Page 231 - 250 **DOI:** *https://doij.org/10.10000/IJLMH.113572*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 5

2022

Technology Crime and Organized Syndicates in Cybercrime: Critical Analysis

HEENA GOYAL[1]

ABSTRACT

Cybercrime is one of the most dangerous crimes in the world. It is one of the most serious offences these days. Cyber is a new technology and within two minutes we will see one recent case related to fraud, extortion, hacking, phishing, and etcetera. This crime is committed by organised syndicates and the mafia. They are making this threat in this world and also doing online black-marketing through the dark web and earning black money from these illegal activities that are creating fear in society day by day. It is out of control. Every day we see another type of cybercrime being done by hackers for illegal money. Even cryptocurrency, Doge coins, and bitcoins are not safe from this crime. The cyber invaders are nowadays expanding their more sophisticated gears to cause destruction and, therefore, the effects are also severe Syndicates are earning digital money. This paper is going to talk about cybercrime and how its deals with organised crime cybercrime are not limited to computers; they also include smartphones. How the mafias have ruled over cybercrime over the last two decades, it is one of the fastest-growing criminal activities against individuals and businesses. Syndicates are doing illegal work day by day and affecting society at any cost. In this paper, the researcher is going to narrow down the concept of cybercrime to contemporary issues related to the present scenario.

Keywords: *Cybercrime, dark web, Mafias, Organized crimes, syndicates.*

I. INTRODUCTION

The internet is growing rapidly in the world. It has given rise to new opportunities in every field we can think of, be it in entertainment, business, gaming, social media, education, etc. But, the Internet has two sides to the coin: one is an advantage, and the other one is a disadvantage, i.e., cybercrime. Cybercrime has a very wide scope in nature, which we all know as computers and the internet, computer-related crime, and internet-related crime. In the new era of Hi-Fi technology, crimes are different and are defined differently. The Internet has brought unfamiliar words into a society like "crime", "net", "electronic", "virtual", "digital currency", etc. There are so many changes in technology that there is no proper definition of cybercrime in the national and international scenario. Everyone has their own definition of cybercrime. This

[1] Author is a LLM Student, India.

 [ISSN 2581-5369]

means cybercrime is an attack on digital currency, hacking of computers, and illegal activities through the internet by syndicates and individuals. Cybercrime has a severe potential impact on individuals and groups.

According To the State security agency of South Africa has defined cybercrime 'means illegal acts, the commission of which involves the use of information and communication technologies.[2]

According to Bert-Jalap Koop's, the Internet provides special opportunities to commit cybercrimes: crimes in which computer networks are the target or a substantial tool.[3]

According to Malcolm Tatum, 'Cybercrimes are generally defined as any type of illegal activity that makes use of the Internet, a private or public network, or an in-house computer system.[4]

The 21st century has recorded different types of cybercrime every day. People from different parts of the world are becoming victims of computer and smartphone crimes, and it is affecting their lives. Earlier, we discussed that there is no proper definition of cybercrime. However, cybercrime has two prefixes: "cyber" and "crime." Cyber" refers to computers, technology, and the internet; "crime" refers to illegal activities that are punishable by law.

Traditional cyber-crime and non-traditional cyber-crime are two types of cyber-crime. i.e., modern cybercrime.

After all, the act of cybercrime is a crime that, after all, the act of cybercrime is a "traditional" crime (e.g., potential) where computers are commonly used for network communication or are a source of information to support criminal organizations. Search for information about victims and how to harm, scam, or embarrass them (Paediatrics Love Group). Removing the Internet reverts to other forms of communication that criminals can easily use, so criminal activity persists. The other is Modern cybercrime is a crime in which it's no secret that organised criminal groups are making millions each year through highly orchestrated, coordinated attacks on businesses of all kinds.

Organized syndicates already make more money from cybercrime than they do from the illegal drug trade, trafficking, etc., and it is on track to surpass all of its other criminal operations

*Student, LL.M IVth semester, Sardar Patel University of police, security and criminal Justice, Jodhpur.

