Journal of Advances and Scholarly Researches in Allied Education
Vol. 17, Issue No. 2, October-2020, ISSN 2230-7540

To study about the conceptual analysis of cyber-Crime

Richa Tiwari[1]*, Dr. Ganesh Dubey[2]

[1] Research Scholar, Jiwaji University

[2] HOD, Institute of Law, Jiwaji University

Abstract - The majority of economic, commercial, cultural, social, and governmental activities and contacts of nations are now conducted in cyberspace at all levels, including people, non-governmental groups, and government and governmental institutions. Cyber-attacks and the hazards of wireless communication technologies are now a concern for many business organisations and government bodies throughout the world. In today's society, which is largely dependent on electronic technology, protecting data from cyber-attacks is a challenging undertaking. Businesses suffer financial losses as a result of cyber-attacks. In some circumstances, cyber-attacks might be utilised for military or political purposes. PC viruses, knowledge breaks (DDS), and other attack vectors are examples of these damages. To achieve this purpose, a range of tactics for mitigating the impact of cyber-attacks are used by many firms. Cyber security is built on the most up-to-date IT data in real time.Until date, scholars from across the world have proposed a range of strategies for avoiding cyber-attacks or minimising the damage they do. Some of the methods are now in use, while others are still under investigation. The purpose of this study is to look at the challenges, weaknesses, and strengths of the various techniques as well as to evaluate the current state of cyber security.

Keywords - Information technology, Cyber-attacks, Cyber security, Emerging trends, Key management

----------X----------

1. INTRODUCTION

The Internet and network computers have provided the greatest threat to judicial systems throughout the globe in the second industrial revolution of the 21st century. New crimes are brought on by the new revolution. For three reasons, cyberspace is a special haven for crooks. To begin, the use of computers and other technology is a more cost-effective way to commit crimes. Second, the typical perpetrator-victim dynamic is complicated by cybercrime's inclusion of new players. There are three reasons why law enforcement organizations may never be able to locate criminals.

The expansion of the information technology industry has become a vital part of the global economy's infrastructure. E-highways are helping to fuel the growth of this century, as well as contributing to different socioeconomic aspects such as employment and the quality of living and variety of people's lives via numerous forms. There is little doubt that information technology (IT) is a major factor in India's rebranding as a global technology and business services provider. Information technology-based goods and services have become more popular in the United States because of government support for their use.The Government of India has set up a National Task Force on IT and Software Development to study the viability of boosting the Indian IT sector in order to elevate and promote it. The world's software sector has relied heavily on venture capital funding. To help the business grow, regulations governing the operation of venture capital funds have been liberalized in accordance with worldwide best practices. Public services, healthcare (mobile clinics), education (e-learning and virtual classrooms), as well as services in the financial sector(mobile banking and payment gateways) have all benefited from the company's use of IT.

Most breakthroughs and improvements have a propensity for human beings to look out the negative aspects of them. Using simple, fast, and high-quality gadgets is a great way to enhance our life today's technology advancements. Terrorists might potentially utilise these new technology advancements as weapons of mass destruction. Internet service providers (ISPs), such as America Online, play a major role in cybercrime. Criminal action may be made more costly by third parties, who may be able to do so in ways the government cannot. Third, there are a slew of tricky issues that emerge due to the fact that most online actions are hidden from third parties and, in some cases,

even from second parties.So, cyberspace provides thieves with a safe and murky area in which to carry out their nefarious plans without really being present at the target location. The history of computer, internet, and cybercrime should be studied. A chronology of computer, internet, World Wide Web, and cybercrime is provided in the next section.

For each year that passes, more crimes emerge. Internet, computer networks and wireless communication technologies are used as tools or targets by cybercriminals to perpetrate cybercrime. One definition of cybercrime is the use of computers and worldwide electronic networks to perpetrate criminal activity deemed unlawful or illegitimate by certain parties. To put it another way, cybercrime is a kind of crime performed via a computer.

