International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 12 Issue 3, May.-June, 2024, Impact Factor: 8.376

Concept and Types of Cyber Crime

Dr. Anmoplreet Kaur

Assistant Professor of Law, Army Institute of Law, Mohali

INTRODUCTION

Nature has gifted human beings with, mind and brainpower which distinguishes them from other creatures and makes man superior among other living creatures of the universe. The progress of human civilization eventually led to the discovery and inventions of new ideas beginning from the need for survival to luxuries of modern life. New communication systems and digital technology have made dramatic changes in our life styles. In today's highly digitalized world almost everyone is affected. A revolution is being witnessed in the way people are transacting. Almost all companies extensively depend upon their computer networks preserving their data in electronic form consumers are using credit card for shoping. Most people are using e-mails, cell phones and SMS messages for communications. Businesses and consumers are increasingly using computers to create transmit and store information in the electronic form instead of the traditional paper documents. Digital signatures and e-contracts are fast replacing conventional method of transacting business. With the coming of the computer age the industry has seen a quantum leap in quality, quantity and speed. There is modernisation of life style. However, the technology is still developing and unfolding. It is the human mind which generates within men desire for knowledge and capacity for reasoning which culminates into the growth of modern science and technology. Of all the significant advances made by the mankind, the invention of computer is perhaps the most noteworthy achievement which has not only made the human life easier and comfortable but acts as a substitute for human mind for storage of knowledge.

From the functional point of view, the computer has even excelled human mind as a source of storing knowledge and information. The emergence of computer networking has greatly facilitated access and storage of information eliminating constraints of distance and time in communication. They have provided an excellent method of transmission of information across the world with the result the world has now virtually become a global village.[1]

Therefore, crimes which relates to technology are cybercrimes and these are not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognised by the Information Technology Act. Cybercrime is the most prevalent crime playing a devastating role in modern world. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation, it can be said that, Cybercrime includes any illegal activity where computer or internet is either a tool or target or both. The term cybercrime may be judicially interpreted in some judgments passed by courts in India;however, it is not defined in any act or statute passed by the Indian Legislature. Cybercrime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Whatsoever the good internet does to us, it has its dark sides too. In short with the advent of computers in the late 1960‘s crimes were mostly related to physical damage to computer networks and telephone networks.[2]

Meaning and Definitions of Cyber Crimes

Cybercrime is an illegal activity that is committed by using a computer or the Internet. Cybercrime can be committed against people, property and organizations. Diligent monitoring of computer networks is necessary to protect sensitive information. The offences which take place on or using the medium of the Internet are known as cybercrimes. These include a plethora of illegal activities. The term 'cybercrime' is an umbrella term under which many illegal activities may be grouped together. Because of the anonymous nature of the internet, there are many disturbing activities occurring in the cyberspace which may enable the perpetrators to indulge in various types of criminal activities which are called cybercrimes. The weapon with which cybercrimes are committed is technology and therefore, the perpetrators of these crime are mostly technically skilled persons who have thorough understanding of the internet and computer applications. As regards exact definition of cybercrime, it has not been statutorily defined in any statute or law as yet. Even the Information Technology Act, 2000 does not contain the definition of cybercrime. However, cybercrimes may precisely be said to be those species of crime in which computer is either an object or a subject of

[1] Tiwari, Shastri and Ravi Kumar, *Computer Crime and Computer Forensics*8 (Selected Publishers, 1st edn.,2002).
[2] *Available at*: https://gethackingsecurity.wordpress.com/2012/06/25/cyber-crime-history-and-evolution/pdf (Visited on January15, 2022).

conduct constituting the crime or it may be even both.[3]As we do not have any precise definition of cyber crime; the following are the general definitions of term cyber crime:

―Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime‖[4]

The oxford Dictionary defined the term cyber crimeas ―Criminal activities carried out by means of computers or the Internet.‖[5]

―Cyber crime 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‖[6]

Cybercrime as defined internationally by the U.N. Congress on Prevention of Cyber Crime and Treatment of Offenders[7] comprises two categories as follows:

1. Cybercrime in a narrow sense connotes a computer crime and includes any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.
2. Cybercrime in a broader sense includes all computer related crimes and consists of any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Thus, any activity that uses computer as an instrumentality, target or a means for perpetrating further crime, falls within the ambit of cybercrime. The foregoing definition of cybercrime clearly indicates that there exists very thin line of demarcation between conventional crime and cybercrime. The sine qua non for cybercrime is that there should be an involvement at any stage, of the virtual cyber medium i.e. the computer. A simple yet sturdy definition of cybercrime would be, "unlawful acts wherein the computer is either a tool[8]or a target[9] or both". Thus, cybercrimes are the crimes directed at a computer or a computer system or a computer network.

