HISTORICAL DEVELOPMENT OF ON-LINE CRIMES

Author's Name: Dr. Kshetrapal Singh

Affiliation: Assistant Professor, Department of Law, J.R.N. Rajasthan Vidhyapeeth, Udaipur, Rajasthan, India

E-Mail: riccikp@gmail.com

DOI No. – 08.2020-25662434

Abstract

In this present world of online processing, maximum of the information is available online and is prone to cyber threats. A huge number of cyber threats is being faced today and their behaviourur is difficult for early understanding. Therefore, it is very difficult to restrict in the initial phases of these cyber-attacks. All such attacks fall into the category of cyber crimes and they have serious impacts over the society in the form of economical disturbance, psychological disorder, social disturbances & threat to National defence etc. Restriction over these crimes depends on proper analysis of their behaviourur and understanding of their impacts over various levels of the society. Therefore, the present article provides the understanding of basics of cyber-crimes and their impacts over society with the future trends of cyber-crimes.

Keywords*: Cyber-Crime, Cyber Legislation, Cyber-Attacks, Interpole, Hacking*

INTRODUCTION

Today, in this world of technology we have left a great time in the past in which we have made growth in every field. Computers and internet are not the exceptions to it. Right from 1970's when the internet started its fame among the users to access to all the basic ideologies on it, since then crime started rooting its existence underneath it. Hence, before studying and researching on the subject like crimes through online tools it will be necessary to have a brief idea of crimes through computers. So, in this chapter it has been tried to look onto the progress of online crimes with timeline.

HISTORY OF CYBER LEGISLATIONS

In this segment, the historical development of cyber legislations globally has been explained. Right from the beginning, various seminars, conferences, and discussions started to place and as per the majority opinion legislation related to online crimes strengthened.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This was the first recorded cyber-crime.

Here are the some of the important areas on historical background on crimes through online tools which will focus on the timeline of such crimes.

THE PIONEERS

The fight against computer crime started very early and many individuals were engaged in this fight. The founder and father of the knowledge of computer crime by many observers considered to be Donn B. Parker, USA. He was involved in the research of computer crime and security from the early 1970's.

COUNCIL OF EUROPE

Council of Europe Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976 was the first place to conduct first international initiative on computer crime in Europe. Several categories of computer crime were introduced in this conference.

THE RIBIKOFF BILL

In the United States a staff study by the U.S. Senate Government Operations Committee in February, 1977 was the first comprehensive initiative on computer crime. Several problems associated with computer programs were addressed and recommended that legislation should be considered that would prohibit unauthorized use of computers. The Bill was not adopted, but this pioneer proposal raised awareness around the world as to the potential problems that unauthorized computer usage could cause many problems of the country.

INTERPOL

Interpol was the first international organization addressing computer crime and penal legislation at a Conference in Paris in 1979. The nature of computer crime is international, because of the steadily increasing communications by telephones, satellites etc., between the different countries. International organizations, like Interpol, should give this aspect more attention. The summary was the first step on the development of harmonizing penal laws dealing with computer crime around the world.

THE OECD RECOMMENDATION OF 1986

The OECD in Paris appointed an expert committee for deciding the need of penal provisions on cyber-crimes which was highly recommended. Various important issues were noted and all the member country started their efforts to make penal legislation at national level. Therefore, the recommendation was highly emphasised.

THE COUNCIL OF EUROPE RECOMMENDATIONS OF 1989

Another expert committee discussed on legal issues on computer related crimes in 1985 and a summary of guidelines were issued to take national initiatives. It included a minimum list of computer fraud, computer forgery, damage to computer data or computer programs, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer program and unauthorized reproduction of topography.

THE COUNCIL OF EUROPE RECOMMENDATIONS OF 1995

The Council of Europe adopted on September 11, 1995, another Recommendation concerning problems of procedural law connected with Information Technology. This Recommendation introduces 18 principles categorized in 7 chapters: search and seizure; technical surveillance; obligation to co-operate with the investigating authorities; electronic evidence; use of encryption; research; statistics and training; international co-operation.

G-8 GROUP OF STATES

The High-Tech Subgroup of the G-8's Senior Experts on Transnational Organized Crime developed and established in 1998 a 24-hour, seven-day network of experts to assist in high-tech crime investigation. The goal was to ensure that no criminal receives safe haven anywhere in the world, and that the law enforcement authorities have the technical ability and legal process to find criminals who abuse technologies and bring them to justice. Other countries have joined the network and are participating in the co-operation. The G-8 Group has also agreed upon principles that should apply when law enforcement agents employed by law enforcement agencies are investigating criminal offenses and require assistance in other countries. Such principles should be implemented through treaties and through national laws and policies.