[2] David Mahlobo & Mr David, *THE NATIONAL CYBERSECURITY POLICY FRAMEWORK (NCPF)* (2015), www.gpwonline.co.za (last visited Aug 17, 2021).

[3] Elias Chachak , Cybercrime is moving towards smartphones – this is what you could do to protect your company | CyberDB, , https://www.cyberdb.co/cybercrime-is-moving-towards-smartphones-this-is-what-you-could-do-to-protect-your-company/ (last visited Aug 17, 2021).

[4] Malcolm Tatum , What is Cybercrime? (with pictures), , https://www.easytechjunkie.com/what-is-cybercrime.htm (last visited Aug 17, 2021).

 [ISSN 2581-5369]

combined within a few years.

When you combine it with the global shortage of skilled security personnel, you have a recipe for a stormy future. There are different types of cybercrime in e of skilled security personnel; you have a recipe for a stormy future. There are different types of cybercrime in society today.

Cyber-crime has different types of crime are:-

1. Hacking
2. Child pornography
3. Dark Web
4. Phishing
5. Related To Intellectual Property Rights
6. Online Harassment/Bullying
7. Cyber-extortion (demanding money to prevent a threatened attack).
8. Crypto-jacking (where hackers mine cryptocurrency using resources they do not own).
9. Cyberespionage (where hackers access government or company data)
10. Malware

These are some examples of cybercrime. People or small groups with limited technological skills can commit cybercrime. Or those with knowledge connected to experienced developers by organised criminal organisations worldwide. To avoid discovery and prosecution, cybercriminals typically operate in nations with weak or non-existent cybercrime legislation. High-end cybercrime groups employ the newest business methods to upgrade their software products with the latest security features and recruit fresh software engineering experts to their companies. Using the Internet, cyber criminals may be trained in an enormous network of remotely controlled "zombie" computers to swarm and attack, infect other computers, send unwanted junk mail distribute or refuse lawful consumer Internet access and services. Cybercrime as a culprit is challenging, as the new technology exceeds police enforcement skills. This new danger to national security can change the discussion as malware improves and the repercussions of criminality increase. As malware changes and cybercrime gets worse, this new threat to national security could make talking about cyberterrorism a matter of national security.

(A) Statement of Problem

Cybercrime is a new technology of illegal crime in this world. Cybercrime has been around since the 19th century, but in the last 3 decades, cybercrime has rapidly increased in nature. Syndicates are hiring professionals to develop technology for cybercrime. Hackers are misusing the internet for their personal gain and threatening individuals, groups, and government

officials. The involvement of syndicates is high in cyber-crime activities. They manage many illegal activities on the internet by using the dark web. The dark web is also a new type of criminal activity, and people are not aware of the dark web and are becoming victims of it. By using the dark web and deep web, they are committing crypto-jacking, cycybercrimeon, cyber espionage, and other illegal activities. There are major issues related to cyber-crime. The first one is the rapid increase of illegal activities by professionals and mafias. Second, people cannot understand this issue because of a lack of awareness about cybercrime and a lack of awareness about various laws regarding this and how they have to file a complaint with the autcybercrimehe authorities are not aware of the cyber-crime activities. In India, there are no proper guidelines related to cybercrime and no proper branches are there in India. These problems are like when victims don't know where to register a complaint and deal with it. Hence, this paper will cover the main reasons behind the illegal activities, the dealing of the syndicates in cyber-crime and the legislative framework and will also suggest some effective suggestions for effective laws and improved in-laws.

(B) Research aim:-

- To learn about cybercrime activities.
- To know about the newest rackets of the mafia.
- To learn about the laws related to cybercrime
- To find out the reason behind the rapidly increasing illegal trading in cyber.
- To suggest methods to reduce and be aware of cybercrime in society.

(C) Research question:-

What is cybercrime and how have illegal activities affected society?

1. What do you mean by Pegasus is infringing the privacy of bureaucrats, journalists, and other individuals and companies?
2. Whether cyber-criminal activities impact digital currency or not,
3. How is cyber-crime becoming the mafia's newest racket?
4. What are the laws and statutes that can prevent cyber-crime and syndicates?