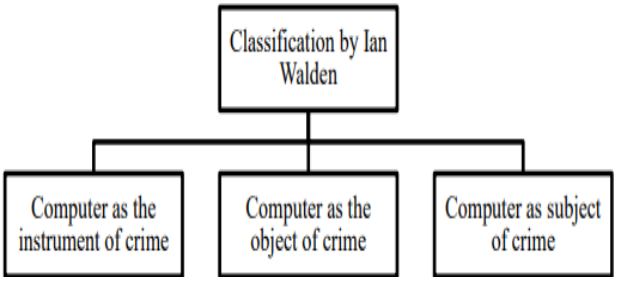
“The internet's roots may be traced back to the end of the 19th century, when the first electrical devices were developed and the first communication systems were invented. Telephone patents were issued in 1876 by Graham Bell after lengthy inventories that spanned over 100 years. More than a century later, this may be considered the seedling he planted for the fast-moving telephonic worldwide communication system that exists today. Today's communication environment is made up of both voice communication (as in the past) and data transfer (like with fax machines and computers). There are several periods in the development of communication and the internet's history.

2. CHARACTERISTICS OF CYBER CRIMES

Because of the anonymity of cybercrime, it often goes unreported. Encryption is the most often used tool for facilitating anonymity. In order to do business via the internet, businesses and consumers alike have grown to rely on encryption. The FBI has long expressed alarm about the growing use of encryption technology, claiming that it might have a disastrous effect on criminal investigations. They can hack/attack computers in various regions of the globe in a nanosecond. As the name implies, cybercrime takes place away from a physical location. Detection begins with locating the crime scene in the conventional sense. However, cybercrimes are not limited to a single location. A hacker in the United States may use software to break into a computer in China or Delhi and transfer money to an account in Australia.

An old-fashioned cop will have a hard time figuring out where the crime scene is and may even dispute if there is one at all. Cybercrime has no geographic boundaries. It has the ability to cross state and national borders in a matter of minutes. Computer crime has a broad operating scope, and the criminal disregards national boundaries. The whole economy of another country may be wiped out from the comfort of one's own country. In a network crime, the whole globe may constitute the crime site, making traditional conceptions of jurisdiction in criminal investigations obsolete.The victim is not completely destroyed by conventional crimes, despite the fact that they may do great harm to him. In bank robberies, for example, the amount of money that can be stolen limits the amount of money that can be stolen. The bank's activities will continue despite the amount buried. Since it is possible to take appropriate preventive steps and upgrade the security of the bank, the odds of another heist at this location are rare. Also, there isn't much of a loss in terms of reputation. On the other hand, in the case of computer crimes, the consequences might last for a long time and the damage is not limited to a single incident. It has the potential to paralyse the sufferer and, in most circumstances, permanently disfigure them. It's the loss of clients, not the monetary damage that would be the real death blow for any company whose primary business relies on electronic trade, or e-commerce. Because of a few mouse clicks, clients would lose confidence in the vendor, and all of their efforts to build that trust would be wiped out.

Cybercrime is interpreted in a variety of ways by different thinkers. Each of them is aware of the computer's involvement in cybercrime, but they classify the offences differently. According to Ian Walden, there are three types of cybercrime using computers. To paraphrase him, a computer may be used as an instrument of crime (as in murder and fraud) or an object of crime (as in the theft of processor chips) or it can be both.