These were the international steps taken for the fight against online crimes but the criminals were always a step ahead and the new mode of committing crime was discovered on routine basis. Some of the examples are as mentioned –

- Cyber-crime began with attacking PCs (Personal Computers) at home because of popularity and accessibility of PCs (Personal Computers) for home users. The most common cyber-crimes during this time were phishing scams, cyber stalking, computer viruses, and identity theft.
- As the years went on crimes like cyber stalking and harassment also became far more popular. School kids began to take advantage of the Internet to taunt their classmates and adults would stalk and harass those they also stalked in real life via the internet.
- Cyber-attacks grown more frequent and destructive afterwards. One form of hacking the Denial-of-Service (DoS) attack has apparently even become a tool of war. The attacks are designed to paralyze websites, financial networks and other computer systems by flooding them with data from outside computers.
- Cyber spies are also targeting regular citizens. News headlines regularly tell of hackers ransacking computer networks for Social Security numbers, banking information and other data that could be used for potential identity theft.

Therefore, the abovementioned steps were taken during the sitting and discussions of this summit. This was one of the unique steps taken in the history in order to achieve cyber free environment at large level.

SOME FAMOUS HISTORICAL CASES OF COMPUTER CRIME

The two Incidents have been considered as **black lettered incidents** in the history of online crimes, because they were the first known crimes in this field by which little or more loss was caused to the society. They can be seen in the brief as follows:

- *Compromising of Milnet, 1986* - The sensitive military information of Soviet was hacked and stolen. Internet security and data protection became a top priority among the users thereafter.
- *The Morris Worm, 1988* – A worm was created by Morris to impress his friends but it caused a massive destruction and caused millions of dollars in damage before its removal. He was convicted for it.
- *Crash of AT & T 1989* - This was another incident which occurred due to fault of the technician of the organization itself and caused a huge loss.

  Apart from these, there are many crimes which can be seen as famous historical online crimes.

A brief study is as under –

Hacking

Hacking means to enter into the database information system of another's computer without his knowledge. There are number of cases on hacking out of which a few examples are mentioned here which are seen as historical events.

Internet time theft

It means the usage by an unauthorized person of the Internet hours or data which is paid for by another person.

- In May 2000, the economic offences wing, IPR (Intellectual Property Rights) section crime branch of Delhi police registered its first case involving theft of Internet hours. In this case, the accused, Mukesh Gupta an engineer with Nicom System (P) Ltd. was sent to the residence of the complainant to activate his Internet connection. However, the accused used Col. Bajwa's login name and password from various places causing wrongful loss of 100 hours to Col. Bajwa. Delhi police arrested the accused for theft of Internet time theft.

  On further inquiry in the case, another accused was arrested who had used Col Bajwa's login and passwords as many as 207 times from his residence and twice from his office. He confessed that Shashi Nagpal, from whom he had purchased a computer, gave the login and password to him.

  The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber-crimes.

  The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested Krishan Kumar under sections 379, 411, 34 of Indian Penal Code, 1860 (IPC) and section 25 of the Indian Telegraph Act. *However, no charges were framed under INFORMATION TECHNOLOGY Act, 2000 as there was no provision foe such online crime.*

  This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.
- In another case reported in USA there was a hobby website for children, which was hacked and a ransom of $1 million was demanded through email for de-hack the website. But the owner of website ignored the threat and afterwards she came to know that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'.

  Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

Logic bomb

A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples in this field. These programming techniques caused great destruction to the database and information is distracted.

Computer Piracy through Malware

Computer "Pirates" Steal Intellectual Property. They also harm your computer by installing viruses or spy ware, or allow others to access the files contained on the hard drive beyond those we intend to share.

- Punjab National Bank was cheated to the tune of Rs. 1.39 crores through false debits and credits in computerized accounts by misappropriation of funds by manipulation of computer records. In another case, Rs. 2.5 lacs were misappropriated from Bank of Baroda through falsification of computerized bank accounts.
- In April 2001, the Hyderabad police arrested two persons, namely, Manohar, an unemployed computer operator and his friend, Moses who was a steward in a prominent five-star hotel in the city. They were arrested and charged under various sections of the IPC and the IT Act for stealing and misusing credit card numbers belonging to others.

Online Retail Fraud

This fraud means cheating or misrepresenting through online auction sites & misappropriates funds of users.

