IJMRT: Volume (5), Issue 3, 2022
International Journal of Multidisciplinary Research Transactions
(*A Peer Reviewed Journal*)
www.ijmrt.in

ISSN (Print):2663-2381
ISSN(Online):2663-4007

Cyber Crime and Criminals: A Detailed Analysis

Ms. Vidita Saini[1*]

Assistant Professor of Law, Bharat College of Law, Rurki, Haryana, India.

"Torture the data, and it will confess to everything."

Ronald Coase

*Corresponding author

Abstract

We are living in a world that is driven by technology and comprises of machines, computers, computer systems and computer networks. The beauty of this world is that it creates a unique relationship between the software, an intangible component and the hardware, a tangible component. This merger of hardware and software creates a world out of a novel based on science fiction. This global world is an open melting pot of different cultures and practices prevalent in society. This process is evolving and continues without pause for a second. Cyber world is a world unique in its nature made by man without geographical boundaries. This paper will showcase an overview of cyber world with respect to the Internet, online resources, security of information. Further, the focus is on the crimes that are being committed using computer.

Keywords: Computer, Computer Network, Cyber Law, Cyber Space, Internet, Technology, Cyber Crimes, Cyber Criminals.

Introduction

Internet is open to all. In developed, developing and least developed countries also globalization, liberalization and privatization are finding their way through commercial activities. The importance and need of Internet is growing numerously. The emergence of new technologies has made the Internet parallel to life and living. With the booming of these technologies new space has been created for the generation, popularly called as cyber space.

Internet has given rise to new opportunities in every field we can think of. Be it entertainment, business, sports or education. Internet has revolutionized the world. It has made the knowledge so easily accessible.

However the negative side to it is that it has the ability to lead to exploitation. It can be used to steel and destroy worthy information. The important facet of any transaction, whether it is commercial or financial, is the confidentiality that can be easily breached on the Internet. 'Intellectual property rights' in the sphere of computer software, trademarks, copyright, art and design becomes an easy target when there is no appropriate redressal available to the aggrieved party. Internet has also oiled the wheels for perpetrators to commit the traditional crimes through the online platform such as criminal intimidation, cheating, slander, breach of trust, defamation, obscenity, forgery etc. called as cyber crime.

2. Historical Antecedents

The first cyber crime occurred in France in 1820. A textile manufacturer, Joseph-Marie Jacquard business was to produce loom. The device helped to weave special fabrics by repeating a series of steps. This resulted in fear in the minds of employees as this would threaten their livelihood. They committed acts of sabotage in order to discourage the manufacturer from using new technology. This was the first recorded cyber crime. After this the concept of 'cyber space' was introduced in the modern law theory when the Supreme Court of America made a comparison between breach of law in physical space and cyber space in the case of *Reno v. American Civil Liberties Union, 521 US 844*. The court at that time applied the laws of physical world into the cyber space. This judgment resulted in groups of two with different opinion. One group of jurists argued that laws of real space can be applied to cyberspace. But the other group stated that both the space has different territory and hence the same traditional laws cannot be extended to cyber space.

The Timeline to show how the cyber crime has progressed:

1980's: MNC Database (pentagon and IBM) were hacked.

1990's: National crackdown on criminals, Microsoft's NT operating system pierced. This is where hacking started becoming more main stream. Before this, hacking was very much limited to organizations who used computers but in the late 80's internet happened and then we had e-commerce coming in which basically lead to our online retail stores, online banking and online

data stores as well which then lead to criminals hijacking the data or money and trying to steal it on the internet itself.

2001: Cyber criminals launched attacks against eBay, Yahoo, CNN, Amazon and other organizations.

2007: The biggest bank hack ever happened in 2007. Swedish bank, Nordea recorded nearly $1 Million has been stolen in three month from 250 accounts.

2013: Adobe had 2.9 Million accounts compromised and their usernames and passwords released on the open internet.

2016: Kaspersky Lab is a multinational cyber security and anti-virus provider headquartered in Moscow, Russia and operated by a holding company in the United Kingdom. It reported around 758 Million malicious attacks that occurred which they identified themselves.

3. Cyber Crime

With the continuous growth in the cyber crimes, the definition of cyber crime is also evolving. The term cyber crime may be defined as- *"any criminal activity in which computer or/and network is a tool, target, or a place of criminal activity."* The criminal activity also incorporates those traditional crimes which are committed using computer or computer networks. Also the major point of conflict here is that there is no geographical boundary in the cyber space and hence it becomes difficult to decide when rights of Netizens in the eyes of citizens of physical space.

The cyber crime was nowhere discussed properly in the statute or Act passed by the Parliament till early nineties. But it is clear that like conventional crime, cyber crime include an act or omission which causes breach of law. Marc M Goodman, a global strategist, author and consultant focused on advanced technologies on security, business and international affairs says that computer crimes can be bifurcated mainly into three categories:

(i) As crimes where the computer is the target,

(ii) Crimes where computer is the tool of the crime and

(iii) Crimes where the computer is incidental.

