Cyber Crime, Cyber Space and Effects of Cyber Crime

Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage

Punyashlok Ahilyadevi Holkar Solapur University Solapur, Maharashtra, India

ABSTRACT

Cyberspace is a domain that uses the electronic and electromagnetic spectrum to store, modify, and exchange data through network and system-related physical infrastructures. Cyberspace is an endless space known as the Internet. Computer transactions, especially transactions between different computers, can be viewed as a space. Images and text on the Internet exist in cyberspace. The term is used in conjunction with virtual reality, giving the name of the imaginary place where a virtual object exists. If a computer creates a picture of a building that allows the architect to "walk in" and see what the nature of a design is, the building is said to be in cyberspace. Cybercrime is a series of organized criminal attack cyberspace and cyber security. Cybercrime such as Hacking into computer, this can be through a network system and clicking on unfamiliar links connecting to unrecognized Wi-Fi, downloading software and files to unsafe sites, consuming energy, electromagnetic radiation waves, and more.

Cyber security is a serious problem and must be taken seriously as it has become a national concern. Currently, most electronic devices such as computers, laptops and cell phones come with built-in firewall security software, but even so, computers are not 100 percent accurate and reliable in protecting our data.

Keywords : Cyber Crime, Cyber Security, Technology

I. INTRODUCTION

In today's world, cyber systems have given rise to the flexibility of illegal use due to the government's Internet policy. There are many risks to the economy, such as the Internet, buying, selling, online transactions and social networking. The Internet has simplified business processes such as classification, summary, coding, editing. Referred to as the "global and dynamic domain" characterized by the combined use of cyberspace electronics and electromagnetic spectrum, the purpose of which is to create, store, modify, exchange, share, and extract physical resources, use, remove, inform and disrupt.

Cyberspace can also be viewed as a conceptual environment in which communication through computer networks. 1990 The term became popular in the 1990s when the use of the Internet, networking and digital communication was increasing and the term was able to represent many new ideas and developments in the emerging term. However, it is through this same cyber network that infiltrates and attacks us in ways that are detrimental

to our privacy, economic, social life. It is also bringing unwanted consequences like criminal activity, spamming, credit card scams, phishing and ATM fraud. Some scholars have argued interestingly that "nobody in the Internet knows a dog". This causes some legal issues and concerns. The IT revolution provides many avenues and facilities that have an unlimited impact on the modern communications, travel and security sectors. While the benefits gained by the information age are not perfect, the widespread interconnection of human activity with electronic resources and infrastructure is a significant vulnerability, which is a constant threat of misconduct, fraudulent handling, and the breakdown of computers and computer networks. The advent of the Internet has had its drawbacks and disadvantages. In recent times, the outbreak of cybercrime has been alarming and the negative impact on the country's social economy has been extremely tragic. Over the past twenty years, unethical cyberspace users have continued to use the Internet to commit crimes; this has led to dissatisfaction with cyber and personal security. The trend has only recently increased and calls for an immediate response in providing laws that protect cyberspace and its users.

Overview of Cyber Crime, Cyber Space, and Cyber Security:

As information technology continues to expand in the activities of physical infrastructure, there is a huge risk that it may harm or disrupt the services that depend on our economy and the daily lives of billions of people. In light of the risks and potential implications of cyber security, the security and flexibility of cyberspace becomes a security mission. Cyberspace refers to the limitless space known as the Internet. It refers to an interdependent network of information technology components, which is the place of many of our communication technologies today. Cyberspace is an electronic medium used to build global computer networks to facilitate online communication. It is a large computer network made up of many computer networks in the world that uses the TCP / IP protocol to assist in the communication and data exchange. Through cyberspace, crimes are now taking place. These include the production and distribution of child pornography and child abuse conspiracy, banking and financial fraud, intellectual property infringement and other crimes, all of which have human and financial consequences. The financial consciousness and national security of the Nations depends on a wide range of interdependent and critical networks, systems, services and resources known as cyberspace. Cyberspace has transformed the way we communicate, travel, power our homes, run our economy, and get government services.