In the Indian context, cybercrime may be defined as a voluntary and wilful act or omission that adversely affects a person or property or a person's computer systems and made punishable under the Information Technology Act, 2000 or liable to penal consequences under the Indian Penal Code. It must be stated that cybercrimes may also involve conventional criminal activities like theft, fraud, forgery, mischief, defamation etc., all of which are subject to punishment under the Indian Penal Code. Besides, the abuse of computer, computer system or internet has given rise to a number of new crimes which were unknown prior to the emergence of computer technology, but are made punishable under the Information Technology Act, 2000. It would therefore, not be correct to say that the crimes that are punishable under the IT, Act alone are treated as 'cybercrime' insofar as the Indian Penal Code also covers many such crimes like e-mail spoofing, sending threatening e-mail, cyber defamation etc.[10]

Major Causes Behind Cyber Crimes

Professor H.L.A. Hart in his classic work entitled "The concept of Law" has stated that human beings are vulnerable to unlawful acts so ruleof law is required to protect them. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them againstcybercrime. The reasons for the vulnerability of computers may be said to be[11]:

1. **Capacity to store data in comparatively small space:** The computer has uniquecharacteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

[3] Pavan Duggal: *Cybercrime* 17(Universal Law Publishing - an imprint of LexisNexis; 2nd edn., 2017).
[4] *Available at*:https://www.naavi.org/pati/pati_cybercrimes_dec03.htm(Visited on January 04, 2022).
[5] *Available at*:http://www.oxforddictionaries.com/definition/english/cybercrimepdf(Visited on January 04, 2022).
[6] *Available at*:http://cybercrime.org.za/definition(Visited on January 04, 2022).
[7] Tenth U.N. Congress on Prevention of Crime & Treatment of Offenders was held in Vienna on April 10-17, 2000.
[8] Cybercrimes which involve computer as a tool are usually modification of conventional crimes ' such as drug-trafficking, on-line Gaming, financial fraud or forgery, cyber defamation, pornography, intellectual property crimes, cyber stalking, spoofing etc.
[9] Cybercrimes where computer is a target include sophisticated illegal activities such as unauthorised access to networks or computer systems, e-mail bombing, Trojan attacks, data diddling, denial of service attack, Internet time theft, logic bombs, virus or worm attacks
[10] Suri R.K. & Chhabra T.N, *Cybercrime*45 (Pentagon Press, 2004).
[11] *Available at*: https://www.geeksforgeeks.org/cybercrime-causes-and-measures-to-prevent-it/ (Visited on January 10, 2022).

2. **Easy to access :** The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.
3. **Complex :** The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.
4. **Negligence :** Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might beany negligence, which in turn provides a cybercriminal to gain access and controlover the computer system.
5. **Loss of evidence :** Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyzes this system of crime investigation.

Classification Of Cyber Crime

There are many types of cyber crime prevailing in the system; broadly we can classify them in to four major categories as discussed below:[12]

Crime Against Individuals

Cybercrimes committed against individual persons include such types of crimes like transmission of Child Pornography, Harassment of any one with the use of a computer such as e-mail, Cyber Defamation, Hacking, Indecent exposure, E-mail spoofing, IRC Crime (Internet Relay Chat), Net Extortion, Malicious code, Trafficking, Distribution, Posting, Phishing, Credit Card Fraud and Dissemination of obscene material including Software Piracy. The potential harm of such a crime to individual person can hardly be bigger.

Crime Against Property

Another classification of Cyber-crimes is that, Cybercrimes against all forms of property. These crimes include computer vandalism (obliteration of others' property), Intellectual Property Crimes, Threatening, Salami Attacks. This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the amendment is so small that it would normally go unobserved.

Crime Against Organization

The third type of Cyber-crimes classification relate to Cybercrimes against organization. Cyber Terrorism is one discrete kind of crime in this kind. The growth of internet has shown that the standard of Cyberspace is being used by individuals and groups to pressure the international governments as also to terrorize the citizens of a country. This crime obvious itself into terrorism when a human being "cracks" into a government or military maintained website. It is across the world agreed that any and every system in the world can be cracked.