In the first category, the attacker attacks the computer of innocent party with intention to do so. In the second one, computer is used as a tool to commit a traditional crime in high-tech way. In the third category, computer is mere incidental. It means perpetrator would have committed the crime anyway; the need of computer was not there. Nandan Kamath says that Internet is

composed of computers and hence it can be said that crimes taking place on internet are computer crimes. Further he states that computer can also become subject of crime if stolen or damaged. It can be the site of crime such as fraud or copyright infringement or it can act as an instrument to access the other machines illegally and hack the confidential information. There is involvement of computer in all these crimes and hence these are termed as computer crimes. Suresh T. Viswanathan defined computer crime as (i) any illegal action in which a computer is a tool or object of the crime; in other words, any crime, the means or purpose of which is to influence the purpose of the computer (ii) any incident associated with computer technology in which a perpetrator by intention made or could have made a gain and (iii) computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data.

There are different opinions with respect to this matter. Some says that crime committed using computer but without Internet are not cyber crime. There has to be an abuse of Internet, geographical boundary, anonymity or speed for a crime to be termed as cyber crime. This would also make difficult for law enforcing agencies and authorities to find out a remedy to this. In some cases, there might be cyber crime alone and in some it might come along with any traditional crime.

4. Cyber Criminology

Cyber Criminology is "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" The term was coined by founding father of the academic discipline Cyber Criminology – Jaishankar to study and explore the cyber crimes from social science perspective. The Cyber Criminology gets tangled with the various other fields like criminology, sociology, internet science and victimology making it a multidisciplinary field.

Belief leads to emotion. Emotion leads to behavior and behavior overtime leads to habit. Cyber security is not just about computer science but it is about behavioral science. We know in behavioral science, one can modify a habit and change someone's behavior. But if the core belief is not addressed, the core behavior will come back. The three core beliefs are:

4.1. I am not important and no one is looking for me.

The cyber criminals are actually looking for people with such belief in their mind. 48% of common man work for small businesses. 49% of small businesses have been hacked. 70% of cyber crime is directed toward small business and 75% of employees have risky cyber behavior. And the companies that have had a critical hack or a severe attack, 60% of them go out of business in under 6 months. Data is collected by Adam Anderson- An IT specialist and an EX-NSA agent.

4.2. I don't have anything anyone would want.

The subject here is not only the intellectual property or trade secrets but money as well for which the hackers would disrupt the life of victim until they get it. Further it affects the businesses, laptops, personal computers etc. When they find the vulnerable target, they touch all these computers and take the personal information and data out of it.

4.3. I can't stop them even if I wanted to.

This belief is boosting the morale of these bad guys harassing the people online for their benefit. One can create a protecting wall by practicing good cyber hygiene. A good cyber hygiene mean to have a systematic way of backing the data up somewhere else in responsible hands who keeps check on the progress and when something goes wrong can help to put the data back. Cyber security policy be taken not to pay to the hackers but to get the professional who can help respond to the disaster. By adopting these beliefs into the core being, one will be able to avoid the horrible consequences suffered online.

5. Why Cyber Crimes Are Committed

Cyber crime is prompted by factors like new technologies, complexity and loss of evidence. Computers can be accessed through these complex technologies. These technologies are installed to have unauthorized access to computer. Like keyloggers can steal the access codes by bypassing firewalls and getting into the system. The reasons behind vulnerability of computers could be listed as:

(i) Capacity to store data in compact form

The primary characteristic of computer is to store large amount of data in a little space. This makes it easy for perpetrator to derive information through physical or virtual medium.

(ii) Easy to access

The problem faced while guarding a computer system is that there is chance of breach due to complex technology. By secretly implanting logic bomb, key loggers can steal retina imagers, access codes, advanced voice recorders that have the ability to fool biometric systems and bypass firewalls and get access to security system.

(iii) Complex Formation

The operation of computer depends upon operating systems which are composed of millions of codes. The fallible mind of human can result in error and the cyber criminals take advantage of such situations and get unauthorized access to the computer system.

(iv) Negligence

Negligence has direct connection with the human conduct. This is why it is probable that while working on computer system there might be some negligence which results in providing access to cyber criminal.

(v) Loss of Evidence

It is very common problem of losing evidence as the routine practice of destroying data is there. Moreover, the territorial jurisdiction of cyber space is unlimited and collection of data from there is too difficult. This aspect paralyses the system of crime investigation.

