Volume II ISSUE III ISSN NO : 2582-6034

LEGALFOXES LAW TIMES

CYBER CRIMINOLOGY:

A STUDY OF CYBER CRIMINAL MIND

By Avantika Mishra and Apoorva Dewan

ABSTRACT

The term "cyber-criminal" sounds like something out of an action film, but is all too real, and they are creating unpredictable chaos in our virtual world. If we analyse the number of people that use the internet the results would amaze you. On one hand, the information technology has helped a number of people of different age groups, having different interests and skills to achieve their goals and objectives especially in this difficult time when everything shifted to the online portals whether it be the schools, universities, and even thebusinesses but on the other hand, the internet is posing adisparaging effect on the life of the people using it. As the internet is easily accessible from any part of the world and by any person, many people can use this platform to do illegal activities and commit a crime. Ergo, even if it appears that the web has bought people closer, there is a flip-side to it.Many laws and acts have been passed in order to curb this evil such as the Information technology act, 2000, National Cyber Security Policy etc but it is still at rise.

The object of this research paper will be to understand cybercrime fromthe context of criminology. It will help you to understand the psychology of cybercriminals and what motivates them to commit such offenses which are having a negative effect on the life of others and leading to increase in suicide rates, depression, anxiety and other mental health issues and precautions and steps are needed to be taken in order to curb such a malicious crime.

I. INTRODUCTION

The easy access to the use of computers has exorbitantly affected the way in which individuals from all around the world carry out their lives.The substantial improvements in the cyberspace are assisting in making the lifestyle of people more laid back and comfortable but theirsquander can have an extremely negative ramification on the lives of people.

Almost every netizen has encountered at some point in their life one if not many cybercrimes against them, be it attack on their privacy or their very identity. These criminals are getting together on the platform known as "Dark Web" in order to effectively commit crimes anonymously. The paedophiles are using these platforms to sexually abuse or assault the minors, people are being bullied and even stalked to the extent that they are facing mental health issues such as depression, anxiety, insomnia and even suicidal thoughts.

To acknowledge what these people are contriving by effectuating such redundant strain on other people's life by doing acts such as cyber bulling, aggression, stalking and many more such deeds and for understanding what really motivates them to do all these spiteful activities various traditional criminological and psychological theories are explained below in relation to cybercrime:

1. **Rational Choice Theory[1]:** This theory is a result of classical school of criminology. As per this theory people rationally make a choice in life, ifa person is given two options, he would analyse those options and choose the one which he thinks will benefit him the most at present,even if the choice made can have a negative impact in future like paying monetary or legal sanction or loss of respect in the society.

For instance, while committing the crime of piracy an individual will consider that if he bought the movie instead of downloading it, it would have costed him a certain sum of money but if he downloads it in this way he may or may not be caught for the same so as the benefit outweigh the negative he will go for the later one.

Therefore, according to this theory a cybercriminal like any other criminal does the offence after thinking rationally and forextrinsic benefit such as money, or some other material benefit, as well as intrinsic benefit for instance happiness, thrill etc.

[1] Rational choice theory *available at*https://www.investopedia.com/terms/r/rational-choice-theory.asp

2. **Self-control theory[2]:**The self-control theory was propounded by M. R. Gottfredson and Hirschi in the year 1990. This theory aimed to institute a general theory of crime. This theory specifies that every human have capability or tendency of committing an offence if he gets a chance to do it. But not everyone becomes a criminal this is due to the distinction in the level of self-control of each individual.

The main reason of commission of an offence is lack of self-control. People usually acquire the skill of self-control with age due to the hormonal development, meeting different people, education and the legal sanctions that they will have to undergo if caught.

A person who has lower self- control will be more susceptible to engaging in criminal activities such as usage of drugs or abuse to alcohol. These people as they lack in self-control are risk-taking, adventurous, impulsive, and insensitive to others.

Therefore, the lower an individual's self-control, lower will be the perceived risks of formal and informal sanctions against the offences related to the computers.

3. **Deterrence Theory[3]:** Deterrence theory of crime was formulated by Cesare Beccaria and Jeremy Bentham as a means to explain the crime and to develop a method to reduce it. It was believed by them that there was no evil in people, this was in contrary to what criminologists of that era assumed. As per Beccaria, Crime was rather a result of inadequate law. He speculated that how effective a law is would depend on how the punishments are supervised.

If the punishment of doing an offence outweighs the reward a person will not commit an offence as a criminal would choose to either follow or break the law after scrutinizing the risk and reward of their actions. For instance, Ram and some of his friends were coming back from school when someone suggested breaking the window of the principle's car. Ram thought 'that if he gets caught, he will get in a lot of trouble'. As Ram did not want to get into any hassle, he decided not to break the window and went home. This is how deterrence plays an important role in making people obey the law.

