Page 1506 - 1515 **DOI:** *https://doij.org/10.10000/IJLMH.113493*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 4

2022

Cyber Crime Invasion in Cyberspace

DR. LEENA[1]

ABSTRACT

Man is curious by nature. His inherent lust for social and economic development has led to tend out new ways as a source of all-round progress. The anxiety of man to lead happy and prosperous life has also played a vital role in course of development and so technological development does not stand still. The ICTs and Internet have changed the style of working, communicating, and doing business almost touching every aspect of life. And this created cyberspace; a virtual world as it generates a virtual interactive experience accessible regardless of geographical location. In this space individuals or netizens can interact, share information, exchange their ideas, conduct business, create artistic media, get entertained, provide social support etc. This virtual world i.e. cyberspace and the real world impact each other. With the coming of new Information and Communication Technologies and the Internet, there is a growing misuse side by side, the scenario has changed. On the one hand, new technologies have facilitated the commission of old crimes by the bad elements and at the same time, new crimes have originated commonly called cybercrime. The Internet is acting as a double-edged technological weapon. On one hand, it is providing so many benefits in the form of different services whereas, on the other hand, it is also an extremely powerful tool in the hands of bad elements for committing cybercrime.

I. INTRODUCTION

The men's curiousness to explore more and more, social and economic development has led to the technological development, development of Computer, ICT and the internet. This development has changed the scenario of the society. These developments created a cyberspace, now man lives in a virtual world or cyberspace. Men's anxiety to lead happy and prosperous life has also played a vital role in course of development and so technological development. From the day men started the use technology to modify their lives they found a series of technological traps. When these technologies reach the criminal-minded person it becomes the weapon to create cybercrime. so we need cyber security and follow some cyber ethics as we follow social norms.

Cyber Crime

[1] Author is an Assistant Professor at the School of Law, Maharaja Agrasen University, Baddi, Distt.- Solan, H.P., India.

 [ISSN 2581-5369]

The term 'Cyber crime' is frequently used in the 21st-century knowledge society and is created by a combination of two words cyber and crime. The term Cyber' donates cyberspace i.e. virtual word, virtual space and means the informational space modelled through the computer in which various objects or symbol images of information exist. It is the place where the computer programme work and data is processed

Dr Vladimir (Ukraine) Director of Computer Crime Research Centre (CCRC) during an interview on the 27th of April 2004, defines "cyber-crime ('computer crime') as any illegal behaviour directed using electronic operations that targets the security of computer systems and the data processed by them.

"Cybercrime" means illegal acts, the commission of which involves the use of information and communication technologies;[2]

Cybercrime" means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them;[3]

Cybercrime has to do with the wrecking havoc on computer data or networks through interception, interference or destruction of such data or systems. It involves committing a crime against computer systems or the use of the computer in committing crimes

II. HISTORY OF CYBERCRIME:

The first recorded cyber crime took place in the year 1820, when Joseph Merrie Jacquard, a textile manufacturer in France produced the loom. This devise allowed the repetition of a series of steps in the weaving of special fabric.[4] This resulted in an exceeding concern among the Joseph Merrie Jacquaid workers that their livelihoods , as well as their traditional employment, were being threatened, and prefer to sabotage to discourage Jacquard so that the new technology cannot be utilized in the future.[5]

Cybercrime has become a global buzzword and everybody is affected by this crime. It also affected e-commerce, e-governance etc. Various types of cybercrime are:-

Cyber Pornography

[2] https://cybercrime.org.za/definition.

[3] *Ibid*

[4] Dr. Jyoti Rattan and Dr. Vijay Rattan, Cyber laws & Information Technology, 232, (8th Edn.,2017, Bharat law House PVT. Ltd.)

[5] Animesh Sarmah, Roshmi Sarmah , et.al. *A brief study on Cyber Crime and Cyber Law's of India* 04, IRJET Volume: 04 Issue: 06, June -2017

 [ISSN 2581-5369]

Cyber pornography refers to stimulating sexual or other activity over the internet. This would include pornographic websites, pornographic magazines produced using a computers to publish and print the material and the internet to download and transmit pornographic pictures photos, photo writing etc.[6]

Information Technology has made it much easier to create and distribute pornographic materials through the internet; such material can be transmitted all over the world in a matter of seconds.[7]

Cyber Squatting

Some enterprises registered the name or trademarks of well-known companies as domain names which sale intention of selling the name back to the companies when they finally woke up.[8]

Cybersquatting is the term most frequently used to describe the deliberate bad faith abusive registration of a domain name in violation of rights in trade mark and service mark.

Cyber Stalking

Stalking in general terms refers to harassing or threatening behaviour that an individual engages in repeatedly towards another person. Stalking is the crime of following and watching somebody over a long period in a way that is annoying or frightening.