6. Classification of Cyber Crimes

Crime is a social phenomenon. It is an act prohibited by law. Cyber crime is the most complicated issue at hand in the cyber world. Any illegal or unethical activity done through the use of computer becomes a cyber crime or using computer as a tool forms the cyber crime. Cyber crime is rapidly on the rise. It has surpassed illegal drug trafficking as a criminal moneymaker. In 2015, UK consumers lost 1.7 billion Euros to cyber crime. The National Crime Agency, UK believes that *"organized crimes have taken advantage of the opportunities presented by the internet, particularly the growth in e-commerce and online banking."* Cyber criminals try to exploit the broken software. They either create or sell the broken software and untested software. Cyber crimes are specific in nature that includes cyber piracy, cyber trespass and cyber vandalism. Cyber related crimes can be further bifurcated into two, Cyber exacerbated and cyber assisted. Cyber exacerbated includes cyber stalking, internet pedophilia and internet pornography within its ambit.

Cyber assisted crime includes online tax fraud. The other form of these cyber attacks are hacking, D.O.S, virus dissemination, credit card fraud, phishing, spoofing, cyber stalking, and salami attack. Cyber assisted crimes are those where the computers are used as tools to assist a particular crime. For example: frauds or online bank hijacking where hackers hack into a bank and digitally steal money from the bank.

Computer as the target of crimes is a section where the computer itself was a target of a crime. For example: A denial of service attack or viruses which rendered the computer useless or sniffing of data packets on the network thus compromising passwords and other confidential information.

In the third category, computer is incidental to the crime where it is used as a temporary measure to store some data such as child pornography or some other data which made the computer incidental to the crime.

The definition of cyber crime is generalized as- *"unlawful acts wherein the computer is either a tool or target or both."* Cyber crimes can be bifurcated on the grounds of- (a) subject of crime, (b) Against whom crime is committed and (c) Temporal nature of criminal activities in cyber space.

The subject of crime can further be divided in three groups. These are:

(i) Against Individuals

It may be against individual persons or their property. Cyber harassment is a distinct Cybercrime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. The crimes that can be committed against individual persons are:

- Harassment via e-mails
- Cyber-stalking
- Dissemination of obscene material
- Defamation
- Unauthorized control/access over computer system
- Indecent exposure;
- Email spoofing

- Cheating and Fraud. (Credit card/debit card fraud involves an unauthorized use of another's credit or debit card information for the purpose of purchases or withdrawing funds from it.)

The cyber crimes committed against the property includes computer vandalism (destruction of other's property), transmission of harmful programs, unauthorized trespassing through cyber space, and unauthorized possession of computer information. The motive here is not to get the data but to destroy it so that the user cannot get benefit out of it. The crimes that can be committed against individual property are:

- Computer vandalism
- Transmitting virus
- Netrespass
- Unauthorized control/access over computer system
- Intellectual Property crimes
- Internet time thefts.

(ii) Against Organization

The attack could be against Government, a firm or a group of individuals. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyber space is being used by individuals and groups to threaten the international governments and also to terrorize the citizens of a country. The crimes that are committed against an organization are:

- Unauthorized control/access over computer system
- Possession of unauthorized information
- Cyber terrorism against the government organization
- Distribution of pirated software.

(iii) Against the society at large

The crimes committed against society are:

- Pornography (largely child pornography/child sexually abusive material (CSAM))
- Polluting the youth through indecent exposure
- Trafficking
- Financial crimes
- Sale of illegal articles

- Online gambling
- Forgery.

However it is to be noted here that all the lists mentioned above are not exhaustive in nature. Traditional crimes also come in the ambit of cyber crimes whenever there is involvement of computer in commission of crime. Moreover, crimes like cyber stalking, hacking, unauthorized access, denial-of-service attack, malicious crime (including use of virus), E-mail bombing, Salami attacks, Data diddling, Web jacking, Cyber Pornography etc. are addition to the list of cyber crime that have emerged with time and became popular.

A. On the basis of commission of traditional crimes: the classification of cyber crimes can be done in following category:

(i) Cyber Theft

When a person without the permission of owner moves something from his computer it is termed as cyber theft. For example- Breaking into computer placed in some part of globe and removing money from the bank account of one and transferring it to the account of another. The theft took place here in this case even without any physical act.

(ii) Cyber Trespass

The information on the Internet can be protected with the help of passwords. The passwords act as barrier for those who do not have right to access to that particular account. Breaking this barrier and getting access to the owner's account (someone else's property) is punishable.

(iii) Cyber Violence

When the cyber activity of a person or group of persons has violent effects on the other person or a community or social group or a country, then it is termed 'cyber violence' There might not be a direct physical impact but victim feels the mental impact.

