



CYBER LAW AND CYBER SECURITY IN INDIA - AN ANALYTICAL STUDY

1008

Navpreet Singh¹, Rachana Vasant Kumar Kunde², Ujjwal Kumar Singh³, Abhiranjan Dixit⁴,
Alankar Upadhyay⁵, Shashank Tyagi⁶, Ramakant Tripathi⁷

Abstract

In India, cybercrime is on the rise. Cybercrime poses a distinct threat to developing countries like India. In this article, we look at India's cybercrime and Cyber Law. The doctrinal approach was used to gather the material for this topic, which included books, magazines, websites, newspapers, states and sentences, and so on. We provide a framework that describes the linkages between formal and informal institutions, the many sources of wealth and poverty, and concerns linked to international relations with cybercrime and Cyber Law, and then use it to evaluate cybercrime and Cyber Law in India. The findings imply that cybercrime and Cyber Law in poor nations are influenced by international relations, institutional challenges, and development.

Keywords: Cyber Law, Cybercrime, Hacking, social media, E-mail, Networking

Number: 10.14704/nq.2022.20.7.NQ33129

Neuro Quantology 2022; 20(7):1008-1014

INTRODUCTION

With the increased usage of computers in society, cybercrime has become a significant problem. Due to technological advancements, humans are now dependent on the internet for all of their work. Due to the internet, humans have gained access to everything while sitting in a single location. Every potential activity that a human can do can be done by the use of the internet. For example, networking, e-shopping, e-schooling, and online employment either

gambling, intellectual property theft, email forgery, forgery, cyber libel, and cyber bullying. Illegal activities that target computers include unauthorised access to computers, computer systems and computer networks; electronic data theft; email bombing; Salami attacks; logic

***Corresponding Author:** - Navpreet Singh

Address:¹Law College Dehradun faculty of Uttarakhand University, Dehradun - 248007, Uttarakhand, India, gillsaab693@gmail.com

²Law College Dehradun faculty of Uttarakhand University, Dehradun - 248007, Uttarakhand, India, rachanakunde11@gmail.com

³Assistant Professor, Law College Dehradun faculty of Uttarakhand University, Dehradun - 248007, Uttarakhand, India, ujjwalsingh@uttarakhanduniversity.ac.in

⁴Assistant Professor, Law College Dehradun faculty of Uttarakhand University, Dehradun - 248007, Uttarakhand, India, abhiranjan@uttarakhanduniversity.ac.in

⁵Assistant Professor, Law College Dehradun faculty of Uttarakhand University, Dehradun - 248007, Uttarakhand, India, alankarupadhyay@uttarakhanduniversity.ac.in

⁶Assistant Professor, Law College Dehradun faculty of Uttarakhand University, Dehradun - 248007, Uttarakhand, India, shashanktyagi1009@gmail.com

⁷Assistant Professor, Law College Dehradun faculty of Uttarakhand University, Dehradun - 248007, Uttarakhand, India, rtripathi@uttarakhanduniversity.ac.in

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Received:

Accepted:

activity. It is an "illegal action in which the computer is a tool or a target, or both." A computer may be used to perpetrate financial crimes, illicit drug sales, Pornography, online

have long hidden behind bogus promotions, giveaways, and offers. Criminals create security phantoms in order to get personal information About internet users. Cybercriminals pose as a



genuine authorised person of the bank in order to get access to the account holder's personal information. Cybercriminals, in particular, have been abusing people's credit card information via online fraud. (Shah)

Hacking, cracking, disseminating obscene material, email spoofing, SMS spoofing, and cyber stalking are examples of cybercrime against people.

Property Crime in Cyberspace: Malware software often includes computer intrusion for personal, website, and email conversations. These assaults assist cybercriminals in destroying computer data or stealing information from internet users, and they deny the victim's vital information, who has already been attacked by this attack. In this case, a cybercriminal gains unauthorised access to a real person's internet bandwidth. Such theft is also classified as cybercrime on the internet. Personal property has been violated in the same way. (Mali)

Cyber Crime against Government: Cybercriminals not only target commercial institutions but also government agencies. A government agency may have one or several secure databases, depending on the department, such as the bank or transportation. These databases were hacked with the intention of abusing private information, a practice known as cyber terrorism. In this context, the word "cybercrime" is usually defined by the CBI as "the premeditated, politically driven attack against computer data, systems, and programmes that results in non-combat violence by cybercrime actors." (Singh)