II. ILLEGAL ACTIVITIES OF CYBERCRIME

Cybercrime is a new technology of illegal crime in this world. Cybercrime has been around since the 19th century, but in the last 3 decades, cyber-crime has rapidly increased in nature. Syndicates are hiring professionals to develop technology for cybercrime. Hackers are misusing the internet for their personal gains and threatening individuals, groups, and government

 [ISSN 2581-5369]

officials. The involvement of syndicates is high in cyber-crime activities. They manage many illegal activities on the internet by using the dark web. They may either buy the malware or let it develop its definition tools and routines. Using the Crime ware server, thieves may launch an organised attack on a user's computer if their data has been taken.

(A) Evolution of Cyber-Crime

Cybercrime is evolved from Morris Worm to ransom ware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation.

Table No. 1 Evolution of cyber-crime[5]

YEARS	TYPES OF ATTACK
1997	Cybercrimes and viruses initiated, that includes Morris Code worm and other.
2004	Malicious code, Trojan, Advanced worm etc.
2007	Identifying thieves, Phishing, etc.
2010	DNS Attack, Rise of Botnets, SQL attacks, etc.
2013	Social Engineering, DOS Attack, Botnets, Malicious Emails, Ransom ware attack, etc.
Present	Banking Malware, Key logger, Bit coin wallet, Phone hijacking, Android hack, Cyber warfare etc.

[5] Animesh Sarmah, Roshmi Sarmah & Amlan Jyoti Baruah, *A brief study on Cyber Crime and Cyber Law's of India*, INT. RES. J. ENG. TECHNOL. (2017), www.irjet.net (last visited Aug 20, 2021).

(B) Classification of Cyber-crimes

There are different types of cybercrime offences that are committed by the syndicates are:-

1. **Hacking**, in simple terms, means an illegal intrusion into a computer system and/or network. The data on computers is stolen by some hackers and professional hackers. Later on, they use the information stolen from the computer against you for threats, fraud, etc.
2. **Child Pornography –** The internet is extensively used for the sexual abuse of children. There are some illegal websites on which sophisticated people buy or sell child pornography. This is one of the most common and earnest businesses for professionals.

   > Child pornography is defined for the purposes of this work, and under the federal statute, as a "visual depiction of a minor engaged in sexually explicit conduct. These visual depictions take the form of photographs, videotapes, films, and magazines depicting children in both heterosexual and homosexual activities. The children depicted range in age from a few months to 18 years. While those who molest children may be very selective in the age, sex, and race of their victims, the exploitation of children transcends any economic, social, ethnic, or religious lines.[6]
   >
   > According to "the Senate and House of Representatives of the Philippine, Anti-Child pornography Act,2009 defines the term child pornography under the section 3(b) "Child pornography" refers to any representation, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities"[7]

3. **Dark Net-** The encrypted Dark Web is where syndicates operate criminal activities.

   > Dark web websites has unusual names. Users must know the URL beforehand.
   > Dark web search engines aren't as popular as Google.
   > Dark web URLs end in.onion, a special-use domain suffix. Dark websites feature mixed-case URLs that are hard to find or remember.
   > Silk Road's URLs were silkroad6ownowfk.onion and silkroad7rn2puhj.onion.[8]

[6] Howard A Davidson & Gregory A Loken, *ChUd Pornography and Prostitutuon Back.ground and legal Ana!ysis* (1987).
[7] REPUBLIC ACT NO. 9775 AN ACT DEFINING THE CRIME OF CHILD PORNOGRAPHY, PRESCRIBING PENALTIES THEREFOR AND FOR OTHER PURPOSES, .
[8] Katie Terrell Hanna, What is the dark web (darknet)?, , https://whatis.techtarget.com/definition/dark-web (last visited Aug 19, 2021).

 [ISSN 2581-5369]

4. **Phishing-** In 1996, hackers stole America Online passwords and accounts, coining the term "phishing." Internet scammers used e-mail lures to "fish" for passwords and financial data from the "sea" of Internet users. Hackers steal personal data and login passwords. Hackers buy data from syndicates and unofficial websites.
5. **Cyber-crime related to Intellectual property Right (IPR) -**Cyber theft of intellectual property involves distributing licenced, paid, or copyrighted software for free or at low costs online.