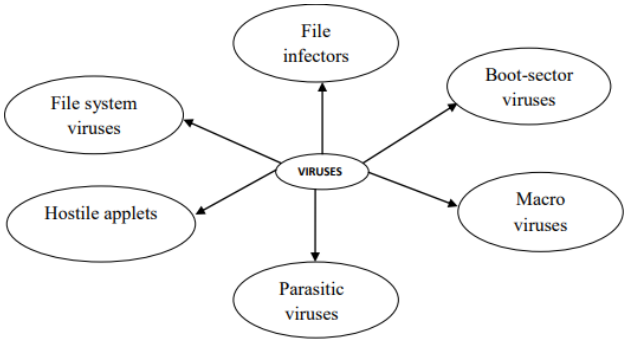


In his book, Walden discusses a number of English criminal offences in which computers have a role. Fraud, for example, falls under the first category of these crimes, which are referred to as computer-related crimes. Intellectual property and pornography are two examples of crimes that fall under the second heading, "content-related." The third type of offences is referred to as "computer integrity crimes," and they are designed to protect the integrity of computer and communication networks. A typical high-tech crime is one of these. D. S. Wall, another thinker, identified three types of computer-related crimes in 1998. "Traditional criminal acts" have been facilitated by computer networks in the first category, he says. "Every crime has the moved or has been re-engineered to operate online" according to this definition.

2.1 Unauthorized Access to Computer Programs and Files

- **Virus**

Virus or Source of Critical Information? In essence, Under Siege is a piece of software designed to do harm. 'computer virus' was coined in 1986 by Dr. Fred Cohen, who refers to viruses that spread by attaching themselves directly to computer programmes in a thesis published that year. Computer users are required to have a rudimentary understanding of how viruses operate in order to protect their systems from being infected.It is possible for a virus to show a message on the screen or knock down the infected computer system. In other words, it has the potential to cause harm or disruption. To get into action, most viruses need an activation mechanism. There is a possibility that they might go unnoticed for a long time. Most of the time, it's waiting in the computer's memory to infect the next software or disc that's opened.



- **Password Cracking**

During a login session, all systems save cached passwords in memory. Since hackers have access to all the system's memory, they may be able to search through it for passwords. In the same way, passwords may often be found by sifting through page files. In order to crack a password, one must decode a password or break through a security system. Passwords may be cracked using a variety of methods, including brute-force attacks, dictionary attacks, and brute-force attacks.

- **Trojan**

The name ‘Trojan’ takes its genesis from the Greek storey of the ‘Trojan Horse’. Greece launched war on Troy in the 12th century BC. When the Prince of Troy kidnapped the Queen of Sparta and announced that he intended to marry her, a rift developed between the two nations. The Greeks were understandably enraged, and for the next 10 years they waged an unsuccessful siege on Troy, which was well-defended. As a final option, the Greek Army left behind a massive wooden horse, pretending to be retiring. They hauled the horse into Troy, believing it was a gift from the Greeks, but what they didn't realize was that the horse was really hollow, and within were some of the greatest Greek troops. The troops sneaked out at night, unlocked the city's gates, and later, together with the rest of the Army, slaughtered Troy's whole army. Similarly to a wooden horse, a Trojan horse software seems to be performing one thing while really doing another.

3. CAUSES OF CYBER CRIME

3.1. Data Storage Capacity in a Small Area

The computer has a unique ability to store data in a relatively tiny amount of memory. This makes it much simpler to delete or derive information, whether on a physical or virtual media.

3.2 Complex

There are millions of lines of code in the operating systems that computers use, and the human mind is prone to error, so the cyber thieves use these omissions to infiltrate the computer network and steal sensitive information from users.

3.3 Easy to Access

If you have a basic understanding of computers, you can hack into other people's computers, even if you're insane. The difficulty in preventing unwanted access to a computer system comes from the fact that the complicated technology used to protect the system leaves little room for human mistake. It is possible to get around many security systems by using hidden logic bombs, key loggers, sophisticated voice recorders, retina imagers and other devices capable of fooling biometric systems and evading firewalls.

3.4 Loss of Evidence

Evidence may be easily destroyed in today's internet age, particularly in cases of cybercrime. Data destruction makes evidence loss a widespread and evident concern. This method of criminal investigation is paralyzed by the collecting of data outside of the geographical reach. When it comes to dealing with incidents of cybercrime, the typically trained police officers are worthless.