Crime Against Society

the forth type of Cyber-crimes relate to Cybercrimes against society. In this category forgery, cyber terrorism, web jacking, polluting the Youth through Indecent, Financial Crimes, Sale of Illegal Articles, Net Extortion, Cyber Contraband, Data Diddling, Salami Attacks, Logic Bombs types of crime is included. Forgery currency notes, revenue stamps, mark sheets etc can be forged using computers and high-quality scanners and printers. Web Jacking hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

TYPES OF CYBER CRIMES

To appreciate the extent and scope of the menace of cybercrime, various types of cybercrimes are briefly discussed.

E-Mail Bombing

In internet usage, an e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelms the server. Mail bombing is the act of sending an email bomb, a term shared with the act of sending actual exploding devices. Mail bombing is sometimes accomplished by giving the victim‘s e-mail address to multiple spammers. In the Russian internet community, there is another sense for mail bomb. There, mail bomb is a form of denial of service attack against a computer system.[13]

[12] Dr. Ajeet Singh Poonia, ―Cyber Crime: Challenges and its Classification‖ 3(6) (*International Journal of Emerging Trends & Technology in Computer Science* ,2014).

[13] A general overview of e-mail bombing is *available at*:
https://www.cert.org/historical/tech_tips/email_bombing_spamming.cfm? and also at
http://www.worldwizzy.com/library/E-mail_bomb (Visited on February 18, 2022).

E-mail bombing refers to sending a large number of e-mails to the victim resulting in the victim's e-mail account (In case of Individual) or mail servers (in case of a company or an e-mail service provider) crashing. In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application, it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently, he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed. E-mail bombing is characterized by abusers repeatedly sending an e-mail message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial-of-service impact.[14]

E-mail spamming is a variant of bombing; it refers to sending e-mail to hundreds or thousands of users. E-mail spamming can be made worse if recipients reply to the e-mail, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users.[15]

Email Spoofing

E-mail is the short form for _electronic mail'. The electronic mail system over the internet can carry messages, letters, pictures, sounds, or anything that can be created and stored in a computer. Data can be send as electronic mail to any other computer connected to the internet, e-mail spoofing is a technique commonly used to hide the origin of an e mail message. The result is that, although the e-mail appears to have come from a particular address it comes actually from other sources. In India the present practice is to charge the offender with forgery under Section 463[16] of Indian Penal Code for making for electronic records. The punishment is imprisonment of either description for a term which may extend to seven years and fine

Prevention of Cyber Crimes:

In order to stop crimes committed through the computer resources and Internet technology, ―Cyber Law‖ was introduced. ―Cyber Laws‖ can be defined as the legal issues that are related to the utilization of communication technology, concretely ―cyberspace‖, i.e. the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, each action in Cyberspace has some legal and cyber legal views12.Based on the United Nations Model Law on Electronic Commerce (UNCITRAL), 1996, the Indian Parliament passed the Information Technology Act, 2000 (also known as the IT Act no

Lottery Frauds

These are letters or emails, which inform the recipient that he/ she has won a prize in a lottery. To get the money, the recipient has to reply. After which another mail is received asking for bank details so that the money can be directly transferred. The email also asks for a processing fee/ handling fee. Of course, the money is never transferred in this case, the processing fee is swindled and the banking details are used for other frauds and scams.[17]

Phreaking

Phreaking is a slang term coined to describe the activity of a subculture of people who study, experiment with, or exploit telephones, for the purposes of hobby or utility. The term _phreak' may also refer to the use of various audio frequencies to manipulate a phone system. It is often considered similar, and therefore grouped in category with computer hacking. This is sometimes called the H/P culture (H for Hacking and P for Phreaking.) Most phreakers range from the ages of 12-17. Most stop after this because punishments can become more severe once the perpetrator is no longer a minor.[18]

Many Phreaking techniques can be implemented with small electronic circuits, easily made by hobbyists once the secret of their operation is known. The first circuit to generate the switching tones needed to reroute longdistance calls was nicknamed the blue box by an early phreak who had built one in a blue enclosure. Soon, other types of Phreaking

[14] Atul Jain (ed.), Cyber Crime: Issues Threats and Management, Isha Books, 2005. *Available at*: http://cybercrime.planetindia.net/frequently_used.htm (Visited on February 18, 2022).