[2] "Self-control theory" *available at* http://criminal-justice.iresearchnet.com/criminology/theories/self-control-theory/
[3] Patrick M. Morgan "The concept of deterrence and deterrence theory" 2017

As the cases of Cybercrime is on the rise, it can be said that the law for the same is ineffective. Cybercriminals believe that they can easily escape the liability as legal sanctions regarding cybercrime is not stringent. Ergo, this transgression can only be stopped if the perceived deterrence on commission of a cybercrime is stronger so that the discern external and internal benefit seem unfavourable.

4. **Routine Activity Theory[4]:**Routine activity theory also presumes that delinquents are rational and sybaritic. This theory is one of the main theories of 'environmental criminology'.

The RAT theory states that the occurrence of a criminal offence takes place when three components or elements come together. First, an ***accessible target*** which can be any person, thing or place which is easily available and hold some value to the offender. Second, ***absence of a guardian*** who is capable and could protect the target, it can be security guards, friends, neighbours or even a lock or security cameras and the last one is ***presence of amotivated offender***who thinks that the target is vulnerable and the guardian is absent.[5]

To ascertain a criminal activity all three of these elements must come together. If any one or more of these requisite elementsare not present, the chances of occurrence of a crime is reduced.

In 2006 *Alshalan* a criminologist while applying Routine Activity theory to cybercrime argued that the netizens who more often use the internet are more likely to be targeted by a motivated offender. He further said, the people who divulge their financial and personal information more on the online space are at more risk of cyber victimisation. Therefore, it can be said that not everyone faces the same level of risk, for some the risk is more in comparison to others. But generally, cyberspace itself is a very tricky place. No one is completely safe or secured.

Choi in 2008 through his research found that people who are engaged in certain activities are at more risk of being a victim of cybercrime. These activities incudes downloading freeware programs, games, music or videos.

[4]Jordanne Morrow "Routine Activity theory" *available at* https://criminology.fandom.com/wiki/Routine_Activity_Theory

[5]"Components of Routine activity theory" *available at* http://www.crimeprevention.nsw.gov.au/Documents/routine_activity_factsheet_nov2014.pdf

Therefore, in accordance with Routine Activity Theory it can be said that in order to reduce victimization we have to educate the people who are more exposed to the internet on what precautions are to be taken so that a motivated offender cannot gain access to them.

5. **Sykes and Matza's Theory of Neutralization[6]:** This theory was proposed by Gresham Skyes and David Matza, who argued that every individual have a set of moral belief that stop them from committing an offence, so if they do something that would go against their norms, they will feel extreme guilt and shame. In order to become a delinquent, they first neutralize their guilt. This technique puts them in a temporary delusion which makes them believe that what they are doing is not wrong. Hence, these morals that stop a person from doing a wrongful act are blocked, which allow them to do criminal activities without feeing any burden of causing harm to their positive self-assessment.

Skyes and Matza gave five neutralization techniques:1. Denial of responsibility 2. Denial of injury 3. Denial of victims 4. Appeal to higher loyalties 5. Condemnation of condemners

In these techniques, the individual tries to shift the blame from himself to any person or thing or circumstance around him and believes that what he is doing is harmless or that the victim deserved this kind of behaviour or they assume that it is fine to break the norms by being loyal to someone higher to them. These can be understood by the following instances, A researcher Copes in 2003 through his research found that the people who joyride someone else's car are convinced that they are not causing any harm to anyone as afterwards they return the car to its original owner or we can look into the case of **Josef Fritzl**[7]who held his daughter in the basement for a period of over 20 years as a sex slave and had seven children with her, and none of them had seen the sunlight. When fritzel got arrested finally and asked why he did that, he **denied the injury** and said that he should have let the older child one die instead of seeking help for her due to which he got caught.

So, this is how several cybercriminals try to justify their unlawful act.

---

[6] "Neutralization theory" *available at* https://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0140.xml#:~:text=Sykes%20and%20Matza%20outlined%20five,loyalties%2C%20and%20condemnation%20of%20condemners.

[7] Bec Heim "The terrifying tale of Josef Fritzel and his bunkers of horrors" 2008

All these theories will be discussed in detail while explaining various kinds of cybercrimes such as hacking, morphing, phishing etc.

