ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

'Chronology of cyber crime First phase of history of cyber crime before 1960s"

Dr. AAYUSHI PAREEK
Assistant Professor Government Law College ,Churu

The aggregation of information and mechanical cryptography system may be dated back more than 5,000 years. Since ancient times, a country's information n system has influenced its foreign attack and military system. An Egyptian has employed the method of encryption and decoding of information from 1900 BC.[i] *In order to guarantee information security, Julius Caesar employed a standard alphabet in official communications from 100 to 44 BC. This phrase, a bilateral cypher, 5-bit binary encoding, was earlier described as a cypher by Sir Francis Bacon in the year 1623. He has enhanced a 5-bit binary encoding as stenographic device by exploiting variation in type face to carry each bit of the encoding. In the 1790s, Thomas Jefferson designed a wheel cypher, which was later modified as the strip cypher, M-138-A, which was used by the United States Navy during World War II. Since the 1870s, the history of hacking may be traced back to the usage of spanking new telephones by teenagers for phone phreaking. William Frederick Friedman was the primary code-breaker of Japan's World War II purple machine, as well as the father of crypto-analysis in the United States. In 1918, he published a treatise on cryptography, which is still used to prevent and regulate cybercrime today.*[ii]

The United States Federal Bureau of Investigation (FBI) was established in the 1920s and 1930s as an office dedicated to combating criminals' use of encryption. According to Mrs. Elizabeth Friedman in the 1930s, "... a complication never even attempted by any Government for its most secret communications... At no time during World War II, when covert techniques of communication were at their pinnacle of development, were they employed in such intricate ramifications as are to be seen in some of the connections of West Coast rum running vessels."

From the 1950s, men's magazines such as Play-boy and Modern Man in the United States depicted nude, semi-nude women participating in sexual activities, which were then copied as pornographic publications.[iii] Before the 1920s, "Tijuana bibles" debuted in the United States as a pornographic comic book. In the late 1950s, a new electronic medium known as information technology emerged. Because of the evolution of computers, a new computer crime problem arose with the pessimistic outcome of new Technology problems, which would also preserve information that is stored in computer as well as in their system data base and to avert and manage Cyber Crimes such as cyber theft, illegal contact with computer, systems, and devices, and so on.

SECOND PHASE OF HISTORY OF CYBER CRIME IN THE 1960S

People who were interested in telephone phreaking in the early 1870s became hackers in the 1960s. Telephone phreakers were also curious about the computer, computer system, and how to utilise it and its operations for their own purposes. Cyber Crimes were dedicated in the early stages of information technology by incredibly knowledgeable technology specialists who had the authority

to utilise this new technology, and this was the primary distinction, for example, programmers, engineers, and administrators with new technological expertise.[iv] In 1960, the artificial intelligence laboratory at the Massachusetts Institute of Technology (MIT) became a playground for hackers. At the time, the word "hacker" was a good one, and only computer specialists with advanced technological understanding were involved in these activities. The Digital Equipment Corporation (DEC) created and trademarked the programmable Data Processor (PDP-I) in 1960.[v] This was the initial computer that was used for commercial time sharing for businesses, schools, labs, and programmers in exchange for rent to the computer's owner.[vi] As a result, they have opened the door for hackers to play with data or information sharing in the vulnerable cyber world.

In the year 1966, cyber crooks plundered a Minnesota bank using new information technology. Two employees at Bell Laboratory created UNIX, a novel operating system. UNIX is viewed as one kind of hacking that makes use of new technology. Dennis Ritchie and Kene Thompson were two of the company's workers. As a result, the procedure of using MIT's computer was figured out by the Stewart Nelson was the phreaker who created telephone tones in order to communicate with telephone companies' long distance services. Some of the phreakers employed the procedure of whistling a blue box to recreate a frequency of 2600 Hz.