(iv) Cyber Obscenity

The term cyber obscenity embodies the principles of Section 292 and 293 of Indian Penal Code. It discusses the presence of obscene materials on the Internet. The Governments of various countries are working to regulate these crimes. The nations try to achieve this goal by making specific law on Internet or through the extension of existing traditional laws. In India, the *Arzika* case became first in this regard where the case related to online obscenity was registered. In another case of *State of Tamilnadu v/s Dr L. Prakash (Fatima Riswana v. State Rep. by ACP., Chennai & Ors AIR 2005 712*) the

doctor used to take private pictures of his women patients. The judiciary took a strong stand against this educated professional and awarded life imprisonment to him.

(v) Cyber Forgery and Fraud

Fake mark sheets, revenue stamps etc. are made using high quality scanners and printers. In October 1995, Economic Offences Wing of Crime Branch, Mumbai seized 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores. These certificates were prepared using desktop publication systems. The most familiar crime on Internet is fraud. There are many crimes in which fraud may manifest itself. In auction fraud, seller posts and advertises about an item in an auction site. The buyer agrees to buy the item and forwards the money. But the seller fails to deliver the item because of theft.

'Phishing' is another method used to collect information from individuals who are least suspected target to commit crimes associated with identity theft. For instance- credit card fraud. These frauds are committed by theft of physical card or by compromising the data associated with the account. This is the other method used to scam the users by sending e-mails (seemingly legitimate looking) or designing web pages in order to collect the online bank information, debit/credit card details or other login information. The users fall prey to these messages and end up giving the confidential information.

(vi) Intellectual Property Crimes

Intellectual property includes the concept of copyright, trademarks, patents and designs. The crimes related to intellectual property mean violation of their rights related to these laws. Online infringement of trademarks, copyright, theft of source code etc. also fall in this category.

B. On the basis of new crimes: Cyber crimes can be classified into following categories-

(i) Cyber Stalking

An act to frighten or threaten the other person to harass using the electronic means is termed as cyber stalking. It is done to stalk someone using Internet messaging service or any other electronic means. The cyber stalkers follow the activities of victim on the online platform. They target victims using bulletin boards, chat rooms and online forums. After gathering their information they post it on the web pages to get reaction from the victim and initiate contacts. In case of response from the victim the stalkers then start tracing victim's online activities. This can further leader to physical stalking and victim might experience abusive phone calls or obscene mails. The various websites

used by stalkers are- http://www.switchboard.com/ and http://www.whowhere.com/. People can request for removal of themselves from such site.

The first case of cyber stalking in India is *Manish Kathuria v. Ritu Kohli (C.C. No. 14616/2014)* in which the girl was being stalked by former colleague of her husband. The case was solved by the agency but since Indian cyber law was not passed at that time, the offence was considered a minor one.

(ii) Cyber Pornography

The offence includes pornographic websites and magazines made, transmitted or downloaded using computers. The first case of this kind of offence is of 2001 of a student of *Air Force Bal Bharati School, New Delhi* who created a website containing sexual details about the girls and teachers of the school. They were classified on the basis of their sexual preferences. He then dedicated the website to the school. When this matter came to light, father of one of girl student registered a case under Section 67 of the IT Act, 2000 with Delhi Police Cyber Crime Cell. The student was arrested and kept at Timarpur (Delhi) Juvenile Home from where he was granted bail after one week.

(iii) Unauthorized Access

Access control is to restring the entrance to a property, or a room of an authorized person. The Access control by mechanical means can be realized using keys and card access system. Thus, unauthorized access means any access without permission of the owner or authorized person of a computer, computer system, computer network. It will also include switching on a computer system of other person without his permission. The techniques used to have unauthorized access are: Packet sniffing, tempest attack, password cracking and butter overflow.

(iv) Hacking

To gain the unauthorized access to the system profit, protest, information gathering or to evaluate system weaknesses, it is the most popular crime in cyber space. It is fact that no computer system on this earth is secured from hacking. Any system can be hacked. IT Act defines hacking under section 66. “Hacker” is an amateur computer programmer who discovers ways to make software run efficiently. “Hacker” is the person who writes computer programs, modifies computer hardware, with computers or electronic devices for enjoyment. Hackers hack till he achieves his aim. Hacker is defined as one who breaks into computer network of others with an intention to steal information. This is a crime with essential ingredients: (a) Intention to cause wrongful loss or damage to any person, (b) knowledge that wrongful loss or damage will be caused to that person due to

his act, (c) the information in the computer must be destroyed or deleted or altered or diminished in value or utility or are affected injuriously.

(v) Denial of service Attack

Distributed Denial of Service is initiated by sending demands to victim's computer that exceeds the limit of server and thereby causes crash. Flooding a computer with more request than it can handle causes the computer resource to crash and go offline and thus denies access to authorized users. To control such attacks is a difficult thing to do. The hacker tries to consume the resources of the victim server in such a way that there are no resources available for legitimate users to connect to the server and conduct their business. This is the most common cyber attack in today's world. The classic example of DOS attacks are those that brought down websites like CNN, Yahoo Amazon etc.