II. SOME OF THE MOST PREVALANT CYBERCRIMES ARE:

In this research paper, the main focus will be on some of the cybercrimes which need more attention than the others, such as - Child pornography and Child grooming which are having a devilish effect on life of children who are being trafficked and abused for this purpose. Hacking which is not only affecting the life of some individuals but are giving rise to terror activities and disrupting multi-billion-dollar companies by gaining unauthorized access to their data. Cyber-victimization which is one of the core causes of high depression and suicide rates in the 21st Century and digital piracy that is causing millions of job losses in the entertainment industry. These cyber crimes have been explained below:

1. Hacking: The gaining of unauthorized access to data in a system or computer.[8]
2. Child Pornography: It isany visual depiction of sexually explicit conduct involving a minor (persons less than 18 years old).[9]
3. Grooming: The action by a paedophile of preparing a child for a meeting, especially via an Internet chat room, with the intention of committing a sexual offence.[10]
4. Cyber Victimization[11]: Itrefers to the process of exploiting, terrorizing and tormenting others by the use of information and communication technologies
5. Digital Piracy[12]: Itrefers to the illegal act of duplicating, copying, or sharing a digital work without the permission of the copyright holder, a violation of copyright laws.

[8]Merriam-Webster's Collegiate **Dictionary** (10th ed.). (1999)
[9]"Child pornography" *available at*https://www.justice.gov/criminal-ceos/child-pornography#:~:text=Child%20pornography%20is%20a%20form,less%20than%2018%20years%20old).
[10]"Grooming" *available at* https://www.collinsdictionary.com/dictionary/english/grooming#:~:text=Grooming%20refers%20to%20the%20things,hair%2C%20and%20skin%20look%20nice.
[11] "Cyber victimization" *available at* https://www.frontiersin.org/articles/10.3389/fpsyg.2019.01159/full#:~:text=The%20term%20cyber%2Daggression%20is,et%20al.%2C%202018b).
[12] Jason R ingram "Digital Piracy"

III. HACKING: THE ART OF EXPLOITATION

When we think about hacking various questions pop in our head like who was the first person to ever think about stealing data and information through computers and why wasn't he stopped then and there?

The origin of the term "hacker" was in 1960s at MIT, back then no one really had any idea what a hacker was, they were viewed as geeks who sat locked in their room all day. A few of them who had some knowledge about computers use to think of them as geniuses who could push the computer systems beyond its limits[13]. But today hacking have become a cancer to the society. Various measures are being taken in order to upgrade the security level, but in one way or other they always find a way to take away crucial information by cracking into the system.

For a better understanding of what really goes on in the hacker's mind, what actually motivates him to commit such a grievance offence? We must first classify the hackers, on the basis of their behaviour and various motivation to understand them better. Various criminologists such as Landreth (1985), Chantler (1996), Post (1996), Parker (1998), Rogers (1999) and many more, tried to classify this diverse community of hackers into sub-categories.

The first attempt was made by Landreth[14] in 1985 who divided the hackers in accordance with the activities they were involved in. He divided them into five categories which were novice, student, tourist, cashier and thief. The **novice**was considered to be the least experienced one and their activities were appraised as trivial. The **students** were the pupil who were still in schools and colleges and instead of studying were exploring the computer systems. These students are usually bright and due to boredom engaged in these types of behaviour. The third sub-category are **tourists** who hacked to get some type of adventure out of it, they do such activities to get some thrill into their lives. The **cashier** was considered to be the worst of all the categories as

[13]"History of hacking" *available at*https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/#:~:text=It%20all%20began%20in%20the,FORTRAN%20and%20other%20older%20languages.&text=Then%20in%20the%20very%20early,to%20be%20used%20with%20UNIX

[14] Bill Landreth, *Out of the inner circle: A hacker's guide to computer security* 1985 (Microsoft Press,U.S. (January 1, 1793)

they were destructive and intentionally damaged the systems. The last category i.e. the **thieves** were the most professional of all and hacked to gain some kind of profit.

After Landreth many criminologists tried to understand the hackers by classifying them into various subsets. But the most prominent of them is considered to be that of M. Rogers who argued that hackers are not homogeneous groups of people and classification was essential in order to understand their behaviour. His classification is considered to be the "new taxonomy". Rogers amalgamated all the classifications made by the previous criminologists and came up with the present classification, that consisted of seven categories: Newbie/tool kit (NT), Cyber punks (CP), Internals (IT), Coders (CD), old- guard hackers (OG), Professional criminals (PC) and cyber terrorists (CT)[15]. This classification consisted of the hackers of the lowest ability such as Newbie and cyber punks to that of the highest potential i.e. the old guards and cyber terrorists. 70 percent of the hacking activitiesare done by the IT that are the internals who hack in the computer systems of their employers to attack them by taking advantage of their privilege and internal knowledge. To understand the reason for which a hacker commits such an offence some of these categories are explained below which will help us to get the wit of a hacker's mind:

The first category is that of a**Newbie**, which includes those people that are new to programming and hacking and generally consists of younger individuals who are attracted towards this aberrant behaviour by either through their friends or by watching some movies, they start believing that doing such things will make them appear "cool" and they will become more acceptable to their friends . They depend for learning these skills and planning their attack on pre-written pieces of software which is given the name tool kits. These tool-kits are very easily available by making a 2 mins search on the internet. These young people try to make their place in the hacker's community, for which it becomes necessary for them to commit a crime. As Rogers explained "The factors of low technical skills and knowledge, and eagerness to prove their worth, make for a dangerous combination". Hence, these newbies get themselves entangled into a dangerous side of the internet. The example of Newbie hacker is Mafia boy from Canada who was a 15 years old teen. He brought down the internet sites of Amazon, ebay, yahoo, Dell and many more.

