access to information by means of video-conferencing and e-mail. Indeed, computers have left such an impression on modern civilization that we call this era as the 'information age'[36].

Networks

The value of a computer increases when it is connected to other computers. It is just like a telephone. If A has telephone then he can use his phone to call any of his friends provided all his friends have telephone. Hence, where his friends are not having telephone then it is useless for A to have telephone. Similarly, where A has computer it will be more useful for him in case it is connected to other computers. This connection among the computers constitute network. Therefore, a network is a collection of computers that are connected through a communication channel i.e., cables, fiber optics, etc. to share data, hardware and software[37].

Internet

The term 'Internet' is derived from two words 'interconnection' and 'networks'. Internet is a worldwide system of computer networks i.e., network of networks which allows the user to share information on those linked computers. It consists of thousands of separately administered networks of various sizes and types. Each of these networks comprises number of computers. LANs are connected by using public switched network to create a WAN and when number of WANs and other interconnected networks such as intranet and extranet are connected, it results in Internet. All computers connected to the Internet communicate to each other only by using a common set of rules which are known as protocol. For this communication, each computer should have its own address which is called as IP address[38].

The World Wide Web

The World Wide Web (abbreviated as WWW or W3, commonly known as the web), is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks. The web was developed between March 1989 and December 1990[39].

8.7 E-mail

It is the oldest application of the internet comprising exchange of digital information between two internet users. It is an asynchronous one-to-one communication. It is the most useful part of the internet and perhaps its greater boon. Letters across the seas taking days or weeks pass on to the other end of the world like a flurry though it is not always true and often a technical lacuna may delay it. The e-mail first was initially exchanged on the ARPANET to the FTP but it is now carried by Simple Mail Transfer Protocol (SMTP). In the beginning, it was "instant messaging "which required both the sender's and receiver's PC to be "on "position but now "store and forward" is more acceptable.

Critical Infrastructure

Critical Infrastructure (CI) is defined as an asset, system or part thereof located in a nation which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in that nation as a result of the failure to maintain those functions[40].

Cyber Crime

The new millennium brings new crimes. Cyber crime can be regarded as "computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks".[41] Cyber crime is a crime which committed by the criminals in a cyber environment using Internet, computer networks, and wireless communication systems as a tool or target. In other words, cyber crime involves crime committed through use of the computer. Department of Justice (DoJ) (1989) as defined cyber crime as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution".

Terrorism

"An act of terrorism, means any activity that (A) involves a violent act or an act dangerous to human life that is a violation of the criminal laws of the United States or any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; and (B) appears to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by assassination or kidnapping."[42]

Cyber Terrorism

Cyber terrorism is the use of electronic networks, and computer technology, as a weapon[43]. Attacks through the Internet need to have a terrorist component in order to be labeled "cyber terrorism." For the historical purpose, the word "cyber terrorism" was born in the late 1980s when Collin, a senior research fellow at the Institute for Security and Intelligence (ISI) in California,[44] coined this hot techno-phrase by combining two linguistic elements: cyberspace and terrorism.

The United Nations (UN) Counter-Terrorism Implementation Task Force (CTITF), although not explicitly using the term cyber terrorism, recognizes that one of the ways a terrorist organization may use the Internet is the "use of the Internet to perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems."[45]

The concept of 'pure' cyber terrorism is related to those terrorist activities that are carried out entirely (or primarily) - in the virtual world. The Internet provides many different ways of anonymously meeting with 'like minded' individuals in a (comparatively) safe way. Furthermore, a successful cyber terrorism event could require no more prerequisite than knowledge-something that is essentially free to the owner once acquired, and an asset that can be used over and over again.

Cyber Crime Cases Reported in India (2016-17)

CASE "A"

Victim complains that Rs.4.25 lacs have been fraudulently stolen from his/her account online via some online Transactions in 2 days using NET BANKING (BANK FRAUD).

CASE "B"

Victim complaints that his Debit/Credit card is safe with him still somebody has done shopping/ ATM transactions on his card. (IDENTIY THEFT)

CASE "C"

Victim complains that somebody has created a Fake Profile on Facebook and defaming her character with abusive comments and pictures. (CYBER STALKING)

CASE "D"

Somebody has posted all her information with Mobile No. on a Pornographic Dating Site and she is getting defamatory calls on her number.(CYBER STALKING)

CASE "E"

Somebody sent an Email from Income Tax Department and asked for all the bank information and after that 40,000/- has been fraudulently taken away from her account.
(PHISHING MAIL)

CASE "F"

A complaint that his/her Email Id is been hacked and messages for asking money has been sent to all his/her contacts. (EMAIL HACKING)

CASE "G"

Got an email that you are a lucky winner for a big amount of prize money and asked to deposit amount to claim that prize.(LOTTERY SCAM)

CASE "H"

A Corporate Complained that his crucial data has been stolen and has been misused against his organization. (DATA THEFT)

CASE "I"

Received a Email for a JOB Notification for a VERY BIG ORGANISATION and ask to deposit X amount and come for the interview with the Pay Slip. (JOB FRAUD)

CASE "J"

Somebody hacked into the Website and posted very defamatory content on his/her website. (WEB SITE HACKING)

RBS Bank Case

Complaint from Ms. Ekta that Rs.4.50 lacs have been fraudulently withdrawn from our account in two days and that she did not received any alerts on Mobile.