THIRD PHASE OF HISTORY OF CYBER CRIME IN THE 1970S

Since 1970, the cyber world and network have been accessible to clients all around the world. By that time, cybercrime had grown into a legal controversy that was referred to as cyber pornography across the world. Boxes with a whistling case In the year 1970, John Draper established a precedent for telephone tampering. He was considered for national semi-conductor as a veteran of the United States Air Force and an engineering technician. He went under the moniker cap'n crunch. He invented the cap'n crunch cereal boxes whistle, which can duplicate a tone of 2,600 megahertz, in 1971 in Vietnam, and he evolved it such that phreakers could make free calls at the time by blowing the whistle into a telephone receiver. The accused John Draper used to make a free long-distance call into a phone by blowing a certain tone. They used to report to the telephone system to discharge a line or link with a line by using this particular tone. At the time, most youths were driven to engage in telephone tampering and phreaking. Magazines and technical aid programmes that printed the method of tampering and telephone phreaking instilled confidence in teenagers.[vii] Whitfield Diffie and Martin Hellman proposed the use of public key cryptography to implement security standard software to detect and regulate computer abuse in 1976. Ronald L. Rivest, Leonard M. Adleman, and Adi Shamir presented software for public key cryptography and digital signatures in the United States in 1977. The word hacker and hacking became known among Russians through Weizenbaum's 1976 book, despite the fact that the general audience was distant from this notion for a different half of a decade, till the 1980s. By the end of the 1980s, they had not even heard of personal computers (PCs). As a result, programmers and hackers in Russia were linked to computer centres and cyber cafés at the time. To create a brand name, they used to work closely together, for example, IBM, DEC, operating system, and software packaging. The Hackers made use of programme code. In the late 1960s and early 1970s, the Russian government employed such programmes for security measures.[viii]

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

FOURTH PHASE OF HISTORY OF CYBER CRIME IN THE 1980S

In the early 1980s, hackers were imprisoned for roughly 60 computer break-ins from Memorial Sloan with Kettering worry centre, who were planning an attack on Los Alamos National Laboratory. Furthermore, in the late 1980s, the Comprehensive Crime Control Act was adopted in the United States allowing secret service authority over computer trickery and credit card information. Two hacking groups were formed during this time period. The first is the Legion of doom in the United States, while the second is the Choose Computer Club in Germany.

In the early 1980s, they discovered 2600 Hackers Quarterly, which shared telephone phreaking and computer hacking tips. The first National Bank of Chicago was named after the victim of a $70 million computer hacking. Not only did a law enforcement agency investigate an Indian hacker known as "fry man" for breaking into McD's information. In the 1980s, the most famous hacker, Kevin Mitnick, was accused of causing computer damage and stealing software and was sentenced to one year in jail for secretly monitoring the e-mail of Mild cognitive impairment (MCI) and Digital Equipment Security. Furthermore, if we talk about this age, the ROT13 USENET groups programme was established in this era to avoid screening of "objectionable information by innocent eyes," because by that time, cyber pornography and cyber terrorism had taken on its own shape due to new communication convergence technology.[ix]

In the year 1983, a court trial was started against a computer programmer for causing a break on an assembly line and was prosecuted in the USSR. In the beginning of 1985, the idea of hackers and hacking became quite prominent among teens and school-age children in Russia, and by 1987, mass media began reporting about hacking, and it became a hot topic in the country Russia. In the USSR, Komsomolskaya Pravda reported in December 1987, "A hacker is assumed to be synonymous with a computer criminal who obtains unlawful access to distant archives and databases in order to whip secret data, and primarily money from bank accounts and credit cards; as we know, hackers are smart at mathematics and information technologies, they are mostly outside politics, but being computer hooligans, they may be susceptible to exploitation.".[x]

For the implementation of law, which was a burning and exceedingly complicated subject at the time, when there was no defined jurisdiction and territorial scope. Until 1977, there was no statement on computer-related crime in Russian criminal law. In Russia, cyber police caught a number of hackers for hacking using a computer as well as a telephone, mobile phone, and crimes involving credit cards and SIM cards.