Cyber Crime against Society: A cyber-attack in society has been a fundamental activity of cybercrime. Internet consumers offer their confidential and sensitive information for the insane purpose of having it exploited by cybercriminals and resulting in financial loss. Online gambling, cyber trafficking, forgery, and child pornography are examples of these crimes. (Gupta and India)

CYBER LAW IN INDIA

Cybercrimes include crime, fraud, forgery, defamation, etc., all of which are covered under the Indian Penal Code. The Information Technology Act of 2000 covers a slew of new contemporary offences that have evolved as a

consequence of the abuse of computer systems. The Act categorizes a wide range of offenses. They've done things like hacking, disseminating obscene or pornographic electronic information, breaking confidentially, and uploading fraudulent digital signatures, to name a few. (Fatima) The Indian Parliament has enacted the present law that deals specifically with cybercrime. The legislative provisions related to cybercrime have been provided under Chapter XI of the Information Technology Act, 2000, titled "Offenses," which deals with the various types of offences that have been committed in the electric types or possibly regarding computer systems, computer systems, or computer networks. The Indian Penal Code, 1860, has also been updated to include cybercrime within its ambit. Surprisingly, neither the word "cybercrime" nor "cyber offense" has been recognized, nor has this phrase been required by the Information Technology Act of 2000.

Cybercrimes are penalised under the Information Technology Act of 2000, as stated below.

These have been listed below.

- Protected system access;
- Invasion of privacy and secrecy;
- Cheating through percolation through the use of a computer resource;
- Offenses involving computers;
- Cyber-terrorist attacks against government organizations
- Information disclosure in violation of a legally binding contract;
- Receiving a stolen computer resource or communication device dishonestly;
- Failure to comply with the controller's instructions;
- Identity Theft;
- Corporate Infractions;
- Electronic Signature Certificate Offenses;
- The publication of obscene content in electronic form;
- Sending obscene texts through a communication service;
- Attempting to tamper with computer source material; and
- Violation of privacy.

The Information Technology Act, 2000 few common offenses have been mentioned below:

-



THE IT ACT , 2000 (The Information Technology Act, 2000)	
SECTION	OFFENCE
43	Penalty and compensation for damage to computer, computer system, etc.
65	Tampering with computer source documents
66	Hacking with computer system
66A	Punishment for sending offensive messages through communication services
66C	Identity theft
66D	Punishment for cheating by impersonation by using computer resource
66E	Punishment for violation of privacy
66F	Cyber terrorism
67	Punishment for publishing or transmitting obscene material in electronic form
67B	Publishing material depicting children in sexually explicit act.
69	Failure to decrypt data
70	Attempting to access of Security System
71	Misrepresentation

Table-1.1 List of offences under IT Act, 2000

Cybercrime under the Indian Penal Code

THE IPC, 1860 (The Indian Penal Code, 1860)	
SECTIONS	OFFENCES
503	Sending threatening emails
499	Sending defamatory emails
463	Electronic record forgery
420	Prohibits bogus websites and cyber fraud.
463	Email spoofing
383	Web-Jacking
500	Abuse through E-Mail or defaming through E-Mail.

Table-1.2 List of Cyber Offences under Indian Penal Code, 1860

MEASURES TO PREVENT CYBER CRIME

Multidimensional public-private partnerships, including law enforcement agencies, the information technology sector, information security organisations, internet corporations, and financial institutions, are essential to effectively tackle cybercrime. (Johansen)

Cyber thieves, unlike their physical counterparts, do not fight for power or control. Instead, they work together to improve their skills and even help one another find new opportunities. As a consequence, standard crime-fighting techniques would be ineffective in combating cybercrime in India.

Some techniques that can be followed to avoid cybercrime:-

Use Strong Passwords: Use separate passwords for various websites, and change your passwords often. Increase the difficulty. This requires at least ten characters, including letters, numbers, and symbols. A password manager may help you keep your credentials secure.

Maintaining Online Privacy: Maintain the privacy of your social networking accounts (Facebook, Twitter, YouTube, and so on). Check your security settings thoroughly. Use caution while posting information on the internet. Once anything is on the Internet, it is there for good.