[15] *Available at*: https://www.cert.org/historical/tech_tips/email_bombing_spamming.cfm? (Visited on February 19, 2022)

[16] Forgery- [Whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

[17] *Available at*: https://www.researchgate.net/publication/274652160_Cyber_Crime_its_Categoriespdf (Visisted on January 12, 2022).

[18] *Available at*: http://academickids.com/encyclopedia/index.php/Phreaking (Visited on February 11, 2022).

circuits were given similar names. Dozens of other type of _boxes' were invented. Modern Phreaking often involves taking advantage of companies Private Branch Exchange systems, especially those which are accessible via toll-free numbers, to make phone calls. Phreakers do not always do illegal things. In fact, they may be thought of as a hacker in the computing world Phreakers may just be interested in the telecommunication world, about the more unknown side of telephones.[19]

Prevention of Cyber Crimes:
In order to stop crimes committed through the computer resources and Internet technology, ―Cyber Law‖ was introduced. ―Cyber Laws‖ can be defined as the legal issues that are related to the utilization of communication technology, concretely ―cyberspace‖, i.e. the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, each action in Cyberspace has some Based on the United Nations Model Law on Electronic Commerce (UNCITRAL), 1996, the Indian Parliament passed the Information Technology Act, 2000 (also known as the IT Act no

Logic Bombs
In a computer program, a logic bomb is a programming code, inserted surreptitiously or intentionally, that is designed to execute (or ―explode‖) under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command.[20] Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed.[21] Many viruses attack their host systems on specific dates, such as Friday the 13th or April fool's Day. Trojans that activate on certain dates are often called ―time bombs‖. It is in effect a delayed-action computer virus or Trojan horse. A logic bomb, when ―exploded,‖ may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.[22] These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Salami Attacks
A salami attack is a series of minor data security attack that that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can he considered a salami attack. Crimes involving salami attacks typically are difficult to detect and trace. 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. A bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.[23] So why do cybercriminals execute these attacks that may yield a relatively small sum of money?

1. To bury it in alerts and logs, making it harder for finance organizations to detect and respond to; or to draw attention elsewhere while planning an even more impactful parallel attack.
2. To pinpoint bank accounts they can easily target. If fraudsters can determine micro-deposits weren't returned — regardless of whether they can see the actual amount — the attackers have confirmation the account and routing number combination is valid. This can directly impact consumers if businesses fail to be proactive, even if the costs to the business are minimal.
3. To test the waters and see what an organization's reaction is in a situation where suspicious activity is present. By examining a bank's defenses, fraudsters can plan a secondary or more significant attack down the road. High-level fraudsters know the ins and outs of staying under the radar to make a big move before financial organizations can detect activity.[24]

Phishing
Perhaps the ―original‖ email scam, phishing is when fraudsters spam users online with emails promising prizes or threatening an account suspension, for example, then asking them to click on a link or go to a site to sort things out. Instead of winning a gift or reactivating that frozen credit card, users instead get their identities stolen or their

[19] *Ibid.*
[20] M. E. Kabay, Logic bombs, Part 1, Network World Security Newsletter, 08/12/02
[21] Julian Layton, How does a Logic bomb work? *available at*: http://computer.howstuffworks.com/logic-bomb.htm (Visited on February 10, 2022).
[22] Meaning of Logic bombs *available at*: http://en.wikipedia.org/wiki/Logic_bomb (Visited on February 8, 2022).
[23] *Available at*: https://www.securitymagazine.com/articles/96510-salami-attacks-small-deposits-respdf (Visited on February 11, 2022).
[24] *Ibid.*

computers infected with viruses. Phishing remains the most popular form of cyberattack, and it has endured despite all efforts to fight it off. In recent years, phishing has evolved in new directions, such as targeted spear phishing, smishing (via text message) or vishing (using voicemail).[25]

Data Diddling

Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating; recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable.[26] Electricity companies are the one who mostly suffer due to this kind of crime in India. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in the bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.[27]

Data Leakage

Data leakage pertains to illegally copying the master file information of the computer for ransom, blackmailing or any other fraudulent purposes.[28]

Data spying

For spying on the sensitive information of an adversary, their computer network is accessed from a remotely located computer, say a home computer, by using the legitimate password, or breaking the password. The data so accessed is sold to others for a price.[29]

Scavenging

Scavenging is a method of obtaining or re-using the information, which might have been left after possessing, in or around a computer system. The scavenging techniques used in this type of activity are based on physical as well as on technical methods.[30]