[15]Marc Rogers "A new Hacker Taxonomy" Department of psychology, University of Manitoba

The second category is **Cyber punks (CP)**, these people have average programming and hacking capabilities. These individuals unlike the newbies create their own software, though these software are not very well written but they have better knowledge of the system they are going to attack. This is the category of people that we are most familiar with because they are the ones engaged in credit card number theft, sending us junk mail or spamming and other telecommunication thefts. They usually commit these crimes in order to get the attention of the media or for monetary gain. These people if caught are glorified by the media as their targets are very high-profiled people.

The third one is **Internals (IT)**, this group is usually made up of discontented employees or ex-employees and use the privilege that they have been given by their employer for performing their jobs to attack their own organization. They violate the trust that their employer has on them for malice purposes such as revenge for being either unreasonably terminated or not getting recognition for their work and try to justify their action by believing that the organization deserved this. According to the criminologist Shaw "Identified risk factors of Internals that, when combined with the proper environmental factors (e.g., stress), trigger attacks".[16] The employees of the IT profession are usually engaged in this kind of activity.

The next is **Old guards (OG),** this is the category that writes the codes that are used by the newbies. These people are extremely skilled and they are more involved in writing scripts though they do not use them they post them on the online platform in order to encourage other members of the hacker society. This group is more interested in the intellectual endeavour and their primary motivation are new challenges. They don't cross the criminal line but are just captivated by the mental exercise it requires.

The last one is **Professional Criminals (PC),** this group is considered to be the most dangerous kind of hackers. These people are the real professional criminals and are usually part of the ex-secret intelligence teams. Though they are considered to be the most dangerous of them all a very little information about them is available and they tend to never get caught. This group is motivated by monetary gains and usually work for very organized criminal groups. They are not

[16]Shaw and Lucas "Sony to Release 'the interview' in more than 300 Cinemas", 2014

interested in any form of fame or media glorification. It has been conjectured that this group has expanded since the dissolution of many intelligence agencies in the past.

Hence, why these computer geeks commit such offence can be understood by the following generalizations. The first one is that, these criminals hardly face any negative consequence for their actions as the technology is still lacking in this field, most of the hackers after doing such activities disappear without a trace and it becomes very difficult for the police to apprehend them and if they do get caught the punishment is not at all stringent or there is no punishment altogether and they can easily get away with it. The second reason for such conduct is that the people as well as the media glorifies such criminal and show their activities to be that of extremely talented people due to which many people as well as children get attracted towards such activities and lastly, it is very easy to hack into the computer systems, the automation are not very secure yet. With enough information available on the internet on this subject, it becomes effortless for people to start doing such ventures in the starting for fun and later on they become addicted to it.

IV. CHILD PORNOGRAPHY

With the progress in the telecommunication sectors, the technologies have become affordable for all the sectors of the society. Almost everyone has a mobile phone with a good internet connection and every middle-class house has a Personal computer or laptops. Due to this new platform easily accessible by almost everyone on this planet. A convenient platform has been found by the child pornographers to share the dreadful images and videos of children in unpleasant situations being sexually abused. Catching these criminals have proven to be a dreadful work as the platform is so huge and the methods that are being employed are very least incompetent in relation to today's technology. As per criminologist Freda Alder "the underground child pornography industry is growing at a very rapid rate than before due to the advent of the printing press or cameras".

People who are involved in checking this misuse have reported that in the year 2019, 45 million photos and videos have been shared of children being sexually abused which was more than

double than what they found in the year 2018[17]. According to the research conducted by Ropelato in the year 2006, the annual net profit made by people involved in this business was more than 3 billion dollars. We can only fear the worst that how much it would have increased today with so much more advancement in technology. There is clearly a linkage between increased child pornography and development in the technology in relation to the internet[18].

As claimed by Morahan-Martin and Schumacher in their work "Incidence and correlates of pathological Internet use among college students", the internet is acting as a playground by the people who are involved in deviant practices. This is because the internet provides the benefit of being anonymous and not having to meet other people. It becomes more convenient for people who think they can't be confronted due to the anonymity to engage in contentious behaviours for instance the child pornographers won't be able to do such conduct if they were in front of someone as they will have the fear of being caught.[19]

This feeling of lonesomeness and facelessness can make the person unable to control their own behaviour or think in a rational manner and such people become distant from others and stop caring what the others will think of them. Hence, clearly with the mix of anonymity and growth in intellectual property a dangerous result of increase in child abuse is resulting.