(vi) Virus and Worm Attacks

The programs that associate themselves to computer or file and then circulate themselves to other files and to other computers on a network are called viruses. This involves direct or search unauthorized access to the system by introducing malicious programs such as viruses, worms etc. Worms can stand alone but the virus needs host. These viruses impact the particulars on the computer badly by deleting or altering it. On the other hand, worms do not require the host to attach themselves to. Worms create functional copies of themselves and repeat this process till they obtain the whole accessible space on a computer's memory. VBS_LOVELETTER also termed as Love Bug or I LOVE YOU virus utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses with the subject "ILOVEYOU". The attached file is named "LOVE-LETTER-FOR-YOU.TXT.vbs" with the message – "kindly check the attached LOVELETTER coming from me". Such catchy words make people a target easily. Often people do not notice the tiny .vbs extension and believe it to be a text file. The question is how it works. .VBS_LOVELETTER first selects certain files and then inserts its own code in place of the original data in the file. This way more and more versions of virus takes birth and keep on increasing.

(vii) Personal Attack

Personal Attack: The attack on the personal data of the user. It includes the email spoofing, telephone spoofing and letter spoofing. An e-mail is spoofed if it appears to be originated from one source but actually comes from other. It can damage the person reputation and can cause him lots of troubles. The classic example of e-mail spoofing is *Nigerian Email Scam Case* where Nigerian persons residing in Mumbai used to send

fake mails to the persons and misinterpret that they will be given services in England. Fake messages of winning lottery were sent to induce to deliver money as processing fee in the case of *State Vs Opara chilezien Joseph & Ors (Regular Criminal Case No. 724/2012)*

(viii) Logic Bombs

Such bombs are event dependent programs. They are initiated when an occasion is there. Sometimes logic bombs are used to work on a particular date only.

(ix) Salami Attacks

These attacks are made in the financial area i.e. associated with electronic data interchange and electronic banking. Generally their affect on the data is so small that it gets unnoticed. *The Ziegler case* is a classic example of salami attack where a logic bomb was initiated in the bank system and 10 cents were deducted from each account opened in the bank and was deposited in the account of person named Ziegler. The amount withdrawn was so small that neither the bank nor the account holders took notice of it. This came to light when a person named Zygler opened his account in that very bank and large amount of money got transferred in his account. On the top of this, it happened every Saturday. Later, bank authorities unveiled this scheme.

(x) Data Diddling

In this attack raw data is altered just before computer could process it and then again changes it after the process gets complete. In India, Electricity Boards becomes victims to data diddling when private parties operate their computer systems.

(xi) Email Bombing

This involves bombing of e-mails in large number to the e-mail account of victim so as to result in crashing. To illustrate- A foreigner was residing in Shimla for thirty years. He applied to avail a scheme of Shimla Housing Board in which land could be bought at lower prices. But owing to his citizenship of foreign country his application was rejected. In anger he sent mails to the Shimla Housing Board in thousand, enough to crash their server.

(xii) Trojan Attacks

This origin behind this specific term is- 'Trojan Horse'. Software field defines it as unauthorized program which takes control over the system of other by posing it as an authorized one. Trojan is installed in the system generally through e-mail. For example- A Trojan was installed in the computer of US film director through the web came while

she was chatting. The cyber criminal then copied her personal pictures and harassed the lady director.

(xiii) Web Jacking

The term derived from Hi-jacking is used when there is a forceful control of a website by someone unauthorized. This is usually done by cracking or bypassing the password. Once the hacker gets access, he can make changes to the website as he desires. The popular case of web jacking is 'gold fish case'. A site was hacked in this case and information related to gold fish was altered. Further 1 million US dollar was demanded as ransom.

(xiv) Cyber Terrorism

Cyber crime as well as cyber terrorism both falls under the category of criminal acts. However, they both are different from each other in many ways. Cyber crime is a domestic problem which sometimes could have international consequences but cyber terrorism is all about global issues. It deals with both domestic and international perspectives. Terrorist attacks take place on Internet by hate e-mails, DOS, targeting sensitive computer networks etc.

The recent example of terrorist attack is of Osama Bin Laden, the LTTE. Attack on Army Development system of America during Iraq war is another example to it. Cyber terrorism can be defined to be "the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives". Another definition of cyber terrorism covers all the aspects of it. A terrorist is a person who engages in wanton killing of people or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to –

- Put the public or any section of the public in fear; or
- Affecting adversely the harmony between different religious, racial, lingual or regional groups or castes or communities; or
- Coercing or overawing the government established by law; or
- Endanger the sovereignty and integrity of the nation.

Similarly, cyber terrorist is that person who achieves all these above mentioned objectives through the means of computer or computer network. Any act done in pursuance of same will be considered as an act of cyber terrorism.