   Piracy is one of India's biggest IP cybercrimes. Pirated movies, software, etc. are available now. Piracy hurts the copyright holder financially. Cyber criminals are hard to discover and prosecute since they do everything online, erasing data and disappearing in a fraction of a second.

   The country is cracking down on this crime. Telangana IPCU is one of the first units to deal with IP crime.[9]
6. **Cyber Stalking/Bullying (Harassment) -** In horror movies and online, stalkers lurk. As creepy as offline. Cyber stalkers torment their victims online. That's not a troll encounter. It's usually a long, persistent process aimed towards one person or group.

   Online stalkers use social media, IM, and other online tools to harass victims. By posting personal information online, we help them. Cyber stalking's motivations vary widely. Cyber stalking can be a kind of enjoyment or a hate crime.
7. **Cyber-extortion-** Cyber-extortion, involves attacking or threatening an enterprise. It also demands money to cease or remediate the attack.

   Cyber extortion occurs when hackers obtain customer data and trade secrets. They "hostage" this information for money. If you don't comply, hackers will tell everyone.

   Ransom ware is newer cyber extortion. Hackers lock you out of your computers or websites by downloading malware. Your firm must pay to remove malware and restore access.[10].
8. **Crypto-Jacking-** Unauthorized crypto currency mining is crypto jacking. Hackers do this by sending you a malicious email link that loads crypto mining code on your computer or by infecting a website or online ad with JavaScript code that auto executes in your browser. The coin mining code runs either way. Installing malicious software on PCs, laptops, and mobile devices to mine cryptographic keys is called crypto jacking.

[9] Cyber Theft Of Intellectual Property - Intellectual Property - India, , https://www.mondaq.com/india/trademark/682548/cyber-theft-of-intellectual-property (last visited Aug 19, 2021).

[10] What is Cyber Extortion & How to protect you? | CoverWallet, , https://www.coverwallet.com/general/cyber-extortion (last visited Aug 20, 2021).

 [ISSN 2581-5369]

With a few lines of code, a hacker can control all computer resources. This causes computers to respond slowly, use more CPU, overheat, and cost more to run.

9. **Cyber espionages: -** Cyber espionage is breaking into computer systems and networks to steal government or corporate secrets. As with other forms of espionage, the purpose is to better understand competitor governments' capabilities and intentions or, in industrial espionage, to get access to private corporate information to comprehend a rival company's business strategy or steal its intellectual property.[11]
10. **Malware: -** Viruses do something. Malware is a broad term for all dangerous software. Ferns are malicious programs that implant their code into others.

    Most cybercrimes target all Internet users. Sometimes hackers use remote control software, although they mainly use hacked zombie PCs. Daily internet attacks target thousands of infected PCs. Online piracy occurs in several jurisdictions and cultures. Criminals design passable websites for web crawlers, but innocent visitors are lead to an infected site. Each visitor receives a unique encrypted version of the site-infecting code. This beats antiviral software. Malware spreads undetected. Criminals don't stop. Cybercrime transitional.

    Organized crime targets cybercriminals. Cybercrime is less personal, organised, and geographical. Some research claims organised crime hierarchies are changeable and online crime focuses on horizontal links and networks.

III. SYNDICATES AND THEIR INVOLVEMENT IN CYBERCRIME

"Today's mafia" has evolved from cybercriminals, and authorities can't establish permanent groupings of serial offenders. Due to the low risk of discovery and identification, hackers are motivated to expand crimes. Cybercriminals employ new technologies to drive their cyber-attacks. Future cybercrime may help scrupulous groups. If vital infrastructure's control systems have flaws, thieves could extort money or help terrorists.

Cybercriminals build coalitions to trade counterfeit or pirated goods. Future cybercriminal organisations may have no central geographic base, function only through network technology, and make law enforcement authorities less competitive.