Albert Bandura in the year 1977 developed a theory named "Theory of reciprocal determination" according to which there are three factors that can affect a human conduct. These factors are: the environment, the individual and the behaviour itself. In conformity with this theory the behaviour that an individual will have will be the result of the social environment in which he is living as well as the personality of the individual. All these factors play a very important role as they complement each other and at last take effect on what the individual does. It is their personality that decides what kind of media content they are interested in.[20]

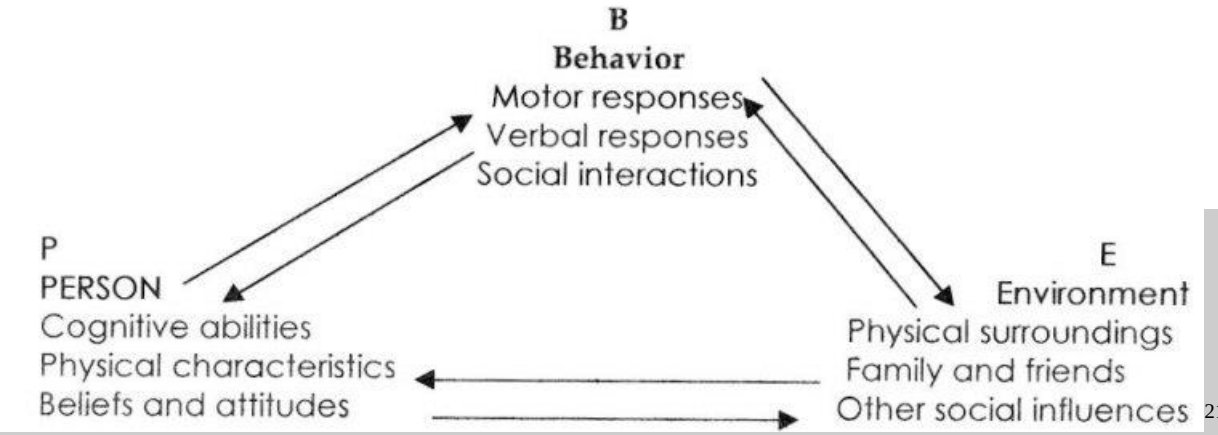
---

[17]"Statistics on child pornography *available at*https://enough.org/stats_exploitation#:~:text=Sexual%20Predation%20%26%20Exploitation%2FChild%20Pornography&text=Just%20over%20a%20decade%20later,of%20the%20total%20ever%20reported.

[18] L. Negredo "Child Pornography on the internet"(2016)

[19]Morahan-Martin and Schumacher "Incidence and correlates of pathological internet use among college students" (2000)

[20]"What is Reciprocal Determination" *available at* https://www.verywellmind.com/what-is-reciprocal-determinism-2795907



[21]

Bandura's theory was applied by Cooper, Howell, Yuille, Williams and Paulhus in their research work "Inferring Sexually Deviant Behaviourfrom Corresponding Fantasies: The Role of Personality and Pornography Consumption" to understand why some of the college students were into pornographic content while the others were not.[22] After conducting a thorough investigation, they found out that the people who had some subclinical psychopathy traits which means that the people who were impulsive, antisocial, had no remorse and did not empathize with others or experienced any form of guilt were involved in looking for porn more than the students who did not have this type of personality. Hence, they proved the Banduras theory of the different personalities effecting the outside behaviour.

The other thing that was laid down by Bandura in his reciprocal theory is that "the personality of a person is high lightened if he is under no constraint from the environment around him". The people who are involved in making and circulating such an horrific thing as child pornography is because as per Bandura they are disconnected from the outside world while using the internet due to which their deepest desire is heightened. All the efforts made by the legislatures are going

[21]Model of Reciprocal Determination *available at* https://www.integratedsociopsychology.net/theory/reciprocal-determinism/

[22]Cooper, Howell, Yuille, Williams and Paulhus "Inferring Sexually Deviant Behaviour from Corresponding Fantasies: The Role of Personality and Pornography Consumption" (2009)

vain as the internet is being accessed from different parts of the world even if they try to close one website uploading such contents hundreds of new will be created in matter of days.

Hence, why these people circulate this type of material can be understood by the above discussion which included firstly that it is the result of the environment i.e they are disconnected from the outside world and slowly the emotionally becomes distant with it too. Secondly, internet provides these people anonymity due to which they feel that they can engage in any kind of behaviour without having any to deal with it or having their image in the society be affected and lastly, personality of a person play a major role, people who are impulsive, unempathetic, antisocial are more likely to engage in this deviant behaviour than others.