Cyber-security is the core of technology, processes and methods designed to protect data from attacks, damage or authoritative access to networks, computers, programs and data. In the computer or cyber context, the word security is cyber-security. A joint effort by both citizens and their information systems must be ensured to ensure cyber-security. The threat posed by our cyber-security breaches is moving faster than we can handle. It is not possible to focus effort on only one aspect of the violation because of its infringement and increased allowance for other matters. This leads us to conclude that we will have to deal with cyber security breaches altogether. Cyber security is a collection of tools, policies, security concepts, security guards, guidelines, risk management approaches, actions, training, best practices, guarantees and technologies that can be used to protect the cyber environment and the assets of organizations and users.

Cybercrime is a series of organized crimes that attack both cyberspace and cyber-security. Cybercrime refers to criminal activity committed using computers and the Internet. These include unlawful access, computer access to or through a computer system,

transmitting computer data .This includes anything from downloading illegal music files to stealing billions of dollars from online bank accounts. Cybercrime also includes non-financial crimes such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Perhaps the most striking feature of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users.

Significance of Cyber Security:

Following are some significance of the cyber security.

- Working collaboratively with public, private and international organizations to secure cyberspace.
- To help individuals and organizations develop and nurture a culture of cyber-security.
- Integrity, which can be truthful.
- Privacy
- To understand the current trends in IT / cybercrime and help develop effective solutions.
- To help people reduce the vulnerability of their information and communication technology (ICT) systems and networks.

Cyber Crime Types:

1. **Terrorism of Cyber:**Cyber-terrorism involves the use of the Internet for terrorism or terrorist attacks. Is this a new way or does it means that the rebels or religious extremists plan strategies for recruiting new members and invading the country?

2. **Online Assisted Kidnaping:**This is not news that the hijacking is on the rise, many are unaware that the hijackers are being helped by their victims' social media activities and by the geo-location data on their smart phones. Geo-location data is information that can be used to identify the physical location of an electronic device using smart phones built into the Global

Positioning System (GPS) functionality, allowing location-based services to discover and publish information about owners. Hijackers have begun to use geographical locations and geographical tags to identify their victims.

3. **Fraud Identity Theft:**It is a criminal act in which someone retrieves important information by pretending to be someone else. For example, creating a false bank webpage to retrieve one's account information. The concept is simple; a person gains access to your personal information and uses it for his or her-own benefit. In Nation, people design web links that request users to fill in their basic information, such as unique things like pin numbers and use them to commit a crime.

4. **Internet Pornography:**Using the web for sexual abuse is a very active research interest. It has been found that internet pornography is a disturbing trend especially among young people. Web filtering programs have been used to detect Internet pornography in the country. It contains obscenity pictures, photos, writings, etc. There is also the use of the Internet to download and broadcast so that the Internet is used to attract children who are not suspected of child abuse and distribute child pornography. Another trend is the use of mobile phones and the Internet for prostitutes. Therefore, prostitutes now advertise their business via the Internet, exposing their sensitive, sexual and private parts to Internet users.

5. **Hacking:**Hackers use vulnerabilities and loop holes in the operating system to destroy data and steal important information from the victim's computer. This is usually done by using a backdoor program installed on your machine. Many hackers try to gain access to resources through password hacking software. Hackers can also monitor what you do on your computer and import files to your computer. A hacker can install many programs on your system without

your knowledge. Such programs can be used to steal personal information such as passwords and credit card information. Important data of the company can also be hacked to get secret information about the company's future plans.

Causes and Effects of Cyber Crime:

1. **Lack of Confidence:**This is one of the reasons why people are engaging in cyber-crime. Some people believe that he can no longer do this in life, they feel frustrated and think that the only way to make mistakes and move on is to get instant wealth, in which case they go back to Internet fraud.