FIFTH PHASE OF HISTORY OF CYBER CRIME IN THE 1990'S

The Computer Fraud and Abuse Act was passed in 1984, and it deals with illegal activities in the judicial system of the United States. The same Act was updated in 1994 and modified in late 1996. This Act prohibits illegal access to computers as well as the commission of surveillance, unauthorised access to non-public government systems, computer fraud, computer damage, password trafficking, and threats to harm a computer. The Computer Emergency Response Team was also established by US defence departments in the late 1980s. Its primary objective was to study the rising amount of assaults on computer networks.

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

While praising the fundamental merits of technology is not difficult, its negative impact on legal standards has been unpleasant. The so-called "Year 2000 Y2K issue, also known as the Millennium Bug, first observed society's reliance on information and is now at its pinnacle as it rises day by day. As a result, this was regarded as the primary issue that received significant attention in both the IT industry and the media in the year's first beginning of 2000, "This is not regarded as a narrative of computer fault and abuse, but it is symptomatic of a society in which Cyber Crime could have a significant impact." All of this was done in preparation for the departure of a terrifying force on law, which can be defined as an embodiment for a certain policy and system intended to broaden fortification towards the rights of persons in a cultured society. It is seen as a protective canopy beneath which individuals feel safe and secure.

Modern technology has also advanced. The traditional nature of criminal law has been broadened by contemporary technology, which has assisted in the creation of goods that are fundamentally regarded harmful. The 'offences of hazard,' or the employment of such tools, are no longer limited to the sphere of tort law, but have abruptly expanded into a new area of criminal law. Elegant, robust, and multipurpose are all characteristics of the Internet, which also has the property of being inoffensive.

Criminal cosmopolitanism, evisceration of legal standards, and enmeshing it with technology improvements are supplied for the basis of laws. Technological streaks have sent shivers down the legal corridors; while the jurist is perplexed, the judge is perplexed. Despite the fact that the computer sector is thriving and the internet is developing, the legal actions are not promising. Throughout the early days of the telegraph and telephone, their governance by law was not considered as a major obstacle, but rather as a matter of practicality. The Internet Age has been characterised by imperceptible characteristics, and as a result, there is a direct influence between the two realms, which are recognised as the legal and the technological. Connectivity is not at a standstill. While technological extravaganza is unending, the Internet provides to insert information that is more appealing to the average user, who is weaker and more gullible. As a result, this is seen as the reason why more and more individuals are utilising the Internet at a faster rate. Tim Berners-assertion Lee's that the semantic web would eventually demand "freedom of expression" with reference to computers has shed light on the argument that technical advancements necessitate a legal shift. The "human" aspect of the Internet cannot be ignored; until the two worlds reconcile, or the obduracy of legal dictums is loosened, or boorish online behaviour is brought within the legal Web, these two worlds cannot live happily ever after.

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

ENDNOTES

[i] shiren Herbert, "A Brief History of Cryptography" web publication, National Crypto Logic Museum website.

[ii] Jain N.C. (2008) "Cyber Crime" Allahabad Law Agency, Faridabad, Haryana.

[iii] Jaishankar K. (2011) "Cyber Criminology-Exploring Internet Crimes and Criminal Behavior", CRC Press, New York.

[iv] Kumar Vinod, (2003) "Winning the Battle against Cyber Crime", A.P.H. publishing corporation, New Delhi.

[v] Sharma, Vakul(2007) "Information Technology - Law and Practice", Universal Law Publisher Company, Delhi.

[vi] Reviewing the History of Cyber Crime http://www.syngress.com/book_catalog/225Cyber Crime/ sample.pdf/History of Cyber Crime, qxd 7.16.18, 4:08 p.m., p.52.

[vii] Stephenzon, Peter, (2000) "Investigating Computer-Related Crime", CRC Press, New York.

[viii] Nandan, Kamath (2009) "Law relating to Computers, Internet and E-Commerce", Universal Law Publication, Delhi.

[ix] Tanenbaum, S. Andrew, (2008) "Computer Networks", 7th edition, Prentice Hall of India Private Limited, New Delhi.

[x] D. Thomas and B.D. Loader: Cyber Crimes, Law Enforcement, Security and Surveillance in the Information Age, Hackers (United Artists, 1995), p.59.