Transnational criminal syndicates and networks, such as the Russian and Balkan mafias, the Asian Triads, the Latin drug cartels, and West African syndicates, undermine the stability and security of all nations through illicit enterprises, including the transhipment of drugs, arms, illegal contraband, trafficked women and children, laundered money, financial fraud,

[11] Nadav Morag, *CYBERCRIME, CYBERESPIONAGE, AND CYBERSABOTAGE: UNDERSTANDING EMERGING THREATS* (2014), www.cnbc.com/id/101605470# (last visited Aug 20, 2021).

counterfeiting, and cybercrime. Organized crime often supplies illegal goods and services. A criminal syndicate or network may focus on one crime, but they commonly do others...[12]

(A) Notorious Groups

Technology has made many people's life easier, but it also has drawbacks. Only a thorough cybercrime investigation can minimise hacker harm. Hackers say a disguised crusader society must maintain market balance. Without cyber security, it's just another fish.

There are 5 most notorious groups in cyber-crime are:-

1. **Anonymous** – Anonymous connects activists to "activists" in a non-threatening fashion. The group's website characterises it as "an online gathering with a very loose command structure" that "operates on ideas rather than directives." Publicity stunts and DDoS attacks made the group famous. Anonymous is active.

   We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.[13]
2. **Global Hell-** Patrick Gregory founded Global Hell. The group was suspected of damaging 115 websites and costing millions. Gregory used the computer to escape the mob. His hacking crew acted like a crime syndicate. "Earth Village Hell shall not vanish," the organisation said on its website.Gregory admitted stealing $2.5 million.
3. **Lizard Squad**- Lizard Squad, infamous for DDoS attacks, took down Facebook and Malaysia Airlines. Lizard Squad recently disrupted social media platforms. Your business offers online customer support. Gather your army.
4. **The Level Seven Crew-** When this hacker team infiltrated the famous 1960s computer system; they travelled to Dante's 7th degree of Hell, "violence" (the NASA First American National Bank Sheraton Hotel). China Embassy website. By 2000, it was decommissioned.
5. **Lulzsec**-Lulzsec is a contraction of "lulz" for laughs and "security," which hacker's compromise. Attack motive? Fox.com dubbed "Common" a "vile" rapper on-air**.**[14]

(B) Cybercrime Hotspots

Complex destructive software, or malware, reaches hackers in Nigeria and Brazil. As the internet spreads, more potential criminals can be assaulted. To make crafts, you must master the internet.

---

[12] International Organized Crime, , https://2009-2017.state.gov/j/inl/c/crime/c44636.htm (last visited Aug 20, 2021).

[13] We are Anonymous. We do not forgive. We do not forget | Dazed, , https://www.dazeddigital.com/artsandculture/article/16308/1/we-are-anonymous-we-do-not-forgive-we-do-not-forget (last visited Aug 20, 2021).

[14] LulzSec: what they did, who they were and how they were caught | LulzSec | The Guardian, , https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail (last visited Aug 20, 2021).

- **Russia-** Sherry said Russian crime syndicates use modern technology. "Russians have excellent cyber skills and hacking capability," he argues. Before the new discovery of stolen online documents, the US accused Evgeniy Bogachev of infecting hundreds of thousands of machines worldwide. Target's 2015 data hack was likewise traced to Eastern Europe.[15]
- **China-** China is another centre for hackers, but the Chinese government has been tied to economic and political espionage against the U.S...[16]
- **Nigeria-** International cybercriminals use Rotech's hometown to send phoney emails.

Nigeria's cybercrimes act makes financial institutions responsible for combating online crime.[17]

Financial institutions, corporations, state agencies, and individuals are increasingly vulnerable to cyber-attacks and fraud, according to Deloitte Nigeria. Disinformation, impersonation, and phishing are used to conduct cyber-attacks on computers, mobile devices, and the intranet.[18]

In addition, cybercriminal regime is using local hackers to spy on journalists as well as dissidents and activists in the country.

IV. INFRINGEMENT OF PRIVACY

Cybercrime lacks privacy. Hackers target privacy. They hack company systems and data to sell on the dark web. Government hackers are pros. If they don't get money or something else, they'll reveal bureaucrats', journalists', politicians', etc. conversations. Mafia and hackers used mesh technology to construct lateral networks. Tiger text and Snapchat automatically delete evidence, and password currency (Bit coin, Rob coin, Doge coin, Lit coin, etc.) establishes a contested value exchange system. Including banking. These three technologies challenge (extra) security and cross-jurisdictional governance.