2. **Poverty:**Most citizens do not have a means of subsistence and have only places to eat, food to eat, clothes to wear, and thus engage individuals in the cyber-crimes listed above for treatment. This is because life is the most worthwhile way of life, and poor people see the Internet as a means to make their lives meaningful.

3. **Unemployment:**This is one of the main reasons people are involved in cyber-crime. Even after all the educational qualifications in the country they are not getting jobs and hence they are depressed and they see that the average life is a means of survival of internet fraud. Even those who are employed are not paid for months, sometimes years and this can also lead to those involved in cyber-crime.

4. **Greed:**Most people engage in cybercrimes because they don't have what it takes to lead a normal life, but they never think about what they have and want to get faster and richer without going through the right process.

Cyber-Crime Effects:

1. **Moderates the competitive edge of organizations:**Over the years, a private and public business firm in the country has suffered greatly due to computer crimes. This has caused a lot of financial and physical damage. Billions have been damaged by cyber-crime. Such offenses could endanger the security and

financial health of the country. For example, cyber-crime has a big impact on a nation's economy. For example, in a recent Ponzi scheme like MMM, Ultimate Cycler etc. Most Nationns are involved. It has been reported that citizens lost eight million from MMM which is a major loss of the Nation economy.

2. **Waste of Time and Reduces the Financial Growth:**Wasting time is another problem because many IT individuals can spend a lot of time handling and repairing harmful or harmful cases caused by computer criminals. The time spent should make the organization profitable. One strange problem is that when a hacker enters an organization and steals confidential information from the company, the company may have confidential information such as customer's credit card, and people who trust the company lose their trust because the information is stolen. The customer will not trust the company again and will go to someone else who can protect their confidential information.

II. CONCLUSION

Information and communication technology (ICT) systems are now essential for our lives as is water and electricity. Many individuals, corporate bodies and government entities rely on ICTs and computer networks to perform simple and complex tasks. However, cyberspace is becoming unsafe as many businesses, agencies and individuals are being hit by cyber criminals in the country. The prevalence of cybercrime has increased in nation. The United States and the United Kingdom are the third-largest country in the world internet crime, while 5.5 percent of the world's hackers are said to be civilians. Most young people, as the "Yahoo" kids are promised, have taken advantage of fraudulent online transactions, electronic shopping and e-commerce growth to engage in heinous crimes. As such, it is

affecting the image of the outside world, and cyber-security should be given serious attention.

III.   REFERENCES

[1].   DamboItari, EzimoraOkezie Anthony, and Nwanyanwu Mercy (2017), 'Cyber Space Technology: Cyber Crime, Cyber Security and Models of Cyber Solution: A Case Study of Nigeria', International Journal of Computer Science and Mobile Computing, Vol-6, Issue-11, pp. 94-113.

[2].   Halder, D., &Jaishankar, K. (2011),'Cyber-crime and the Victimization of Women: Laws, Rights, andRegulations', Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9.

[3].   Esharenana E,&Igun 'Combating cyber-crime in Nigeria' Electronic library, Vol-26, Delta, Emerald Grouppublishing Ltd, 2008, pp.717.

[4].   Cameron S.D. Brown (2015), 'Investigation and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice', International Journal of Cyber Criminology, ISSN 0975-5089, Vol-9, Issue-1, pp. 55-119

[5].   Moses A. A. and Hight C. I. (2015), 'Cyber Crime Detection and Control Using the Cyber Under Identification Model', International Journal of Computer Science and Information Technology and Security, ISSN 2249-9555, Vol-5, Issue-5, pp. 354-368

[6].   Yanbo Wu, Dawei Xiang, JiangMingGao and Yun Wu (2018), 'Research on Investigation and Evidence Collection of Cybercrime Cases', Journal of Physics: Conference Series 1176 (2019) 042064, IOP Publication, pp. 1-6