Keeping Smartphone Safe: Many people are unaware that their cell phones are vulnerable to hazardous malware like computer viruses and hackers. Make certain that you only download software from reliable websites. It is also vital to keep your operating system up-to-date. Install anti-virus software as well as a secure lock screen. Otherwise, if you misplace your phone or set it down for a few seconds, anybody may access all of your sensitive information. Someone may even install malicious software that tracks your every move using your GPS.

Safeguard your data: Encrypt your most sensitive files, such as bank documents and tax returns, to protect your data.

Protect your identity online: When it comes to securing your identity online, it is better to be too cautious than not cautious enough. You must use great care when submitting personal information such as your name, address, phone number, and/or financial information via the Internet. When making online purchases, etc., be sure the websites are secure. This includes accessing or browsing social networking sites with your privacy settings turned on.

Update your Operating System and Security Software Update: This is especially important for your operating system and Internet security software. Cybercriminals often use known vulnerabilities, or flaws, in your software to get access to your system. By repairing such vulnerabilities and flaws, you may lower your chances of becoming a cybercrime target.

Use a full-service internet security suite: A range of security technologies are required for basic Internet security. Antivirus and firewall software are required for security. A firewall is often the first line of defense for your computer. You have complete control over who and what is allowed to connect to your computer via the Internet. Consider a firewall to be a kind of "police" that inspects all data trying to enter and depart your computer through the Internet, allowing secure connections but blocking "bad" traffic such as cyber-attacks.

LANDMARK CASE LAWS

The following are some of India's most significant cybercrime cases. When the first polymorphic virus was disclosed in 1992, it was



the first cybercrime. One of the early incidents of cybercrime in India was (Yahoo v. Akash Arora, 1999). According to the court, "the defendant, Akash Arora, was accused with utilizing the trademark or domain name 'yahooindia.com,' and a permanent injunction was requested in this case." Other case of (Vinod Kaushik v. Madhvika Joshi, 2012), in which the Hon'ble court held that accessing the spouse and father's accounts through email without their authorization is illegal under section 43 of the IT Act 2000. In 2011, a decision was made on this issue. All of these instances are about the rise of cybercrime, with an emphasis on India."

Arif Azim v. CBI (Sony Sambandh Case):

"India's first cybercrime conviction occurred in 2013. It all began with a complaint filed by Sony India Private Ltd, which operates the website www.sony-sambandh.com and targets Non-Resident Indians (NRI). After purchasing Sony things online, NRIs may utilize the service to transfer them to friends and relatives in India". "The company assures that the things will be delivered to the correct people. In May 2002, a person going under the name Barbara Campa visited the website and purchased a Sony Color Television and a cordless earphone. She gave her credit card details and requested that the things be sent to Arif Azim in Noida. The payment was cleared by the credit card company, and the transaction was completed. After the company performed the relevant due diligence and inspection procedures, the items were delivered to Arif Azim". "During the delivery, the company took digital images showing Arif Azim receiving the box. The transaction was completed at that moment, but the credit card company informed the business one and a half months later that the purchase was unlawful since the genuine owner had denied making it. The business reported online cheating to the Central Bureau of Inquiry (CBI), which launched an investigation under Indian Penal Code Sections 418, 419, and 420. Arif Azim was arrested when the event was investigated. According to investigations, Arif Azim stole the credit card details of an American citizen while working at a contact center in Noida, which he exploited on the company's website". "The CBI recovered the color television and cordless headphones in this one-of-a-kind cyber fraud case. The CBI had enough evidence to prove their case in this case,

thus the accused admitted his guilt. Arif Azim was found guilty under Indian Penal Code Sections 418, 419, and 420, making him the first cybercriminal to be proven guilty. The Court, on the other hand, decided that a humanitarian approach was warranted since the accused was a young child of 24 years old and a first-time offender. As a consequence, the accused was sentenced to a year of probation by the Court. The judgment has far-reaching consequences for the whole nation. Apart from being the first cybercrime conviction, it has shown that the Indian Penal Code may be utilized successfully for various forms of cybercrime that are not covered under the Information Technology Act 2000." (Arif Azim v. CBI , 2013)