(xv) Computer Vandalism

Computer vandalism means to destroy or damage the property belonging to another. It involves any physical harm to the computer of any person. The theft of computer or some part of computer or attached material to computer will also be included in computer vandalism.

(xvi) Drive by attack/ Cross site scripting attack

Where the web applications get compromised and scripts are embedded within those applications or within the commands that are sent out by the users.

(xvii) Distributed Attack

The distributed attack can hit the PC or mobile device through various ways. This includes encryption or ransom ware. Hackers encrypt the files and hold the data to ransom.

(xviii) Browser Manipulation

The browser manipulates what you see on your browser and steals your data. For example: the malware inserts a few extra lines of code into the bank's website. The website looks the same but the malware is stealing your data.

(xix) Keylogger

This malware sits in the background of the PC and captures what you are typing to learn your behavior and potentially catch your personal data.

(xx) Central Attack

A central system is hacked in a bid to get customer data usually for financial gain through central attack. Alternatively, a central attack may be one in the name of hacktivism for moral, social or political reasons. A prime example of central attack is "The Ashley Madison hacking scandal in 2015" which saw the thousands appliance from the infidelity dating website have their personal details stolen with the threat of exposure if the parent company didn't shut down.

(xxi) Password Attacks

Under these attacks, hackers try to compromise the passwords of users by tracking them based either on group based attacks or password guessing.

(xxii) Eavesdropping Attack

These could be physical in nature where somebody overhears what you are saying or tries to capture data packets that contain your voice transmission. For example through Skype based call.

(xxiii) Secret Injection Attacks

Again here the attackers target the database and try to send in the malicious queries which will compromise the database and the data within.

(xxiv) Birthday Attacks

These attacks are based on cryptography where permutations and combinations of how algorithm functions are looked and then looking at how the permutations on how many times the processing needs to be done for that algorithm to be reversed.

(xxv) Malware Attacks

There is malicious software that delivers a Trojan virus or a worm to the victim thus infecting the victim's machine and rendering it useless.

(xxvi) Man-in-the-middle attack

Here the hacker would put himself in between your machine and the router and start sniffing the data packets that you are sending thus trying to compromise information contained within those packets.

There are various methods through which these attacks are launched and that is where the cyber security expert comes in with their knowledge of identifying what exactly is a threat to the organization and how they are going to prevent it from happening.

7. Cyber Criminals

Any criminal commit a crime with an objective in his mind. Similar is the case for cyber criminals. These objectives form ground for categorization of cyber criminals. The first category includes children and teenagers of 8 to 18 ages who by nature are curious to explore and know new things. Internet comes with both advantages and disadvantages. The guardian and educational institutions must teach students about the same. The awareness in students about the good and bad effects of Internet will itself eliminate this category from the list of cyber

criminals. The other category is of *hackers.* Some hackers have political objectives in their mind and some indulges in these activities to get confidential material of the opposite party. The other kind of hacker hack the valuable information of their enemies to put them in problems and controversies.

Having a computer hacked can be life altering! We are fearful of hackers and those who want to engage in identity theft. The hackers these days are international sophisticated groups. Sometimes hundreds of people who have multiple tiers of org chart some of whom are working in almost a call center which will see some pictures of who are also working at higher levels of cartel like infrastructure. When they actually begin these attacks they don't stop until they get everything one possess. So, the more vulnerable the individual or organization is, the more they go for this kind of trick. The more likely it is that they will actually get all of the home equity, all of the balance of one's credit card, all of the money in the bank accounts and then add it to the database that they then sell to other criminals so that they can hit you with the next attack. But the question is why does this keep happening? Hackers make a virus or worm or call the victim or use a fake cell tower to actually intercept the radio coming from the devices. Attack on the things like *"Internet of Things"* or cellular empowered drones or self-driving vehicles or smart televisions or smart fridges or such similar things are even better for the hackers as these things do not complain. The attack will hit them and this cycle will go on until somebody gets a bill for 2 million dollars.

7.1. Types of Cyber Criminals

When it comes to protecting your business from a data breach, you will want to be on the lookout for a new kind of criminal i.e. the cyber kind. They can be tough to spot. But if one can recognize these common cyber-criminal threats, it will save the organization from a costly but preventable cyber attack. The categories of cyber criminals are:

1. **The social engineer**

Cyber criminals fake an identity and request data rich information like to fill out tax form frequently in a time pressured scenario.

2. **The spear phisher**

These thieves send malicious emails altered to appear legitimate containing links that unlock access to banking credentials, trade secrets and personal information.

3. Hacktivism / Organized hacktivists

Most confirmed data breaches are the result of hackers leveraging weak, default or stolen passwords. Organized hacktivists are the people who promote a political agenda by hacking especially by defacing or disabling the websites. The difference between the suicide hackers and the hacktivists is that suicide hackers have a social cause that they want to promote but the hacktivists have a political agenda.