3.5 Motivation

For criminals in the past, learning a complicated system was a source of motivation; nowadays, however, criminals are motivated by money, hunger for power and vengeance, as well as adventure. Criminals are motivated by the desire to inflict harm or retribution.

i. **Affordability of Goals**

Many cyber thieves are driven by a desire for financial gain, especially when the risk of punishment is lower. Many cyber criminals are motivated to carry out malware, phishing, identity theft, and fraudulent money request assaults because of the perceived low risk and big payoff.

ii. The Second Type of Motivating Factor

As a result of the firms' refusal to contribute to hacktivist organisations, cyber-attacks are more likely. Companies' servers were rendered inaccessible to Internet users as a result of an anonymously coordinated series of boot assaults. These sorts of assaults are carried out to convey complaints against people, firms, organizations, or even national governments by destroying or disabling computer equipment and networks.

3.6 Negligence

Detriment is a direct result of carelessness. Because of this, it is highly likely that while defending the computer system, a cybercriminal may be able to get access and control over the computer system via neglect.

3.7 Opportunities

Increased criminal opportunities are being created by vulnerabilities in information technology that are being exploited by the growth of computing capabilities in financial services, securities, air traffic control, telephony and electric power. These advancements have reduced costs while enabling revolutionary changes in business, communication and entertainment as well as education.

3.8 Poor Response from Law Enforcing Agencies

Many nations in the poor world do not have enough laws in place to combat cyber-attackers. Since of this, criminals are able to avoid sanctions because they are far away and difficult to locate.

3.9 New Challenge - Cyber Crime

People in the twenty-first century are rapidly becoming Knowledge Networkers who are well-versed in the local and global events that affect them. Their activities are based on universal, objective, timely, and retrieved from many sources of information. Human rights and opportunities are increasingly being recognized by the general populace. Computers, the internet, and information technology are to blame for this transformation. As a result, government and industry now operate in different ways.

Intriguingly, the topic of cybercrime now emerges. The description of cybercrime is a major issue. The first challenge in defining cybercrime is that there is no commonly recognized definition at the outset. It's hardly unexpected, as cybercrime is used as an umbrella term to designate, at least in part, to a relatively new collection of behaviors that have yet to be completely absorbed into national legal frameworks across the globe.

Cybercrime is invariably used with “computer crime”, “computer misuse” or “IT crime”.

4. NEW THREAT - CYBER TERRORISM

Cyber terrorism is the use of electronic networks, particularly computer technology, as a weapon. Attacks using the Internet need to include a terrorist component in order to be branded “cyber terrorism”. For the historical purpose, the term ‘cyber terrorism’ was formed in the late 1980s when Collin, a SRF at (ISI) in California, developed this hot techno-phrase by merging two language elements: cyber space and terrorism.

Today, over two decades later, cyber terrorism remains difficult to describe since this phrase does not have a straightforward, universally recognized precise meaning. Part of the reason is because there is some debate in the definition of cyber terrorism itself: the term comprises of ‘cyber’- a meaning for which most people would agree on - and ‘terrorism’- which, since 1793, has had over two hundred definitions. ‘Cyber’ is everything relating to computers, computerized things (both actual and imagined), and/or automated systems (both in terms of hardware and software) (both in terms of hardware and software). On the other hand, one man’s terrorist is another man’s freedom warrior. No wonder that even top researchers in the area of communication and information technology cannot agree on one single definition of cyber terrorism. An e-mail bomb may be an act of pure hacking for some, while it can be an act of cyber terrorism for others.