Cyberstalking is where electronic mediums such as the internet are used to pursue or contact another in an unsolicited fashion; it is just the extension of the physical form of stalking an electronically. The term is used to refer to the use of the internet, e-mail or other electronic communication devices to stalk another person. It generally involves harassing or threatening behaviour that an individual engages in repeatedly such as following a person appearing at a person's home or place of business making harassing phone calls, leaving written messages or objects vandalizing a person's property[9]

Hacking

Hacking is unauthorized access to a computer and refers to access to the whole or any part of a computer system without permission. Hackers worldwide attempt to hack into the remote computers for multiple purposes caves dropping data theft, fraud, destruction of data, causing damage to computer systems or mere pleasure or personal satisfaction.

[6] Vikram Singh Jaswal and Shweta Thakur Jaswal, Cyber Crime and Information Technology Acr, 2000, 20, (2014 Regal Publications, New Delhi)
[7] Rahul Muthan, The Law Relating to Companies and Internet, Pg. 238, 2000
[8] V.k. Unni, Trade Mark & Engineering Concept of Cyber Property Right, 22, (2002, Eastern Law House)
[9] *Supra* note 5

 [ISSN 2581-5369]

When a person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, he is said to have committed an offence hacking.[10]

Cyber Fraud

The Audit Commission of the United Kingdom defined "Cyber Fraud as any fraudulent behaviour connected with computerization by which someone intends to gain financial advantage"

D, Bainbridge defines it as 'computer fraud is used to describe stealing money or property using a computer that is using a computer to obtain dishonestly, property including money and cheques, credit card services or to evade dishonestly some debts or liability, it involves dishonestly instructing a computer to transfer funds into a bank account or using a forged bank card to obtain money from an automated teller machine"[11]

Viruses

Viruses are computer programmes that migrate from computer to computer and attach to the computer operating system[12] Viruses are a programme that have the ability to infect other programs and make copies of themselves and spread on another program. It generally affect data on a computer by modifying or deleting them.[13] The effect of virus may be temporary or permanent depending upon the purpose for which a virus is inserted. The Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused 80 million dollars in damages to computers worldwide.[14]

Trojan

Trojan or Trojan Horse is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damaged, disrupt, steal or in general inflict

[10] Information Technology Act, 2000, S. 66

[11] D. Bainbridge, Introduction to Computer Law,(4th Edn., 2000)

[12] Dr. Farooq Ahmad, Cyber Law in India, 383, (3rd Edn., 2008)

[13] Prof. Saquin Ahmad Khan, Cyber Crime in India: An Empirical Study, p691, International Journal of Scientific & engineering research , 11 (5), (2020)

[14] P.T. Joseph, S.J. and Sanjay Mohpatra, Management Information system in The Knowledge Economy" 498,(2nd Edn, 2014, PHI Learning Private Limited Delhi)

 [ISSN 2581-5369]

some other harmful action on one's data or network.[15] Trojan are presented as free softwares and they set-off the system by downloading and loading by users. [16]

Worms

Worms is a type of malware that infect a computer system without getting attached to its operating part. Worms can multiply without any known intervention and without the need to be attached to a file and moves from one computer to another computer. Worms have the potential to grow exponentially and wind their way through the internet. Worms are designed to invade computers without authorization and can cause damage in overloaded servers and anti- worm extracation.[17]

Cyber Defamation

Cyber defamation means using the internet as a tool to defame and malign another person. It involves use of social media and online campaigns to tarnish the image of the victim. It involves publishing of defamatory material related to person in cyberspace or through electronic way.

Cyber Bullying

Bullying is unwanted, aggressive behavior that is repeated or has the potential to be repeated over time[18] and cyber bullying is the bullying with the use of modern digital technologies. It is also the repeated behavior aimed at scaring, angering or shaming those who are targeted and can take place on social media, messaging platforms, gaming platforms or mobile phones.[19] The effects can last a long time and affect a person mentally emotionally and even physically.

Cyber Terrorism

Dorothy Denning , a professor of computer science has defined it as "cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computer, network and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."[20] The 9/11 attack ,2001 was a first major cyber attack by Al Qaeda against the US Government which carried not only the threat messages but also deface many websites, disrupted internet communication for

[15] Alison Grace Johansen, What is a Trojan? Is it a virus or is it malware. July 2004. ,https://www.us.norton.com

[16] Mehmet Ali Gezkaya, Cyber Security, Tools and Methods of Cyber Threats, Dimension of Cyber Threats at the present Time and Cyber Armies, 218International journal of Advances in Science Engineering and Technology, Vol-4 Spl.Issue-2, (2016), http://www.iraj.in

[17] United States v. Morris, 982 F.2d 504 (2d Cir. 1991)

[18] https://ww.stopbullying.gov

[19] UNICEF, "Cyberbullying; What is it and how to stop", https://www.unicef.org

[20] Gabriel Weimann, Cyberterrorism : How real is the Threat" Special Repot 119, Dec. 2004, https:www.usip.org

the government as well as peopleand encouraged muslim hackers to support the militant forum in their jihad[21]

III. NEED OF CYBER SECURITY FROM INVASION

The term "Security' means a 'freedom from risk or danger safely', but this definition is somewhere misleading when it comes to computer and networking security, because it implies a degree of protection that is inherently impossible in the modern connectivity- oriented computing environment. So, when security is concerned to computer it means 'the level to which a program or device is safe from unauthorized use'