Virus

The term computer virus was coined by Fred Cohen in 1985 and has been borrowed from biological science with almost similar meaning and behavior, the only difference is that the victim is a computer system and the virus is a malicious software. A virus is a piece of software code created to perform malicious activities and hamper resources of a computer system like CPU time, memory, personal files, or sensitive information. Mimicking the behaviour of a biological virus, the computer virus spreads on contact with another system, i.e. a computer virus infects other computer systems that it comes into contact with by copying or inserting its code into the computer programs or software (executable files). A virus remains dormant on a system and is activated as soon as the infected file is opened (executed) by a user. Viruses behave differently, depending upon the reason or motivation behind their creation. Some of the most common intentions or motives behind viruses include stealing passwords or data, corrupting files, spamming the user‘s email contacts, and even taking control of the user‘s machine. Some well-known viruses include CryptoLocker, ILOVEYOU, MyDoom, Sasser and Netsky, Slammer, Stuxnet, etc.[31]

Worm Attacks

A worm is a program that spreads to other comput- ers through networks, without the use of an infected host file.[32] An infected host file is a host file attachedwith malicious code, for example a program infectedby a virus. A virus uses infected host files to infect new systems. So if worms don‘t spread by the help of in- fected host files, how do they spread? A worm spreads by creating a new file with a copy of itself and then sending it to new computers. The file is sent through email attachments or different types of file transport protocols, for example the Internet Relay Chat. This means that the worm doesn‘t need to infect any host files on the attacked system to propa- gate.

---

[25] *Available at*: https://www.mimecast.com/blog/types-of-cybercrime/pdf (Visited on January 22, 2022).
[26] *Available at*: http://www.niagarapolice.ca/en/community/computercrimeprevention.asppdf (Visited on January 22, 2022).
[27] *Available at*: http://indiaforensic.com/compcrime1.htmpdf (Visited on January 22, 2022).
[28] Dr. Amita Verma, *Cyber Crimes in India* 80 (Central Law Publications,1st edn., 2012).
[29] *Ibid.*
[30] *Ibid.*
[31] *Available at*: https://ncert.nic.in/textbook/pdf/lecs112.pdf (Visited on January 19, 2022).

[32] Symantec, ―What is the difference between viruses, worms, and Trojans?‖, *available at*: http://service1.symantec.com/SUPPORT/nav.nsf/pdf (Visited on January 12, 2022).

Worms need often very little human intervention to propagate compared to Trojans and viruses. A user needs to actively download the Trojan/virus-infected- file to the computer and then execute it to infect the system. In the case of worms the user just needs to open a document containing the worm to get infected and spread it further to everyone on his or her e-mail list.

Sometimes there is even less human intervention. Another way a worm can spread is through vulner- abilities in the computers connected to the network. These vulnerabilities are found in operating systems, web servers, database servers, etc. The worm searches the network for computers with vulnerabilities. There are different types of vulnerabilities. Some make it possible for a worm to execute malicious code directly on remote computers. The worm doesn‘t even have to send a copy of itself in a file. It can reside in runtime memory and propagate further to new hosts.[33]

Trojans

The name Trojan horse comes from Greek mythology. In the Iliad, by Homer, the legend speaks of how the Greeks had laid siege to Troy, without any victory, they pretended to retreat. But they had left behind a big wooden horse, in which a number of Greek soldiershad hidden themselves. A spy convinced the Trojans,to move the horse inside the city as a war trophy. In thenight, the soldiers left the horse and attacked the Tro- jans. This led to the Greek victory.[34]

Today some writers of malicious programs try to apply the same tactics as the Greek did with their wooden horse. These malicious programs are called Trojan horses or just Trojans.

A Trojan horse is a computer file that claims to be something useful and desirable. The Trojan can either provide the claimed features or just pretend to have them. But under this layer of desirable functions, other unexpected or unauthorized functions are hidden, like the Greek soldiers in the wooden horse.[35]

These unexpected and unauthorized functions do purposefully something the user doesn‘t expect. This may cause unexpected system behaviour but even more seriously a compromised security of the system. The Trojan horse can affect the confidentiality, integrity and the availability of the data on the computer. The confidentiality is affected if the Trojan succeeds in copying confidential data from the system to a nottrusted host. The integrity is affected if the Trojan manages to modify the data on the attacked system. The availability is affected if the Trojan makes it im- possible for trusted users to access the data.