V. CHILD GROOMING THROUGH CYBER SPACE

"Grooming is when someone builds a relationship, trust and emotional connection with a child or young person so they can manipulate, exploit and abuse them[23]". The intention of the predator for grooming can vary from having sexual conversation to asking them to send naked pictures and videos of themselves or having them do something of erotic nature on the web cam and the most dangerous one of all is asking them to meet in person which can lead to horrific things such as sexual abuse, trafficking etc,. The predator can be of any age, old or young or can be a male or a female.

Internet has been considered to be a very risky platform for children. Due to their young age they can be very vulnerable. The internet groomers can intentionally reach out to children by keeping a tab of the social media platforms they are available on and can sort out their target according to the locations. There are numerous social networking websites such as Instagram, facebook, snapchat etc, through which these predators can chat with them and through their tactics know the name of the parents, the school they go to, or any other places that they frequently visit. This delicate information can get them kidnapped, exploited and trafficked. But the one question that comes to everyone's mind after reading about child sexual abuse is that how and why would anyone do such things to such innocent souls?

"Before all this, I thought a predator is someone who lurks in the bushes. I didn't think I was one. But then I realized the computer monitor was my bushes."

[23]"Grooming" *available at*https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/

This quote was said by a serial child predator named Jake Mattew Clawson while explaining his online obsession.[24] According to an analysis made by the authorities of famous social networking site "Myspace" in the year 2007 that the total number of users of their website were around 180 million and out of which 29,000 were the profiles of registered sex offenders in the U.S. This information is so chilling because these were the people who made account under their names, there will be millions of other offenders who might have made their profile under a fake name. After almost 14 years and development of the new chatting rooms such Instagram and many other,the dangers of grooming have increased more than tenfold times.

Many researches and studies have been done by criminologists and psychologists from all around the world to understand the behaviour of paedophilia. According to a report by Bogaert in the year 2001, he conducted a survey on male college students to know what kind of pornographic material they enjoyed. When they were given the opportunity, half refused to watch porn of any kind, 4% chose aggressive pornography and 3% chose child pornography.

O'Connell in the year 2003 conducted a sting operation in order to find out the methodology used by them for grooming the vulnerable children on the internet. She posed as a girl aged between 8-12 years and depicted herself having family issues and no friends on number of social medias and chat rooms, this style of communication played an important role in the process of grooming.

When the question about child predators was asked from Maya Nicholas, a former parole officer who had worked with the sex offenders as to what she have learnt from her experience? Why do they do such things to children?[25]

Maya was still in her internship when she was given an opportunity address meeting in which all sex offenders were to go for their therapy and for complete one year, she watched them ask each other questions like what attracted them towards children? She answered that the behaviour of the sexual predators is usually similar to those who were addicted to an addictive substance such as drugs. Most of them did not realise their mistake even when arrested and see nothing wrong

[24] Christine D. Marcum "Book Review of Sexual Predators: How to Recognize Them on the Internet and on the Street - How to Keep Your Kids Away"pg 252

[25] "Views and Experiences with sexual offenders*" available at* https://journals.sagepub.com/doi/10.1177/0306624X11432301

with their behaviour. When asked why? The most common answer was that they liked the feel of it and that they felt sexually stimulated only by children and not by women or any other person.

They said that there are chances of being rejected by women but children can easily be manipulated through presents and even by showing support and acting like you understand what they are going through. It is easier to build trust within children and make them do whatever they wanted. The children could not just shut them out. While some other claimed that it was due to loneliness that they were triggered.

As per a study conducted by M.L. Scott the main cause of paedophilia can very well be ascribed to the biological as well the environmental factors of that individual. According to him the dominant factor in paedophilia is cerebral dysfunction in an individual. Whereas, as per DiChristina the preferences of sexual nature are a result if sone childhood trauma or experience that the child underwent.[26]

There is also a study thar says, paedophiles are usually those people who have been themselves abused when they were of a young age. When they were young, they could not control what was happening to them. So, when they become adult, they want to be the master and assault young children like they themselves were molested. They want to now have the upper hand over someone who either look like them or is of the same age when they were assaulted.

Hence, it is now somewhat clear now that why do these people hurt such innocent children the main reason that we have understood is they themselves have been molested by someone else at a very young age which lead to a traumatic experience and has ingrained in the nervous system of these paedophiles which is why they attempt to relive the situation but now be dominant and not helpless. The other thing we learned was to paedophiles sexual activity with children was like drugs. They have same brain structure as those who have an addiction to a substance and hence, they can't see anything wrong in their behaviour.

VI. CYBER VICTIMIZTION

With the advancement in the information technology platform many types of new form of business have developed that were not in existence before, one such thing is being able to

[26]Minte L. Scott "Neuropsychological Performance of Sexual Assaulters and Pedophiles" (1984)

communicate with other people by sitting in any corner of the world. The development in telecommunications have become so advanced that one can communicate with others without even reviling who they really are. So, many of the haters or bullies have taken advantage of this and started the victimization of others and majorly of young adults through this medium. This have led to a tremendous increase in the cases of depression, anxiety, low self-esteem and suicides among adolescents as well as adults and is a major health concern.