Shreya Singhal v. Union of India: "The validity of Section 66A of the Information Technology Act was challenged in this case on the basis of the right to free speech and expression guaranteed by Article 19(1)(a) of the constitution. In the current instance, two ladies, ShaheenDhada and Rinu Srinivasan, wrote a message on social media criticizing the state's Bandh declaration mourning the death of the founder of a political party, Shiv Sena. The women were detained under Section 66A of the Information Technology Act, which specifies the penalty for conveying unpleasant remarks through electronic means. The Supreme Court ruled that section 66A of the IT Act is not legally unconstitutional and hence affirmed its constitutionality." (Shreya Singhal v. Union of India, 2015)

Fraud at the Citibank Mphasis Call Center in Pune: "In 2005, \$350,000 was transferred illegally from four Citibank accounts in the United States to a few bogus accounts through the internet. The employees gained the customers' confidence and obtained their PINs with the expectation that they would be able to aid them in coping with difficult circumstances. They were seeking for weaknesses in the Mphasis system rather than decoding encrypted software or breaking firewalls".

"The defendants in this case, according to the Court, are former Mphasis contact center workers. Every time an employee enters or leaves the building, they are vetted. As a consequence, the employees were able to recall the numbers. The monies were sent through SWIFT, or the Society for Worldwide Interbank



Financial Telecommunications. The offense was committed through gaining unauthorized access to customer electronic accounts. As a consequence, this event has been labeled a cybercrime. The IT Act is wide enough to include these kinds of violations, and any IPC violation using electronic documents might result in the same penalties as conventional materials". "The Court determined that Section 43(a) of the IT Act 2000 applies because of the sort of unlawful access involved in conducting transactions. Sections 66 of the Information Technology Act of 2000, as well as Sections 420, 465, 467, and 471 of the Indian Penal Code, were also brought against the defendants."

Avinash Bajaj v. Delhi State: "In this case, the petitioner was the managing director of the Baze Company, an online shopping platform. A pornographic movie was published to the website, and the corporation waited 2-3 days to delete it, but many people bought it before that, therefore he was prosecuted under sections 292 IPC and 67 of the IT Act. The court determined that Mr. Avinash was not involved in the uploading of a pornographic video, and that the site is similar to a third-party platform where sellers register to sell their products and buyers purchase goods and services from them, and thus the petitioner was released after paying two sureties of Rs. 1 lac each." (Avinash Bajaj v. State, 2008)

Ajay Sood v. The National Association of Software and Service Companies: "The plaintiff in this case was the National Organization of Software and Services Companies (Nasscom), India's biggest software organization. Owners and operators of a recruiting and recruitment firm were the defendants. On behalf of Nasscom, the defendants produced and distributed emails to third parties in order to obtain personal information for headhunting purposes. The Delhi High Court, according to the Court, acknowledged the plaintiff's trademark rights and ordered an ex parte ad interim injunction preventing the defendants from using the trade name or any other name that was confusingly similar to Nasscom. The accused were also forbidden from claiming Nasscom membership or affiliation". "During the investigation, it was discovered that the defendants, who sent the illicit emails under their names, were using phony identities created on the directions of an

employee in order to escape discovery and legal consequences. The defendant was ordered to pay damages for infringing on the plaintiff's trademark rights. The Supreme Court declared that internet phishing is unlawful and susceptible to injunctive relief and monetary penalties in this historic decision." (National Association of Software v. Ajay Sood, 2005)

Poona Auto Ancillaries Pvt. Ltd. of Pune v. Punjab National Bank, HO New Delhi: "In one of the largest compensation verdicts in a judicial adjudication of a cybercrime case, Maharashtra's IT secretary Rajesh Aggarwal ordered Punjab National Bank (PNB) to pay Rs 45 lakh to complainant Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries, in 2013. A fraudster deposited Rs 80.10 lakh from Matharu's PNB account in Pune after he reacted to a phishing email. Since he responded to the phishing email, the complainant was asked to share responsibility, but the bank was held accountable due to a lack of proper security checks against fraudulent accounts established to defraud the Complainant." (Poona Auto Ancillaries Pvt. Ltd. of Pune v. Punjab National Bank, HO New Delhi, 2011)