India has no cybercrime definition. The IT Act of 2000 and its 2008 modification do not cover all cybercrimes. As if it was a criminal rights issue India's cybercrime is unimportant to the probe. One illustration of how India's outmoded practices lag behind the country's development. Criminal and tort laws recognise culpability and have procedural and conciliatory aspects.

The Information Technology (IT) Act of 2000 and the 2013 Criminal Code Amendment Act manage the online world, which is a new platform. Legal reform is criminalised.

[15] Here Are the World's Five Cybercrime Hotspots | Time, , https://time.com/3087768/the-worlds-5-cybercrime-hotspots/ (last visited Aug 20, 2021).
[16] Ibid
[17] Cybercrime in Nigeria demands public-private action - ISS Africa, , https://issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action (last visited Aug 20, 2021).
[18] Ibid

 [ISSN 2581-5369]

Section 66E of the Information Technology Act of 2000 states that capturing, publishing, or transmitting a private area without permission is a three-year felony. You can also impose an Rs 20,000 fine. These situations endanger privacy. "Privacy breach" means a person expects to be naked for private protection, which is embarrassing. (ii) A portion of his private area may not be seen to the public.

(A) Case study on Pegasus

Recently, Israeli NSO Group's Pegasus spyware emerged. Pegasus is a dangerous spyware along with names and software. Pegasus is the world's most advanced cyber intelligence system, allowing organisations to anonymously acquire information from people's mobile phones (primarily VIPs). Pegasus hacks a cell phone. It can be installed through programme vulnerabilities or a malicious link. Once installed, it can send any device data to an attacker. Pegasus attacked politicians, authorities, executives, and media. Amnesty International emphasised that despite mobile platform security updates (Android and IOS), users must not click on fraudulent emails or SMS.

(B) Case study on Dark Market

The black market is a syndicate and mafia weapon. They commit crimes on the dark web. Dark web is a security threat. Dark Web syndicates do Hawala. India's Prevention of Money Laundering Act, 2002, prohibits money laundering. Section 3 of this Act and Schedule A, Part 22 discuss money laundering (Offences under the Information Technology Act, 2000).

(C) Case Study on Jamtara

Jamtara, India, is a phishing hotspot. Jharkhand's Jamtara district. Jamtara is India's cybercrime hub. The 18-24-year-old was phishing. They target seniors and illiterates. They claim to be bank officers to steal credit card and debit card information. Cyber cops caught the phishing group.

(D) Laws and Policies:-

There are different acts which talks about the dark market. In those Acts the provision are given:-

Act	**Section**	**Punishment**
Indian Penal code[19]	• Sending threatening	• A term may extend to two

[19] India Code: Indian Penal Code, 1860, , https://www.indiacode.nic.in/handle/123456789/2263?locale=en (last visited Aug 21, 2021).

	messages by e-mail (Sec .506 IPC) • Word, gesture or act intended to insult the modesty of a woman (Sec.509 IPC) • Sending defamatory messages by e-mail (Sec .499 & 500 IPC) • Bogus websites , Cyber Frauds (Sec .420 IPC) • E-mail Spoofing (Sec .463 IPC)	years, or with fine, or with both. • Punished with simple imprisonment for a term which may extend to three years, and also with fine. • Punished with a simple imprisonment for a term which may extend to two years, or with fine, or with both. • Punished with imprisonment which may extend to 7years & fine also? • Punished with imprisonment this may extend to 7years & fine also.

	• Making a false document (Sec.464 IPC) • Forgery for purpose of cheating (Sec.468 IPC) • Forgery for purpose of harming reputation (Sec.469 IPC) • Web-Jacking (Sec .383 IPC) • E-mail Abuse (Sec .500 IPC) • Criminal intimidation by an anonymous communication (Sec.507 IPC)	• Punished with imprisonment this may extend to 7years & fine also. • Punished with 3 years' imprisonment or fine or both. • Punished with 2 years' imprisonment or fine or both. • Punished which may extend up to two year'. Also refer Section 506 of this Act. • Punished, on first conviction with im-prisonment of either description for a term which may extend to two years, and with fine which may extend to two

 [ISSN 2581-5369]

	• Obscenity (Sec. 292 IPC)	thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees. • Punished with fine & 2,000 Rupees. • Punished with imprisonment which may extend up to 3 months, fine or both. • Punished with imprisonment which may extend up to 3 years, fine or both.