Cyber victimization is that process in which the users use the information and communication technology in order to exploit, torment or terrorize others. Cyber victimization can include cyber bullying, cyber harassment, hacking or malware infection.There have been several different studies in this regard. According to the report by Sandra Brochado, Sara Soares and Silivia Fraga in their paper "A Scoping Review on Studies of Cyberbullying Prevalence Among Adolescents"[27] has mentioned that almost 4.9 and 65% of young adults have experienced cyber victimization through internet.

Have you ever thought why due to discovery of online platform the aggression of people has increased two-fold than it used to be before? Why have the victimization surged?

This can be explained by "Online Disinhibition effect" given by Suler which provides that people are more likely to behave differently while on web than they do face to face because internet helps them feel freer and they tend to communicate more blatantly than when the person is right in front of them. A term digital schizophrenia has been coined in order to explain the dual personality of people, some people who are shy in person can have a completely opposite personality while using such devices. The reason behind it can be the benefit of anonymity.[28]

Now this might have some positive effect such as people being able to express their opinion more openly but at the same time the negative impact far exceeds the positive one. For instance, if a child is using this and start telling everything about themselves to a stranger, they are talking to on the social media can lead to trafficking, kidnapping etc

[27]Sandra Brochado, Sara Soares and Silivia Fraga "A Scoping Review on Studies of Cyberbullying Prevalence Among Adolescents" (2016)
[28]Suler, J. (2005) The Online Disinhibition Effect. Int J. Appl. Psychoanal. Stud., 2(2): 184-188

It was suggested by criminologists Roncek and Mater that various kinds of cyber victimization can be best explained by the "Routine activity theory". This theory states that in order for a crime to occur three components must be present. (a) a suitable target (b) there must not be any guardian around (c) there must be a motivated offender.

An ***accessible target*** can be any person, thing or place which is easily available and hold some value to the offender. Second, ***absence of a guardian*** who is capable and could protect the target, it can be security guards, friends, neighbours or even a lock or security cameras and the last one is ***presence of amotivated offender*** who thinks that the target is vulnerable and the guardian is absent

In 2006 *Alshalan* a criminologist while applying Routine Activity theory to cybercrime argued that the netizens who more often use the internet are more likely to be targeted by a motivated offender. He further said, the people who divulge their financial and personal information more on the online space are at more risk of cyber victimisation.[29]Therefore, it can be said that not everyone faces the same level of risk, for some the risk is more in comparison to others. But generally, cyberspace itself is a very tricky place. No one is completely safe or secured.

For instance, if a girl posts a picture on Instagram and does not keep her profile private, she is tending to be exposed to more bullying than the people who just add their known and keep the privacy of their profile on.

Hence, we now understand that even a small mistake such as giving an information to a stranger which might not mean anything to you can be used against you. Cyber aggressors might be a polite social butterfly but while operating the web their personality can change completely and all the hatred that they have kept hidden deep down in their hearts are vented out on such platforms which may cause hatred filled comments, messages etc and can have a destructive impact on the mental health of the victim ergo victimization.

VII. DIGITAL PIRACY

BabumoshaiBandookbaaz, Udta Punjab, Paa, Manjhi, Tera kyahoga johnny, we all have heard about these Bollywood movies, but what do all these movies have in common? All these movies

[29] Abdullah Alshalan, Cyber-crime Fear and victimization 109 (Mississippi State University, 2006)

were leaked on the internet before their official release on the cinema. We can't even imagine the work and effort that goes into the making of these films and all their efforts goes in vain due the infringement of their copyrights.

Piracy is one of the most prevalent form of copyright infringement in India. Cyber Piracy has been defined as "various deceptive practices that the companies or individuals engage in to profit from the online users"[30]. It come about when an individual copies information from the legit sources and distributes or sells that material online, unaccompanied by the assent of the indigenous developer of the creation. This illegal sharing can of games, movies, software, etc.

There are primarily 5 types of online piracy:

1. **Counterfeiting:** To counterfeit means to copy something that is real or original, with the ill will to sell or distribute it for their own profit.

2. **Internet Piracy:** It means to download an authentic material from somewhere and then illegally uploading it on different webpage without the permission of the creator.

3. **End-User Piracy:** It is when an individual uses an unlicensed copy of software for its own operation without authorization.

4. **Client-Server Overuse:** Client-server overuse refers to the form of piracy where a central program is being used by too many people at the same time, without any license.

5. **Hard-Disk Loading:** Usually in order to boost up their sales or to make the purchase more attractive, some users illegally load copyrighted software on the hard disk of a new computer, this is known as Hard disk loading.[31]

Piracy has a negative effect on the life of every single person involved in these industries. Due to the illegal downloading of software, movies, songs, games etc, these industries are not making profits as much as they should because of which less money is being invested into new projects. Hence, there is less wok for the people who play a major role in these industries such as developers, directors, musicians, security guards, sale people and many more. Most of these people have lost their livelihood and are suffering.