In cyberspace, Russia has interfered in Ukrainian elections, targeted its power grid, defaced its government websites and spread disinformation. Strategically, Russian cyber operations are designed to undermine the Ukrainian government and private sector organizations. Tactically, the operations aim to influence, scare and subdue the population. They are also harbingers of invasion.[22]

"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." Articulating a concise, inclusive, meaningful, and unifying definition will enable an enhanced and enriched focus on interdisciplinary cybersecurity dialectics and thereby will influence the approaches of academia, industry, and government and non-governmental organizations to Cybersecurity challenges.[23]

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing in the cyber space. More sophisticated techniques are now used by attackers, so security plan to be adopted is to make an attempt to strike the proper balance between the two objectives. The first step is to determine what needs to be protected and to what degree. Because not every asset is equally valuable, some assets need stronger protection than others. This determination leads to the concept of instituting multiple layers of security. An effective security plan does not rely on one technology or solution but instead takes a multilayered approach. When you talk of business physical security measures, most companies don't depend on just the locks on the buildings door to keep intruders and thieves out. Instead, business entity might also have perimeter security, perhaps additional external security such as a guard or guard dog, external or internal

[21] *Supra* note 3 at 276

[22] Maggie Smith 'Russia has been at war with Ukraine for years – in cyberspace" The Conversation, 7tH Feb. 2022

[23] Dan Craigen, Naidu Diakun- Thibault, et. al., 'Defining Cybersecurity" Technology Innovation Management Review, Oct. 2014

 [ISSN 2581-5369]

alarm system, cctv, to protect special valuables, further internal safeguards such as a vault IT security should be similarly layered

IV. CYBER SECURITY TECHNIQUES

- **Access control and password security**

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

- **Authentication of data**

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus a good antivirus software is also essential to protect the devices from viruses.

- **Malware scanners**

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

- **Firewalls**

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

- **Anti-virus software**

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

PHYSICAL SECURITY

One of the most important aspects of a comprehensive network security plan a physical access control. This matter is often left up to facilities managers and plant security departments or outsources to security guard companies.

 [ISSN 2581-5369]

Physically breaking into the server room and stealing the hard disk on which sensitive data resides may be crude method of committing cybercrime; it could be easiest way to gain unauthorized access, especially for an intruder who has help "on the inside"

- Create a visibility over all access points, their criticality and access control measures deployed at all these points[24]
- Ensure that the facility is divided into security zones, based on the criticality of each function, project or task being carried out. Derive a map of access requirements for each zone and user groups that require access to these zones[25]
- Ensure that the entry to a facility is restricted to only those users who provide proof of their organizational identity.[26]
- Protecting file servers
- Protecting workstations
- Protecting network devices- fiber cable is more difficult to tap into because it does not produce electrical pulses but instead uses pulses of light to represent the 0s and1s of binary data
- Protecting laptops- physical security for portable computers is especially important because it is so easy to steal the entire machine, data and all

One should always take some preventing measures to protect himself from cyber attacks. The following points should be kept in mind while working on computers and the Internet-

- Exercise caution while sharing personal information such as your name, E-mail address etc. Do not respond to e-mail messages that ask for your personal information
- Do not visit unwanted gambling or related websites
- Avoid sending any photographs to strangers as these may be misused
- Choose strong passwords so that these cannot be easily decoded. It is always recommended to keep changing the passwords at regular intervals
- Always keep on reviewing your credit card and bank statement regularly, if one get tip of being stolen than timely action can be taken.

[24] Advanced Cyber Security Techniques, https://www.cemca.org
[25] *Ibid*
[26] *Ibid*

 [ISSN 2581-5369]

- Always keep your computer up-to-date. Install all necessary software at regular intervals as they are a great start towards keeping you safe
- Keep internal corporate web servers separate from public sites
- Always keep backup of the data stored on your computer to safeguard against viruses
- It is better to use security programs that keep guard on cookies as leaving cookies unguarded might provide fatal.

V. NEED TO FOLLOW CYBER ETHICS

Cyber ethics are nothing but the code of the internet. It refers to the basic ethics and etiquette which must be followed while working on computer. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way.ew The below are a few of them:

- Do use the Internet to communicate and interact with other people**.** Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world [27]
- Never bully on the Internet. Never send embarrassing pictures of them, make lie statement on electronic media, or do anything else to try to hurt them.
- Never operate others accounts using their passwords without their authority or permission
- Do not send any kind of malware to other's systems and make them corrupt.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

VI. CONCLUSION

Cyberspace is the space or areas which are created by the use of electronics and the electromagnetic spectrum for communication, exchange of ideas, data storage, modify and exchange data via networked systems and associated physical infrastructures. With this the

[27] https://www.aarp.org

cyber crime is also perpetuated on the cyber space. There is invasion in one, space either through hacking, defamation, implantation of viruses, worms, cyber fraud or through various ways with the purpose of creating threat and harm. For this we needed cyber security, which is more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are more challenging and there is no perfect solution for protection from such an invasion what is needed is that we must follow some ethics in cyber space in order to have a safe and secure future in cyber space.

*****

 [ISSN 2581-5369]