	• Sale, etc., of obscene objects to young person (Sec .293 IPC) • Obscene acts and songs (Sec.294 IPC) • Theft of Computer Hardware (Sec. 379)	
Copy Right Act, 1957[20]	• Offence of infringement of copyright or other rights conferred by this Act(Sec. 63) • Enhanced penalty on second and subsequent convictions(sec. 63A)	• Punished with imprisonment not less than 3 months or which may extend up to 3 years or fine (not less than 50,000 up to 2 lakhs) • Punished with imprisonment for a term which shall not be less than one year

[20] THE COPYRIGHT ACT, 1957 (14 OF 1957), .

	• Knowing use of infringing copy of computer programme to be an offence(sec.63B)	but which may extend to three years and with fine which shall not be less than one lakh rupees but which may extend to two lakh rupees • Punished with imprisonment for a term which shall not be less than seven days but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees:
Information Technology Act,2000[21]	• Tampering with computer source Documents (sec. 65 IT Act)	• punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both

[21] MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department), .

	• Hacking with computer systems, Data Alteration (sec. 66 IT Act)	• punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both
	• Sending offensive messages through communication service, etc. (sec. 66A IT Act)	• e punishable with imprisonment for a term which may extend to three years and with fine
	• Dishonestly receiving stolen computer resource or communication device (sec. 66B IT Act)	• Punished with which may extend to three years or with fine which may extend to rupees one lakh or with both.
	• Identity theft (sec. 66C IT Act)	• Punished with which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
		• Punished with which may

 [ISSN 2581-5369]

	• Cheating by personating by using computer resource (sec. 66D IT Act) • Violation of privacy (sec. 66E IT Act) • Cyber terrorism (sec. 66F Act) • Publishing or transmitting obscene material in electronic form (sec. 67 IT Act)	extend to three years and shall also be liable to fine which may extend to one lakh rupees. • Shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. • Punishable with imprisonment which may extend to imprisonment for life. • Punished with imprisonment which may extend to three years and with fine which may extend to five lakh rupees. • Punished with five years and with fine which

	• Publishing or transmitting of material containing sexually explicit act, etc. in electronic form (sec. 67A IT Act) • Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form (sec. 67B IT Act) • Preservation and Retention of information by intermediaries (sec.67C IT Act)	may extend to ten lakh rupees. • Punished with imprisonment of five years and with fine which may extend to ten lakh rupees. • Which may extend to three years and also be liable to fine.

V. CONCLUSION & SUGGESTIONS

Researchers want to conclude that information availability makes it easier to facilitate and automate fraudulent behaviour and gives organised groups easier access. Your crime network may link opportunistic offenders. Knowing that prevention is better than cure, intelligent internet users should take precautions against cybercrime. Illegal activities are expanding, according to researchers. Syndicates target individuals, groups, and companies with advanced technology. National and international governments have made attempts to prevent cyber-

attacks, but they need syndicates' advanced technology. The cyberattack was simply terminated.

Suggestions

Everyone should be freely and swiftly notified about cyber-attacks, including governments, private organisations, hospitals, physicians, schools, and enterprises. Everyone should know about new technology and take precautions. Every school needs a cyber-orientation. The government should explore mafia cyber-attack patterns using forensics. Computer forensics helps identify criminals. Every authority must follow cybercrime laws and rules. Address cyber complaints immediately. The Indian government can make new laws about criminal acts and should update them. Government should develop new criminal standards and policies. After privacy violations, Beijing implemented an online privacy law. India passed this law with the Anti-Child Pornography Act.

This is a good effort to stop cyber and criminal activity and notify everyone. Democratize threat intelligence data.

*****

 [ISSN 2581-5369]