The phrase ‘cyber terrorism’ has been defined in numerous ways and from different viewpoints. Cyber terrorism originally described as hacking or harmful software assaults against target systems, but the concept of the cyber terrorism has increasingly broadened include illegal behaviours such as prostitution or child pornography over the Internet. The most worrying situations are that Internet users are attracted to cyber space and follow terrorists wholeheartedly and thoughtlessly.Over a decade ago, in 1998, Ehud Tenenbaum, an eighteen-year-old Israeli hacker known as the ‘Analyzer’, accessed the computer systems of the Pentagon, NASA, the Massachusetts Institute of Technology, NUWC and other highly secured computer systems in the U.S. A U.S. Defense Department source termed it “the most orchestrated and methodical strike the Pentagon has seen to date”. Tenenbaum’s hacking operation was even given a code name, the ‘Solar Sunrise’, by the F.B.I. 'Mafia Boy', a 16-year-old

Canadian hacker, was also able to get into some of the most sensitive computer networks in the US in 2001.

Cyber terrorism is, at its core, the act of carrying out terrorist acts via the use of computer technology. In order to communicate, propagate, recruit, and gather information, terrorist organisations have turned to the Internet. Terrorists may easily communicate through computer-mediated networks because they are decentralized, difficult to monitor, and open to anybody who wants to use them. As a result, the cyber world may be utilised in a variety of ways, not only as a tool for conducting an assault but also as a direct weapon.

Terrorism and cybercrime are both subcategories of cyber terrorism. Whether it's cybercrime or terrorism, these categories are either relatively new or have taken on new historical importance. It's the consequences of this debate that are keeping the definitions of these groups vague. Cybercrimes are defined as crimes committed using computers or other information systems, often over the Internet, however this is not always the case. There are several definitions of terrorism offered by the United States government, and there is even less agreement on a definition of terrorism globally. In order to communicate, propagate, recruit, and gather information, terrorist organizations have turned to the Internet. Terrorists may easily communicate through computer-mediated networks because they are decentralized, difficult to monitor, and open to anybody who wants to use them. As a result, the cyber world may be utilized in a variety of ways, not only as a tool for conducting an assault but also as a direct weapon.

Is cyber terrorism comparable to the other types of terrorism we've discussed so far in terms of its characteristics? I'm sure there's a distinction between hijacking an airliner with a pistol and hijacking it by gaining control of the plane's computer systems. Defining the legal character of cyber terrorism is essential to the international community's efforts to combat terrorism using international legal instruments, as indicated above.Terrorism, as previously said, includes aspects of physical injury as well as a purpose to instill fear and influence people's behaviour. For example, disrupting traffic light systems, hospitals' computers and energy firms' computer systems might inflict bodily injury. Fear and uncertainty among the victims leads to pressure on the government to 'do something' about it as a result of these actions. You don't have to bring a weapon on board a plane in order to carry out a terrorist attack. You don't need to leave the comfort of your own home to receive the same effects.

Anti-virus and information security measures are also in place to defend the majority of possible infrastructure targets of cyber terrorism. It takes time and expertise to break into these programmes, and it can only be done if the hacker intends for it to be done. Ehud Tenenbaum is not necessarily a terrorist since he planned to hack into sensitive networks. The intention factor also suggests that there was an intention to influence a government course of action, as per the aforementioned definition.Cyber terrorism, however, differs from previous kinds of terrorism in numerous important ways. To us, terrorism was defined as an attack on a specific target that may result in a significant loss of human life. It didn't matter what the people looked like in the flesh. Another kind of terrorist attack, known as "cyber terrorism," has the potential to harm a narrowly defined group of individuals, such as government agencies, large corporations, and the nation's key infrastructure.

Cyber terrorism, on the other hand, makes use of cyberspace as a weapon. For example, if a cyber terrorist attacks a crucial national infrastructure, it might have an impact on the lives of those who rely on that infrastructure. According to Joel Trachtman, cyber terrorists can attack military and civilian defence networks, as well as other governmental networks (police and fire), privately or publicly owned networks that control public utilities and other systems for providing infrastructure services (electricity, water), and public networks used by individuals and businesses for communication, education, and other purposes.