SMC Pneumatics (India) Pvt. Ltd v. Shri Jogesh Kwatra
"The Delhi High Court has gained jurisdiction over a dispute involving a corporation's reputation being defamed via emails and imposed a strong ex parte injunction in India's first cyber libel case In this case, Defendant Jogesh Kwatra, an employee of the Plaintiff Company, began sending derogatory, defamatory, obscene, vulgar, lewd, and abusive emails to his employers, as well as to various subsidiaries of said company around the world in order to smear the company and its CEO, Mr. RK Malhotra, among the many cyber cases in India. The plaintiff filed a lawsuit seeking a permanent injunction prohibiting the defendant from sending him disrespectful emails The defendant's emails were clearly obscene, vulgar, abusive, threatening, humiliating and defamatory, according to the plaintiff. The purpose of sending the aforementioned emails, according to the lawyer, was to tarnish the plaintiff's legendary reputation in India and the world. He went on to say that the defendant's actions in sending the emails had infringed the plaintiff's legal rights".



(SMC Pneumatics (India) Pvt. Ltd v. Shri Jogesh Kwatra, 2014) In addition, the respondent is prohibited from transmitting the aforementioned emails. It should be noted that the plaintiff company fired the defendant after learning that the aforementioned employee had been sending abusive emails. The Honorable Judge of the High Court of Delhi ordered an ex parte injunction ad interim after hearing extensive arguments from the plaintiff's lawyer, ruling that the plaintiff had established a prima facie case. As a result, the defendant was prohibited from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails to the plaintiff or its sister corporations worldwide, including their CEOs and sales and marketing departments, in this cyber fraud case in the India. Additionally, the defendant is prohibited from posting, distributing, or causing to be posted any derogatory, defamatory, or abusive information in the real world or online, according to the Honorable Judge. The Delhi High Court's decision is important because "it is the first time that an Indian court has assumed jurisdiction in a case involving cyber defamation and issued an ex parte injunction prohibiting the defendant from defaming the plaintiff by sending derogatory emails, defamatory, abusive or obscene. to the plaintiffs or their subsidiaries." (SMC Pneumatics (India) Pvt. Ltd v. Shri Jogesh Kwatra, 2014)

Suhas Katti v. State of Tamil Nadu: "The lawsuit originates from an obscene, libelous, and abusive statement posted in a Yahoo chat room about a divorced lady. The defendant also wrote the victim, asking for information, using a fake email account she put up in the victim's name. Following the publishing of the message, the woman was bombarded with unsolicited phone calls from individuals mistaking her for a lawyer. The defendant paid the fine and was sentenced to Central Prison in Chennai. This was India's first conviction under Section 67 of the Information Technology Act of 2000." (Suhas Katti v. State of Tamil Nadu, 2004).

Pawan Kumar Rana v. The State of Jharkhand: "The criminal petition has been filed for quashing the criminal proceeding, a FIR was logged stating that ajaykumarojha had a saving bank account at SBI Branch, he received a phone call and the caller introduced himself as bank officer and on his demand the informer

narrated the OTP number and the informant's money was deducted after asking the OTP number. Considering the facts the compromise between the parties had already received the amount in question. This cybercrime case arising out of case pending in the court of learned Additional Session Judge-II-cum-special Judge, Jamshedpur, were quashed." (Pawankumarrana v. The State of Jharkhand, 2022).

Faiyaz Ansari v. The State Of Jharkhand: "The petitioner was made an accused in connection with the Dhanbad cyber crime and was registered under sections 419, 420 of IPC and sections 66C, 66D of the I.T Act, pending in the court of Additional Session Judge-II. The earlier bail application was rejected to expedite the trial. It was submitted that two witnesses were examined and they turned hostile. It also appeared that during the course of investigation it transpired that some of the pilfered amount was also transferred to the account of the petitioner. considering the facts and circumstances of the case, the petitioner was directed to be released on bail on furnishing the bail bond of Rs. 20,000/-." (Fayaz Ansari v. The State of Jharkhand, 2022).

CONCLUSION

The Information Technology Act and the rules were enacted for the control of cyber legal. The provisions of the Indian Penal Code, 1860, may be considered where the Information Technology Act is not able to deal with the offence. The current cyber law system, on the other hand, is incapable of dealing with the wide range of cybercrime that occurs. Cybercrime is growing at a quick rate as the country works toward the 'Digital India' movement, with new categories of cybercrime being found to the cyber law regime on a regular basis. Since social media and e-commerce websites started getting popular, The Information Technology (Amendment) Act 2008, did bring many changes into the Act but in today's time it has not been able to keep up with the growing technology and use. Data Protection Bill was also introduced by has not been passed yet in the parliament, this bill may solve many problems related to data protection and right to privacy. As a consequence, some legislative amendments are required in order to reduce such crimes.