4. The rogue employee

Current or former disgruntled workers can abuse their insider access and knowledge.

5. The ransom artist

The growth of ransom ware as a service makes it easier for bad actors to seize control of data and force businesses to pay them.

6. Kids/Script kiddie (age group 9-16 etc.)

A script kiddie is an unskilled hacker who compromises systems by running script tools and software already developed and made available by real hackers. They have very minimal technical knowledge. They have no idea how the attack works. They just use an automatic tool and hope that the attack succeeds.

7. Cyber Terrorist

These are the individuals with wide range of skills motivated by religious or political beliefs to create fear by large-scale disruption of computer networks. For example: organizations like ISIS who have lot of digital propaganda that they use and target weak-minded people to join their causes or people who spread ransom ware who terrorize organization and hold them to ransom and demand money from them by encrypting their data.

8. State Sponsored Hackers

The individuals employed by the government to penetrate and gain the top secret information and damage information systems to other governments are state sponsored hackers. For example: Cyber wars going on between the countries. This is why most of the countries nowadays have a secret cyber cell consisting of highly skilled hackers who are entrusted with the task of spying on the enemies and trying to gather information by hacking into their infrastructure. This is not a legit job; it will always be masked by an alleged organization.

9. Black Hat Hackers

The individuals with extraordinary computing skills resorting to malicious or destructive activities are termed as black hat hackers. These are the criminal hackers who try to profit from their crimes. They have malicious intent in trying to hack a victim organization.

10. Grey hat hackers

These are the individuals who work both offensively and defensively. It mean they could work as black hat hackers with malicious intent and try to harm some organization while on the other hand they would also try to work as a security analyst and try to enhance the security posture of an organization for remuneration.

11. White hat hackers

The white hat is what we want to be or what we want to achieve ourselves as. An individual, who professes the same skills as a black hat hacker and uses the same tools, has the same kind of knowledge but the intent is different. They use them for defensive purposes and there is no malicious intent. They act with authorization from the organization and they try to detect any flaws and try to plug out those flaws so that black hat hackers would not be able to misuse those flaws to gain access.

12. Suicide Hackers

These are the individual who aim to bring down critical infrastructure for a cause and are not worried about facing jail terms or any other punishments. So, any organization or group of people, for example anonymous or these kind of organized hackers who have a political cause or a social cause that they want to promote and they achieve this aim by hacking the critical infrastructure of organizations, defacing the website. These are not put in the category of black hat hackers because unlike them suicide hackers would not try to hide their identity. On the other hand black hat hackers will always have a fake identity that they will utilize and try to hide behind it. Suicide hackers take responsibility for the acts that they have done and boast about it and are not worried about the repercussions for the attacks.

8. Conclusion

Cyber as defined under Merriam Webster is "*relating to or involving computers or computer network such as the internet*" and hence it can be put that real or virtual world of information in cyber space is called Cyber World. The definition suggests that in its ambit cyber world contains the concept of cyber space, cyber security, cyber safety, cyber crimes and the law dealing with the respective branches to cater the growing offences in the society. Internet has dramatically changed our life. We are living in era of internet society. It changed our life rapidly and the human being saw the transition from paper to paperless world. Since the laws of real world cannot be interpreted in the light of emerging cyberspace, we needed the law governing cyber space. Cyber Law is the branch of law that deals with any illegal act committed using a computer network (especially the Internet). Cyber crime is a subset of computer crime. The term *"Cyber Crime"* proposed by Sussman and Hueston cannot be actually described by a single definition. The Cybercrime also known as electronic crimes, computer-related crimes, e-crime, high-technology crime, information age crime are the crimes that takes place over electronic communications and affects the computer data or systems. These crimes are illegal activities where there is no need of physical presence of the offender and hence we see constant rise in the volume of cyber crimes. Cyber criminals prefer to function from those countries where there are weak cyber laws so as to avoid chances of being caught. Also, there is a myth that cyber crimes takes place only in the cyber space but the truth is that it is not necessary for a cyber criminal to be online to commit cyber crime. The classic example is of software piracy.

Other than these, new crimes have also arisen with the use of Internet. Already present laws and regulations are not fit enough to deal with the malpractices in cyber space. Further, there is no cop surveillance over the transactions done through this channel. The absence of legal structure compels the users to rely on technical methods to save themselves from the perpetrator. All this combined together represents the need for framework to tackle the problems that have come along with the Internet and hence to regulate the cyber crimes committed in the cyber space. Hart in his work, *The Concept of Law* has said *"human beings are vulnerable so rule of law is required to protect them".* Putting this equation to cyber space and we find that computers are vulnerable and thus rule of law is must to shield them.