As technology advances, so do the defense mechanisms available to governments, allowing them to better defend themselves against assaults of this kind. Cyber terrorism is also notable for its low financial and risk stakes. Terrorist attacks in the real world need the recruitment of an executor, the provision of weapons and explosives, and the assurance that the executor will pass all security checks en route to the intended target. Counterterrorism using cyberspace is likely to save the terrorist both money and time. Assuming you know how, launching a cyber-attack does not need the purchase of weapons or physical presence at the target. When it comes to waging cyber war, all you need is a powerful computer and superior hacking abilities to your adversary. Anyone may learn the necessary technological abilities in today's society, thanks to the abundance of "Hacking " crash courses that can be accessed on the Internet.

5. CONCLUSION

As a result, the use of a computer as a tool to promote illicit purposes, such as fraud, child pornography and intellectual property trafficking, identity theft or privacy violations, is known as cybercrime. As computers have become more important in business, entertainment, and government, so has the threat of cybercrime. In nations where private entrepreneurship is

promoted, contracts are an essential aspect of the economic system. As a result, thieves are tempted to break into other people's accounts and use their money unlawfully.

The vast majority of cybercrime involves the theft or alteration of data pertaining to a person, a company, or a government. Essentially, our digital identities have become an integral part of our daily lives, since we are a collection of numbers and identifiers in different computer systems held by governments and companies. Computer crime exposes the vulnerability of supposedly solid facts like an individual's identity, and the relevance of computer networks in our life. Cyberspace is nothing more than a more elaborate replica of the physical space occupied by a telephone conversation between two persons on the other end of the line from each other. Internet thieves have various hiding spots both in the actual world and in the network itself because of the Internet's global reach. Despite their best attempts, cyber thieves leave traces that can be followed by a professional tracker, much as people walking on the earth leave a trail of footprints. However, international cyber-crime treaties must be adopted in order to pursue these leads beyond national borders. As a starting point, we'll look at the primary variables: cyber terrorism, vulnerability, comprehensive collaboration and the law and rules that govern them.

REFERENCE

1. BazelonDana L, Choi Yun Jung and ConatyFJason: Computer Crimes, 43Am.Crim.L.Rev.259, 264(2006).
2. Catherine D.Marcum, George E.Higgins, TinaL.Freiburger and Melissa .L. Ricketts:Battleof theSexes: An Examination of Male and Female Cyber Bullying,International Journal of CyberCriminology, IJCC, January – June.
3. Catherine D. Marcum1, Georgia Southern University, George E. Higgins, Richard Tewksbury,"Doing Time for Cybercrime: An Examination of the Correlates of sentence Length in the UnitedStates "International Journal of Cyber Criminology, Vol 5 Issue 2 July - December 2011.
4. D. Glenn Baker, "Trespasser will be prosecuted: Computer Crime in the 1990's", Computer/Law Journal. 1993. 12 (1) 68.
5. Dennis Lloyd, "The Idea of Law", Penguin revised edition, 1970, pp37-40,186-190,224-5, and 238-239, Passim L. Henkin, "How Nations Behave ", 2nd edition, 1979, and J. G. Merrills," Anatomy of International Law ", 2nd edition, 1981.
6. Holt.J.Thomas,Strumsky Deborah, Olga Smirnova and Kilger Max: Examining The SocialNetworks of Malware Writers And Hackers, International Journal of Cyber Criminology, IJCC,January – June.
7. MakkarAshokDr.:Legislative Framework to Combat Cybercrimes in India: An Overview, CyberLaw Cybercrime Internet an E-commerce, By Prof. VimlenduTayal, Bharat Law Publications(2011).
8. Nappinai N.S: Cybercrime in India: Has Law kept Pace with Emerging Trends?An EmpiricalStudy.
9. Starke G:Introduction to International Law, Aditya Book, Butterworths& Co (Publishers) Ltd1989, 10th edition, Pg
10. Times Of India - Article – 5 Lakh Cyber warriors to bolster India's e-defense – dated 16thOctober 2012.
11. UnnithanSandeep:ENTER THE CYBER – By Today, dated 5th November 2012.

Corresponding Author

Richa Tiwari*

Research Scholar, Jiwaji University