According to the statistics - 126.7 billion of loss is endured by the television shows produced in the united states every year. Almost 70,000 of the people working in the music industry lose their

[30] Digital piracy *available at* "https://sites.google.com/site/cybercrimewiki/4-program-study-outline/7-piracy"
[31] "Types of piracy" *available at* https://www.nortonlifelock.com/us/en/legal/anti-piracy/types-piracy/

jobs each year. Annually, movie industry globally suffers a loss due to pirated content of $40 billion to 97.1 billion[32]. The question here is if piracy is illegal why so many people are still engaging in this atrocity?

If we try to find the answer to this question, we can explain it with the help of Differential theory given by Sutherland and Cressy in the year 1960, this theory is known to be the first of all the social learning theory. This theory explains that a criminal behaviour is learnt, and that if a person is exposed to an environment which is not in compliance of law for a very long time. They will start learning it. As per, differential theory it is the most intimate group of our life which has the most effect on us such friends, family members or even the movies or series that we love to watch. And hence what they do feel normal to us it is not of importance if it abides by law or not.[33] Some aspect of piracy has been found to be associated with differential association theory and has been confirmed by the test done by Skinner and Fream which was the first test conducted in this regard. Higgins and his colleagues have also through their studies supported the differential association theory.[34]

Another theory of criminology which can help us understand this behaviour is deterrence theory given by Cesare Beccaria and Jeremy Bentham. They speculated that how effective a law is would depend on how the punishments are supervised.[35]

If the punishment of doing an offence outweighs the reward a person will not commit an offence as a criminal would choose to either follow or break the law after scrutinizing the risk and reward of their actions. For instance, Ram and some of his friends were coming back from school when someone suggested breaking the window of the principle's car. Ram thought 'that if he gets caught, he will get in a lot of trouble'. As Ram did not want to get into any hassle, he decided not to break the window and went home. This is how deterrence plays an important role in making people obey the law.

---

[32]Statistics on Digital piracy *available at* https://www.ibc.org/trends/digital-piracy-costs-us-economy-30bn-annually/4037.article

[33] "Sutherland's Differential Association theory" *available at* https://www.thoughtco.com/differential-association-theory-4689191

[34] Whitney Decamp "Piracy on the high speeds: A test of social learning theory on digital Piracy among college students" (2008)

[35] Patrick M. Morgan "The concept of deterrence and deterrence theory" 2017

In case of digital piracy, as well there maybe advancement in technology but the measures to control it is still not sufficient. Hardly one 1% of the people who are engaged in this type of behaviour are caught and the reward if we see is lot more. They get to download shows and movies for which they might have to pay hundreds of dollars for free.

Hence, from the above discussion it is clear why people are taking part in such activity. The main reason is that there is a lot of gap between the technological advancement and the legislative remedies for this. People are getting more than what theymay not lose. Further it is the people around us who are helping us learn this kind of behaviour and if we ask them about it the most common answer, we will get is that they were not even aware that it was a criminal act as everyone does it. Therefore, the awareness is also less and needs to be improved in order to stop this deviant behaviour.

CONCLUSION

"Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weaknesses. An accurate vision of digital and behavioural gaps is crucial for a consistent cyber-resilience." — Stephane Nappo

Cybercrime is one of the most considerable menace now than it was ever in the history of humans. If a cyber-criminal is able to pull off even one successful attack, it can have an extensive imputation on other's life. It can lead to huge financial losses as well as the trust of the consumer in their organisation is also affected. The estimated loss to an industry due to these cybercrimes is of billions of dollars annually. This nefarious crime does not have only monetary effects but cybercrimes such as Cyberbullying, cybervictimization, cyber stalking. Victims of these crimes often fall into depression and experience extreme sadness, loneliness, and feel low self-esteem, they may feel they are not loved. All these can lead to suicidal thoughts and behaviour.

There is a very strong need to fight against all these cybercrimes and criminals and this can only be done through new and more effective laws by the legislators. Instead of focusing and investing in making the technology better, they should now invest in successful implementation of these laws in order to cover the gap between the technological advancement and its control as most of the deviant behaviours in the above cases were because the award was bigger than the punishments. Therefore, in order to curb this evil this needs to be reversed i.e. the punishment should be increased so that the people think many times before causing these breaches and hurting others. People must also try to take all the precautions that they can such as keeping the computers updated so that you block the accessors from accessing the old vulnerable software. The passwords selected must be solid and unpredictable with certain symbols such as @, $, # etc. so that they become hard to guess. Taking such safeguards can ensure safety of yourself as well as your loved ones.