BIBLIOGRAPHY

- Arif Azim v. CBI, (2008) 105 DRJ 721: (2008 150 DLT 769 (2013)).
- Avnish Bajaj v. State, NCT 2008 150 DLT 769. (Delhi High Court 05 29, 2008).
- Bahuguna, R., & Parvez, A. (2018). Scientific Evidence & the Law: Challenges and Prospects. *Research Journal of Social Science & Management*, 8 (1), 127-132.
- Fatima, Talat. *Cyber Law in India*. Alphen Aan Den Rijn, Wolters Kluwer, 24 Feb. 2017, www.amazon.in/Cyber-Law-India-Talat-Fatima-ebook/dp/B07W4M6CKJ.
- Fayaz Ansari v. State of Jharkhand (High Court of Jharkhand, 18 09, 2022).
- Gupta, Apar, and India. *Commentary on Information Technology Act : With Rules, Regulations, Orders, Guidelines, and Reports*. Gurgaon, Lexis Nexis Butterworths Wadhwa Nagpur, 2011.
- Johansen, Alison Grace. "Norton." *Norton.com*, 2018, us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html.
- Mali, Adv Prashant. "Classification of Cyber Crimes." *Lawyersclubindia*, 7 Aug. 2009, www.lawyersclubindia.com/articles/classification-of-cybercrimes--1484.asp.
- National Association of Software v. Ajay Sood, 119 (2005) DLT 596 (Delhi High Court 03 23, 2005).
- Pawan Kumar Rana v. State of Jharkhand (High Court of Jharkhand, 28 03, 2022).
- Poona Auto Ancillaries Pvt. Ltd. of Pune v. Punjab National Bank, HO New Delhi, 4 (11 09, 2011).
- Shah, Ms. "Cyber Crimes in India: Trends and Prevention." *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (Supreme Court of India 03 24, 2015).
- Singh, Y., & Jha, R. S. (2014). Copyright Protection in Present IPR Regime: A Critical Analysis of Different Protection Standards. *The Horizon, A Journal of Social Science*, V (II), 102-113.
- Singh, Yatindra. *Cyber Laws: A Guide to Cyber Laws, Information Technology, Computer Software, Intellectual Property Rights, E-Commerce, Taxation, Privacy, Etc., along with Policies, Guidelines, and Agreements*. Gurgaon, Haryana, India, Universal Law Publishing, An Imprint Of Lexisnexis, 1 Jan. 2016.
- SMC Pneumatics (India) Pvt. Ltd v. Shri Jogesh Kwatra (Delhi District Court 02 12, 2014).
- Suhas Katti v. State of Tamil Nadu, 4680 (Metropolitan Magistrate, Egmore 11 05, 2004).
- The Indian Penal Code*. (1860).
- The Information Technology Act*. (2000).
- Totla, Molshree. "Pune Citibank Mphasis Call Center Fraud." *Black N' White Journal*, 17 July 2020, bnwjournals.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/. Accessed 22 May 2022.
- Vinod Kaushik v. Madhvika Joshi, W.P.(C) 160/2012 (High Court of Delhi 01 27, 2012).
- Yahoo v. Akash Arora, 1999 ILAD Delhi 229 (02 19, 1999).
- Jha, A., Kumari, A., Rawat, P., Dixit, A., Jha, R. S., 'Is India's Cyber-Security an Outdated System on Life-Support?' *International Journal of Mechanical Engineering*, Vol. 7 No. 3 March, 2022.
- Agarwal, A., Singh, V. S., Dixit, A., Singh, M., Jha, R. S., 'A Legal Analysis of Emerging Threats of Cyber Crimes

in India' *International Journal of Mechanical Engineering*, Vol. 7 No. 6 June, 2022.

Supriya, R., Tomar, P., Singh, K., Bhardwaj, M., Tyagi, S., 'Cyber Crimes in India: A Critical Analysis' *International Journal of Mechanical Engineering*, Vol. 7 No. 6 June, 2022.