- One approach to retail fraud has involved placing banner advertisements on an auction site that offers the same types of goods being auctioned. Prospective buyers who click on the banner advertisement are taken to a different website that is not part of the auction site, and that offers none of the protections that leading auction Websites have adopted for their members.
- Another approach involves using unsolicited commercial e-mail ("spam") to lure prospective victims to a website which purports to sell items of the same type that are available through well-known online auction sites. In a variation of this approach, the criminals send counterfeit merchandise in place of the promised merchandise.
- A third approach involves the criminal contacting losing bidders in a particular online auction, informing them that additional units of the item on which they bid have become available, and taking the bidders' money without delivering the items.

Online auction fraud typically involves several recurring approaches. The most common approach appears to be the offering of some valuable item, such as computers, high-priced watches, or collectible items, through a known online auction site. The individuals who are informed that they are successful bidders send their money to the seller, but never receive the promised merchandise.

Pump-and-Dump

The most widely publicized form of online market manipulation is the so-called "pump and dump" scheme. In a "pump and dump," the companies whose stock is thinly traded is identified by criminals, and then adopt various means to persuade individual online investors to buy that company's stock. These means can include posting favorable, but false and misleading, representations on financial message boards or Websites, and making undisclosed payments to people who are ostensibly independent but who will recommend that stock.

Once the price has increased sufficiently, the participants in the scheme -- who may be company insiders, outsiders, or both, sell their stock, and the stock price eventually declines sharply, leaving uninformed investors with substantial financial losses. While an outsider who merely expresses his opinions about the worth or likely increase or decrease of a particular stock may not be committing criminal fraud, outsiders or insiders whose conduct extends beyond mere advocacy to manipulation of markets for their personal profit by giving the public false and misleading information may violate securities fraud statutes and other criminal statutes.

Cyber smear

It is the opposite of the "pump and dump". A "cyber smear" scheme is organized in the same basic manner as a "pump-and- dump," with one important difference: the object is to induce a decline in the stock's price, to permit the criminals to realize profits by short-selling, to accomplish a sufficiently rapid decline in the stock's price. The criminal must resort to blatant lies and misrepresentations likely to trigger a substantial sell off by other investors.

Email bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Data diddling

Data diddling means entering raw data before processing and changing it back after processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

Salami attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

Cyber Pornography

This would include pornographic websites; pornographic magazines produced using computers and the Internet (to download and transmit pornographic pictures, photos, writings etc.

Sale of Illegal Article

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. E.g., many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'. Such cases are historical in themselves.

Online Gambling

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Cyber Defamation

This occurs when defamation takes place with the help of computers and/or the Internet. E.g., someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Harassment

Internet harassment includes directing obscenities toward others, as well as making derogatory comments based for example on gender, race, religion, nationality, sexual orientation. This type of Internet crime can take place often in chat rooms, through newsgroups, and even through the sending of hate email to targeted mailing lists. Unsolicited email messages and advertisements can also be considered to be forms of Internet harassment where the content is offensive or of an explicit sexual nature.

Virus Builders

Viruses' incidents have resulted in installing Trojans, worms, virus, etc. There are many simple ways of installing a Trojan in someone's computer.

CONCLUSION

Hence, it can be concluded that the historical aspect of online crimes, though cannot be claimed as a matter of fact, but yet, it is evident from the facts available that online crimes have their existence right from their use. Initially, when the software was designed for welfare and facilitation, then at the same moment their misuse and criminal activities were also started. The historical aspects and the crimes discussed above are only illustrative and not exhaustive, because there were many such other similar crimes which were in existence and occurred but not put on record due to initial unknowingness or any such other thing.

REFERENCES:

[1] http://www.bezaspeaks.com/cybercrime/history.htm
[2] An overview of his archives visited on www.cybercrimelaw.net, "Computer Crime" (1976). https://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf
[3] Ahmed Farookh, Cyber Laws in India – Law on Internet, II edition, Pioneer Books, 2005
[4] A Paper for the 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic. https://cybercrimelaw.net/documents/Strasbourg.pdf
[5] http://www.scribd.com/doc/83073623/Cybercrime-History
[6] Computer-related criminality: Analysis of Legal Politics in the OECD Area (1986)
[7] Computer-related crime: Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems. (Published in Strasbourg 1990)
[8] Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995,
[9] G-8 consists of the following States: Canada, France, Italy, Japan, Russia, United Kingdom, Germany and USA. See www.g7.utoronto.ca
[10] http://www.brighthub.com
[11] http://www.time.com/time/nation/article/0,8599,1902073,00.html
[12] http://www.indiaforensic.com/compcrime1.htm
[13] Dr. Farooq Ahmed, Cyber Law on Internet
[14] http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Cybercrime.doc
[15] S.C. Agrawal, Computer Ethics, Child Sexual abuse, pornography and regulation of child pornography with Internet
[16] http://www.nashikruralpolice.gov.in/CyberCrimeCell.html.