The biggest difference between Trojans and vi- ruses/worms is that Trojans do not replicate them- selves. This means that the Trojan does not copy itself to other files in the system. Even if Trojans do not replicate like viruses and worms, they can be just as destructive.[36]

Trojans need help from computer users to propa- gate to new systems. The user must invite these pro- grams onto the computer to get infected. Similarly to what the ancient Trojans did when they invited the wooden horse into the city Troy.[37]

Denial Of Service Attack

This involves flooding of a computer resource with more requests than it can handle. This causes the resources (e.g., a web server) to crash thereby denying authorized users the service offered by the resources.[38] Popular flood attacks include[39]:

---

[33] Princeton University, ―How Computer Viruses Spread‖, *available at*: http://www.princeton.edu/~protect/BasicConcept sAndTips/Viruses/HowComputerVirusesSpread, (Visited on January 12, 2022).

[34] Micha F. Lindemans, ‖Trojan Horse‖, *available at*: http://www.pantheon.org/articles/t/trojan_hors e (Visited on January 19, 2022).

[35] Trend Micro, ―Virus Primer‖, *available at*: http://www.trendmicro.com/en/security/general/ virus/overview.htm, (Visited on January 19, 2022).

[36] McAfee, ―Virus Glossary‖, *available at*: http://us.mcafee.com/VirusInfo/VIL/glossary_app.asp, (Visited on January 19, 2022).

[37]Symantec, ―What is the difference between viruses, worms, and Trojans?‖, *available at*: http://service1.symantec.com/SUPPORT/nav.nsf/pfdocs/1999041209131106, (Visited on January 19, 2022).

[38] Dr. Amita Verma, *Cyber Crimes in India* 81 (Central Law Publications,1st edn., 2012).

[39]*Available at:* https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (Visited on January 13, 2022).

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks
- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- **SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Distributed Denial of Service (DDoS) attack

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once.[40] The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

- He can leverage the greater volume of machine to execute a seriously disruptive attack
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)
- It is more difficult to shut down multiple machines than one
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

Cyber Defamation

Cyber defamation is a new concept but the traditional definition of defamation is injury caused to the reputation of a person in the eyes of a third person, and this injury can be done by verbal or written communication or through signs and visible representations. The statement must refer to the plaintiff, and the intention must be to lower the reputation of the person against whom the statement has been made. On the other hand, Cyber defamation involves defaming a person through a new and far more effective method such as the use of modern electronic devices. It refers to the publishing of defamatory material against any person in cyberspace or with the help of computers or the Internet. If a person publishes any kind of defamatory statement against any other person on a website or sends E-mails containing defamatory material to that person to whom the statement has been made would tantamount to Cyber defamation.

According to section 499[41] ―Whoever by words either spoken or intended to be read or by signs and visual representations makes or publishes any imputation concerning any person intending to harm or knowing or having reason to believe that such imputation will harm the reputation of such person is said, except in the cases hereinafter excepted to defame that person.‖. however, the punishment is provided under section 500[42] of the Indian Penal Code,1860. In case anyone creates a false document or fake account by which it harms the reputation of a person. The punishment of this offence can extend up to 3 years and fine.[43] Section 503[44] of IPC deals with the offence of criminal intimidation by use of electronic means to damage one's reputation in society. The first case on Cyber Defamation in *SMC Pneumatics (India) Pvt. Ltd.* v. *Jogesh Kwatra*,[45] wherein a disgruntled employee sent derogatory, defamatory, vulgar and abusive emails to the company's fellow employers and to its subsidiaries all over the world with an intent to defame the company along with its managing director, the High Court of Delhi granted ex-parte ad interim injunction restraining the defendant from defaming the Plaintiff in both the physical and in the cyber space. Also, in the case

[40] *Ibid.*
[41] The Indian Penal Code, 1860.
[42] Section 500 ―any person held liable under section 499 will be punishable with imprisonment of two years or fine or both.‖
[43] The Indian Penal Code, 1860, s. 469.
[44] Criminal intimidation—Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation. Explanation. -A threat to injure the reputation of any deceased person in whom the person threatened is interested, is within this section. Illustration A, for the purpose of inducing B to desist from prosecuting a civil suit, threatens to burn B's house. A is guilty of criminal intimidation.
[45] Suit No. 1279/2001, District Court of Delhi.

of *Kalandi Charan Lenka* v. *State of Odisha*[46], the Petitioner was stalked online and a fake account was created in her name. Additionally, obscene messages were sent to the friends by the culprit with an intention to defame the Petitioner. The High Court of Odisha held that the said act of the accused falls under the offence of cyber defamation and the accused is liable for his offences of defamation through the means of fake obscene images and texts.