Investigation Started with BANK and Section 91 Crpc notice served to bank to furnish the details. As per bank details 341 transactions were done online from her account and also they provided the IP address and Merchant Name. IP Address were traced to ISP and details still awaited from the ISP. From the merchant – rechargeitnow.com the details were asked and as per there report around 20 BSNL PUNJAB CELL Numbers were reacharged with that amount. THE DETAILS of CELL Numbers are still awaited from BSNL PUNJAB.

Genpact BPO Case

We received a complaint from Mr. Vikas, G.M. H.R. of Genpact. It was mentioned that some unknown person is sending obscene mails to female staff working at the organization. We asked the complainant for email copy along with email header. After receiving the above header copy we checked for the IP address mentioned in the header part. Once we found the ISP's name we sent notice to the ISP to provide us the IP address detail. We got the email address which was used by the accused to send mails and it was found to be from rediffmail.com. We sent notice to the rediffmail.com to provide login, account creation and password change IP details. We received all the IP details from ISP and checked it at the APNIC site and found that it's from the same ISPi.e. Airtel. We received IP address detail from ISP, and it was done from a cyber café at Dwarka, Delhi. We called-up the cyber café guy to verify the given IP address details. We checked the register maintained by the cyber café owner and found the guy using internet. We got the phone number and name of the accused person. We called-up complainant to check their employee database and provide us those names who are residing at Dwarka, also asked them to check those who left the organization within a period of last 3-4 months. The above case was traced and the accused was found to be an employee of the complainant organization.

Job Fraud

A Email Received by the Victim which posed to be from Maruti Suzuki (info@marutisuzuki.com) (SPOOFED) that his resume has been shortlisted from a Job Site Monster.com for engineer at MARUTI SUZUKI PLANT offering him a salary of Rs.2.0 lacs /month. He has to deposit Rs.8,200 in a STATE BANK OF INDIA Account Number and come for the interview with the pay slip and also that it was said in the email that this amount is refundable. The Emails traced were from all foreign countries, and the BANK Account were also fake to which the money was deposited and the amount was immediately withdrawal from ATMs. The Criminal was also doing SMS and Phone Calls to the victim. The Criminal were traced with the help of MOBILE Calls and was arrested.

10. Expected Outcomes:

The world is changing very fast as the internet has grown exceptionally and gets space in our life. Dependence of human being on cyberspace for social, economic, governance, and security and other purposes has increased. At the same time the dimensions of computer-related crimes are also expended. Therefore, it is need of the time to adopt appropriate regulatory legal measures and gearing up the law enforcement mechanism to tackle the problem of cyber terrorism with stern hands. A slight delay in detection gives enough time to cyber terrorists to manage or delete or destroy the important data to evade detection. Very important point is that the peculiar nature of cyber terrorism provides safe zone to the terrorists and they never be face to face, as happened in traditional terrorist attacks.

This peculiar nature facilitates the terrorists to continue their terrorist activities without difficulty and even without the fear of any identification, arrest or prosecution. Therefore, a multi-facet and concerted approach of all law enforcement and IT experts is required to curb this menace in the cyber world.

So our cooperation is a key element in addressing the challenges of cyber security particularly exchange experiences and share best practices for protection of information infrastructures.

Bibliography

1. M. Zanini, & S.J.A. Edwards, "The Networking of Terror in the Information Age". *In J. Arquilla & D. Ronfelt (Eds), Networks and Netwars*, p. 30.
2. M. Zanini, & S.J.A. Edwards, "The Networking of Terror in the Information Age". *In J. Arquilla & D. Ronfelt (Eds), Networks and Netwars*, p. 45.
3. M. A. Sussmann, "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium." *Duke Journal of Comparative & International Law*, (2013) (9).
4. "Cyber Thieves are Caught, But Conviction is Wobbly", Hindustan Times, August 9, 2006, p. 18.
5. Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co. Pvt. Ltd., 2010.
6. A & M Records Inc v. Napster Inc, 114 F. Supp 2d 896(N.D. Cal 2000)
7. Kabushiki Kaisha Sony Computer Entertaining v. Stevens, 2002 FCA 906
8. MGM Studios Inc. v. Grokster Ltd., 545 US 193
9. Vivek Sood, Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 2010
10. Vivek Sood, Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 2010, P. 172
11. Vivek Sood, Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 2010, p. 173

12. Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, Central Law Agency Publication, Allahabad, 2010.
13. Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, Central Law Agency Publication, Allahabad, 2010, P.166.
14. Nandan Kamath, Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Universal Law Publishing Co., New Delhi, 2012.
15. Nandan Kamath, Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Universal Law Publishing Co., New Delhi, 2012, P. 52.
16. Dr. M. Dasgupta, Cyber Crime in India: A Comparative Study, Eastern Law House Publication, Kolkata, 2014.
17. Dr. M. Dasgupta, Cyber Crime in India: A Comparative Study, Eastern Law House Publication, Kolkata, 200p, P. 8
18. S.K. Verma and Raman Mittal, Legal Dimensions of Cyber Space, Indian Law Institute Publication, New Delhi, 2004.
19. S.K. Verma and Raman Mittal, Legal Dimensions of Cyber Space, Indian Law Institute Publication, New Delhi, 2004, P. 1
20. S.K. Verma and Raman Mittal, Legal Dimensions of Cyber Space, Indian Law Institute Publication, New Delhi, 2004, P. 2
21. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., New Delhi 2010.
22. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., New Delhi 2010, P. 251-53
23. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., New Delhi 2010, P. 257.
24. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., New Delhi 2010, P. 260.
25. Rodney D. Ryder, Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet), Wadhwa Publication, Nagpur, 2016.
26. R.K. Chaubey, An Introduction to Cyber Crime and Cyber Law, Kamal Law House Publication, Kolkata, 2009.
27. S.C. Agarwal, "Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements", pp. 4-11, CBI Bulletin, 2001 Feb.
28. S.C. Agarwal, "Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements", pp. 4-11, CBI Bulletin, 2001 Feb. P. 08.
29. S.C. Agarwal, "Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements", pp. 4-11, CBI Bulletin, 2001 Feb. P. 09.
30. Abhimanyu Behra, "Cyber Crime and Law in India", pp. 16-30, *Indian Journal of Criminology and Criminalistics*, 2010.
31. A.S. Dalal, "Jurisdiction in Cyberspace", pp. 37-56, M.D.U. Law Journal, 2010.
32. www.icann.org.
33. www.mit.gov.in.
34. Netizen is a person who is associated with the computer. Available on http://www.wisegeek.com/what-is-a-netizen.htm, Retrieved on 21 November, 2013.
35. "Total number of Websites, Available on http://www.internetlivestats.com/total-number-of-websites/., Retrieved on 21 November, 2014.
36. B.R. Sharma, Computer Crimes: Scientific Criminal Investigation, p. 27, Universal Law Publishing Co., 2006.
37. L.C. Amarnathan, "Crimes Related to Computer Network", p. 39, CBI Bulletin, February, 1999.
38. Chetan Srivastava, Fundamentals of Information Technology, p. 341, Kalyani Publishers, 2015.
39. "Inventing the Web: Tim Berners-Lee's 1990 Christmas Baby", Posted on November 24, 2010 by Eric Rumsey, Available on http://blog.lib.uiowa.edu/hardinmd/2010/11/24/inventing-the-web-tim-berners-lees-1990-christmas-baby/. Retrieved on 21 March 2012.
40. EC: Council Directive 2008/114/EC, of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the need to Improve their Protection, EC, Brussels, Belgium (2008).
41. D. Thomas & B.D. Loader, Introduction. In D. Thomas & B. D. Loader (Eds), Cybercrime: Law enforcement, Security, and Surveillance in the Information Age, p.-3, Routledge, New York, 2000.
42. (United States Code Congressional and Administrative News, 98th Congress, Second Session, 1984, Oct. 19, volume 2; par. 3077, 98 STAT. 2707 [West Publishing Co., 1984]).
43. J. F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, Citadel Press, New York, 2003.
44. B. Collin, "The Future of Cyberterrorism", Proceedings of 11th Annual International Symposium on Criminal Justice Issues: The University of Illinois at Chicago, 1996.
45. U.N. Counter-Terrorism Implementation Task Force, Report of the Working Group on "Countering the Use of the Internet for Terrorist Purposes", 8 (February 2009), Available on http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf. Retrieved on 30 June 2012.
46. Jitender k malik, CYBER CRIMES- POLICY IN INDIA, *International Research Journal of Human Resources and Social Sciences*, Volume 5, Issue 04, April 2018, 554-565.
47. Jitender Kumar Malik and Sanjaya Choudhury, Policy XZ. *International Journal of Recent Scientific Research*, Vol. 9, Issue 12(A) , December, 2018, pp. 29811-29814

****