As we discussed, cyber crime with the passage of time has now developed into a threat against mankind. Keeping the safety and security of the country in consideration, the Government of

India passed Information Technology Act, 2000 to govern the issues related to cyber crimes. The Act revises the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 to bring at par with it. Wide efforts are being taken to address prevention, response, and cooperation. Across the globe, industries are establishing information sharing and analysis centers (ISACs) to share real-time information related to threats, vulnerabilities, attacks, and countermeasures. A recent Global Information Security Summit sponsored by the World Information Technology and Services Alliance (www.witsa.org) brought together industry, governments, and multilateral organizations across economic sectors to share information and build partnerships. Post-summit working groups are now developing cooperative approaches addressing the most critical information security problems. But all the legislation will go in vain without the active participation among the member countries. It is also true that owing to trans boundary nature of cyber crimes, the menace of cyber threats cannot be curbed to the fullest extent. In fact it sometimes destroys the legislative wisdom. In India, since we don't have a super legislation covering all forms of cyber crimes, becoming party to the respective international conventions and treaties is desirable so that we can implement those provisions by enacting relevant municipal laws in that regard.

REFERENCES

[1]. A. Goldfoot, "Antitrust Implications of Internet Administration", 84 (Virginia Law Review 909 (1998))
[2]. David S Wall, "Policing and Regulation of Internet", (Criminal Law Review) Special Edition 81(1998).
[3]. Dr. Farooq Ahmad, Cyber Law in India :Law on Internet (New Era Publications, 4th Edition 2011)
[4]. H. L. A. Hart, The concept of law (Oxford: Clarendon Press, APA 6th edition, 1961)
[5]. K. Mani, Legal Framework on Cyber Crimes (Kamal Publishers, Edition: 2008)
[6]. K. Jaishankar, Cyber Criminology: Exploring Internet Crimes and Criminal Behavior (CRC Press, Taylor and Francis Group, Edition 2011)
[7]. Marc M Goodman, "Why the Police don't Care about Computer Crime?" 10 Harvard Journal of Law and Technology 468 (1997).
[8]. Nandan Kamath, Law Relating to Computers Internet and E-commerce 22 (Universal Law Publishing Company Pvt. Ltd. New Delhi(2000))
[9]. Suresh T Viswanathan, The Indian Cyberlaw13 (Bharat Law House, New Delhi (2000))
[10]. Sussman and Hueston, Cybercrime and Cybercriminals: A comprehensive study (Springer International Publishing, 1995 Edition)
[11]. Vishnu Konoorayar, "Regulating Cyber space: The Emerging Problems and Challenges" (Cochin University Law Review, Vol. 27 (2003))
[12]. http://www.bezaspeaks.com/cybercrime/history.htm
[13]. https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm
[14]. https://www.careeranna.com/articles/cyber-crime-and-their-prevention/
[15]. https://www.youtube.com/watch?v=c_2Ja-OTmGc
[16]. https://www.projectfive.co.uk/2016/07/12/types-of-cybercrime-and-how-to-avoid-them/
[17]. https://en.wikipedia.org/wiki/Online_predator
[18]. https://criminal.findlaw.com/criminal-charges/crimes-against-the-person.html
[19]. https://www.igi-global.com/dictionary/investigating-cybercrime-in-nigeria/82852
[20]. https://www.toppr.com/guides/business-laws-cs/cyber-laws/classification-of-cyber-crimes/
[21]. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6428311/
[22]. https://www.scribd.com/presentation/152082666/Forgery-defamation-cyber-stalking

[23]. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/intellectual-property-crime
[24]. https://study.com/academy/lesson/what-is-a-worm-virus-definition-examples-removal-tools.html
[25]. https://www.cybercrimechambers.com/blog-salami-slicing-attack-84.php
[26]. https://lawsisto.com/legalnewsread/NjQyNg==/DETAILED-OVERVIEW-WEB-JACKING
[27]. http://jayantcci.blogspot.com/2013/09/web-jacking.html
[28]. https://timesofindia.indiatimes.com/topic/osama-bin-laden
[29]. https://study.com/academy/lesson/vandalism-in-digital-crime-types-evidence.html
[30]. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
[31]. https://fnfaruk.blogspot.com/2019/06/what-is-cyber-crime.html
[32]. https://phoenixnap.com/blog/cyber-security-attack-types
[33]. https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf
[34]. https://theconversation.com/global/topics/computer-hacking-2497
[35]. https://www.travelers.com/business-insights/topics/cyber/5-types-of-cyber-criminals
[36]. https://www.merriam-webster.com/dictionary/cyber
[37]. https://www.pandasecurity.com/en/mediacenter/panda-security/software-piracy/
[38]. https://www.buguroo.com/en/blog/the-worlds-top-3-cybercrime-and-online-fraud-hotspots