Cyber Terrorism

Terrorism in today‘s age consists of conventional terrorism, where classic weapons are used to destroy property and kill victims in the physical world and techno terrorism, in which weapons are used to destroy infrastructure, targets and causes a disruption in cyberspace and cyberterrorism is where new weapons like malicious software, electromagnetic and microwave weapons will operate to destroy data in cyberspace to destroy certain aspects of the physical world. Terrorism is a global phenomenon that is not limited to any national borders. Terrorism doesn‘t take into account geographical limitations and transcends the boundaries. Due to the increasing dependence on computer networks and virtual connections, a global sphere in cyberspace has been created which has the greatest potential to be misused, to carry out cyberterrorism and pursue other international terrorist goals. With new technology coming up every day and changes in its usage and development, the risks of potential threats have been rising continuously, ranging from leaking of valuable information to misuse of the power and irreversible consequences across the globe. Some efforts have been made to define cyber terrorism precisely. Most notably, Dorothy Denning, a professor of computer science, has put forward an admirably unambiguous definition before the House Armed Services Committee in May 2000: ―Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.‖[47]

According to NATO (2008), cyber terrorism is *―a cyber-attack using or exploiting computer or communication networks to cause sufficient destruction to generate fear or intimidate a society into an ideological goal.*‖[48]

Cyber Security Policy, 2013

In the year 2013 India introduced its national level cyber security policy. This policy lays down the broad framework for upholding and protecting the cyber space security. The main aim of this policy is to create a broad umbrella of cyber security framework in the country so that the Indian cyber space is secure and free from any kind of attacks both by terrorists and other anti-social elements. However, there is a need to amend this policy to encompass newer methods of ensuring the safety of the ever-evolving cyber space.[49]

Cyber Stalking

According to Oxford Dictionary Stalking means ―pursuing stealthily‖. In simple terms, it refers to extension of physical form of stalking where electronic medium such as computer, internet, e-mail or any other electronic device is used to pursue, harass or contact another person in an unsolicited manner. It generally involve harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person‘s house or place of business, making harassing phone calls, leaving written messages or objects or vandalizing a person‘s property ―Cyber stalking‖ is defined as a crime where the stalkers use internet or any other electronic device to stalk someone.

Online harassment and online abuse are synonymously used for cyber stalking. It involves a conduct of harassing or threatening repeatedly to an individual. Stalking can be done in the following ways such as: to follow a person till his home or where he does his business, to cause destruction to a person‘s property, leaving written messages or objects, or making harassing phone calls. The Cyber stalkers always think that they‘re anonymous and can hide. In other words, the cyber stalker‘s biggest strength is that they can rely upon the anonymity which internet provides to them that allows them to keep a check on the activities of their victim without their identity being detected. Thus, there is a need of efficient cyber tools to investigate cyber-crimes and to be prepared to defend against them and to bring victims to justice. Despite a decade of research by criminologists on the matter, there exists no universally accepted definition of cyber-stalking.[50]

[46]BLAPL No. 7596 of 2016.
[47] *Available at*: https://www.usip.org/sites/default/files/sr119.pdf (Visited on February 01, 2022).
[48] NATO, (2008). Cyber defence concept MC0571. Brussels, Belgium.
[49] *Available at*: https://www.meity.gov.in/content/national-cyber-security-policy-2013-1pdf (Visited on February 01, 2022).
[50] L. McFarlane and P. Bocij, ―Seven fallacies about Cyber Stalking‖ 149(1) *Prison Service Journal* 37(2003)

As a result, the exact scope and boundary of the behaviour, pattern and tactics of cyber-stalkers is majorly unknown.[51]Irrespective of the glaring void in criminal jurisprudence on the point, for the purposes of this paper, cyber-stalking shall be defined as: ―A group of behaviours in which an individual, group of individuals or organisation, uses information and communications technology to harass another individual, group of individuals or organisation. Such behaviours may include, but are not limited to, the transmission of threats and false accusations, damage to data or equipment, identity theft, data theft, computer monitoring, the solicitation of minors for sexual purposes and any form of aggression. Harassment is defined as a course of action that a reasonable person, in possession of the same information, would think causes another reasonable person to suffer emotional distress.‖[52] While this is only one of the several definitions propounded by criminologists, one factor that is accepted universally is the fact that the behaviour of stalking can range from the sending of a non-threatening e-mail to a more serious encounter between the stalker and his target and generally involves behaviour and action that is premeditated, repetitious, aggressive and vengeful.[53]

Cyber Pornography

The word _Pornography' derived from Greek words _Porne' and _Graphein' means writing about prostitutes, or referred to any work of art or literature dealing with sex and sexual themes. Defining the term pornography is very difficult and it does not have any specific definition in the eyes of law as every country has their own customs and tradition. The act of pornography in some countries is legal but in some it is illegal and punishable. Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.[54]

Child Pornography:

The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cybercrime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents onthe internet. According to section 2(da)[55], child pornography is any kind of visual display of overt sexual activity that engages a child. Such content may be an image, a video or any computer-generated picture which cannot easily be differentiated from a real child.Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including theirengagement in sexual positions. Sometimes pedophiles contact children in the chat rooms posing as teenagers or a child of similar age and then they start becoming friendlier with them and win their confidence.

Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them

Following are some of the ways:

(a) Pedophiles use false identity to trap the children/teenagers.
(b) Pedophiles contact children/teens in various chat rooms which are usedby children/teen to interact with other children/teen.
(c) Befriend the child/teen.
(d) Extract personal information from the child/teen by winning his confidence.
(e) Gets the e-mail address of the child/teen and starts making contacts on the victims e-mail address?
(f) Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him are normal and that everybody does it.
(g) Extract personal information from child/teen.
(h) At the end of it, the pedophiles set up a meeting with the child/teen out ofthe house and then drag him into the net to further sexually assault him or to use him as a sex object.

Cyber Bullying

Cyber bullying is similar to that of cyber stalking. But in this case, it involves threats, violence, body shamming, etc. It is offensive and abusive in nature. People post pictures, videos which have content to trouble the victim. It is similar to

[51]EE Mustaine and R Tewksbury, ―A Routine Activity Theory Explanation for Women's Stalking Victimizations‖, 5(1) *Violence Against Women* 43 (1999).
[52] L. McFarlane and P. Bocij, Online Harassment, ―Towards a Definition of Cyber Stalking‖, 139 *Prison Service Journal* 31 (2002).
[53] ML Pittaro, Cyber Stalking: An Analysis of Online Harassment and Intimidation, 1(2) INT'L J. Cyber Criminology 180, 181 (2007).
[54]*Available at*: http://blog.ipleaders.in/cyber-pornography-law-in-india-the-grey-law-decoded (Visited on February 4, 2022).
[55] The Protection of Children from Sexual Offences Act, 2012 (POCSO).

bully but on an online platform. Women are discriminated on the basis of their color, body type, class performance, etc. They are asked to stay away by a particular group of people. Sometimes they are not allowed to involve or associate with a particular group of people. The messages or the mails may include slut shamming, body shamming etc.

Morphing
Morphing is editing the original picture by unauthorised user or fake identity. It was identified that pictures are downloaded by fake users and again Re-posted/uploaded on different websites by creating fake profiles after editing it. This amounts to violation of IT Act,2000 and sec. 43& 66 of the Act. The violator can also be booked under IPC.

Cyber Fraud
Stack manipulation, pyramid schemes, fraudulent bsiness opportunities, offshore scams, are all types of cyber frauds. The internet has made these all the easier with fraudulent schemes.

Credit Card Fraud
Millions of dollars are lost annually by consumers who have credit card and calling card numbers stolen from online databases. Bulletein boards and other online services are frequent targets for hackers who wnt to access large database of credit card information.

Spamming
Spam is the practice of sending unsolicited emails to others. Spam causes immense nuisance, as a recipient without his/her request or consent, becomes the receiving point of unwarranted, commercial and other nonsensical emails.

Industrial espionage
Corporate and commercial espionage are essentially another term for industrial espionage. The term industrial espionage refers to the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. This activity is a covert practice often done by an insider or an employee who gains employment for the express purpose of spying and stealing information for a competitor. Industrial espionage is conducted by companies for commercial purposes rather than by governments for national security purposes. Cyber espionage distinguishes one of the common means for undertaking it and _intellectual property crime‘ covers a broader field to also encompass the substantial trade in counterfeit goods.