International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Laws in India: Assessing the Current Landscape and Challenges

Dr. Rana Parveen[1], Ranjana[2]
[1]Research Supervisor, School of Law & Jurisprudence, Shri Venkateshwara University, Gajraula.
[2]Research Scholar, School of Law & Jurisprudence, Shri Venkateshwara University, Gajraula.

Abstract
The rapid evolution of communication technologies has revolutionized global connectivity while simultaneously escalating the prevalence of cybercrime, commonly called e-crimes. These digital offenses severely threaten individuals, businesses, and nations, affecting millions worldwide. Given the borderless nature of cybercrime, a unified and strategic approach is essential to mitigate its impact. This paper provides a comprehensive analysis of cybercrime, exploring its definitions, classifications, and key manifestations. Furthermore, it examines India's legislative framework for combating e-crimes, offering insights into how legal systems adapt to counter emerging cyber threats.

Keywords: Cybercrime, Cyber Law, Digital Security, E-Crimes, Internet Crimes

A. Review of Literature

(i) Joshua B. Hill et al. (2016), in *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*, discuss how technological advancements have led to a rise in cyber-enabled crimes, making them a growing global concern. The book provides a detailed analysis of the evolution, legal framework, and countermeasures against cybercrime at various governmental levels. It explores different forms of cybercrimes, including emerging internet-specific offenses, and examines their far-reaching impact.

(ii) Shubham Kumar et al. (2015), in *Present Scenario of Cybercrime in India and Its Preventions, categorize and analyze Cybercrimes in India*, highlighting instances driven by ignorance or malicious intent. The authors present statistics indicating India's high cybercrime rates, ranking second in Asia per International World Stats. The paper defines cybercrime in legal terms, examines various offenses such as email spoofing, phishing, identity theft, and internet fraud, and discusses existing cyber laws, penalties, and preventive measures.

(iii) Jigar Shah (2016), in *A Study of Awareness About Cyber Laws for Indian Youth*, proposes a conceptual model for enhancing cybercrime awareness among internet users. Shah provides statistical insights and multiple definitions of cybercrime, followed by an analysis of cybercrime categories. The study emphasizes the importance of user awareness and presents a data-driven evaluation of the issue.

B. Research Objective & Design

This research aims to analyze the cybercrimes in India concerning the authentic data available. The data obtained has been standardized, studied, and exhaustively analyzed. The objective of this paper is to kn

[1] Research Supervisor, School of Law & Jurisprudence, Shri Venkateshwara University, Gajraula.
[2] Research Scholar, School of Law & Jurisprudence, Shri Venkateshwara University, Gajraula.

ow:

1. What are the types of Cybercrimes?
2. What are the Laws related to Cybercrime in India?
3. How can we prevent Cybercrimes?

This paper examines cybercrime and deals with its various types, including hacking, salami attacks, phishing, spoofing, email bombing, logic bombs, trojan attacks, and many others. Additionally, the paper provides a mind map of these types of cybercrime in decent detail. Moreover, the paper talks about Cyber laws in India.

Various sections of the Information Technology Act, 2000, BNS, BSA, etc. are discussed along with broad areas covered under cyber law like internet fraud, copyright, defamation, etc. We further have dealt with the future of Cyber laws. The following 3 sections examine the statistical data of Cyber-crimes in India. Additionally, section 3 concludes the measures to be taken to prevent cyber-crime.

C. Research Methodology

This study employs a combination of doctrinal and rational research methodologies. It relies on both primary and secondary sources to ensure a comprehensive analysis. Primary sources include various statutes, legislative reports, and judicial decisions that shape the legal framework of cyber laws in India. Additionally, secondary sources such as books, academic journals, research articles, newspapers, magazines, blogs, and credible online resources are utilized to supplement the study. By integrating these diverse sources, the research aims to provide a well-rounded perspective on the current landscape of cyber laws in India.

1. Introduction

Cybercrime is a modern form of criminal activity involving illegal acts committed through computers, the internet, or other digital technologies recognized by the Information Technology Act. It is one of the most prevalent crimes in India, causing significant harm to society and the government while allowing perpetrators to conceal their identities.

Broadly, cybercrime refers to any unlawful activity where a computer or the internet serves as a tool, a target, or both. Although Indian courts have interpreted the term in various cases, it is not explicitly defined in any legislation. With the rapid integration of technology into daily life, cybercrime continues to evolve, encompassing offenses such as cyberstalking, cyberterrorism, email spoofing, email bombing, cyber pornography, and cyber defamation. Additionally, certain traditional crimes may also fall under cybercrime when committed via digital means.

2. Cybercrime: A Way Forward

Cybercrime involves the use of technology to commit traditional offenses such as theft, fraud, and robbery or to execute targeted attacks like hacking security systems to gain unauthorized access. These crimes can occur at individual, governmental, or national levels, often driven by political, economic, or military motives. However, in cases of cyber warfare, no legal framework or law enforcement agency can guarantee absolute protection or resolution.

Cybercrime also includes "virtual-only" offenses, such as distributing illegal content or sensitive data. Organized cybercriminal groups provide digital tools and services, ranging from denial-of-service attacks to system breaches, catering to individuals and even governments. As digital dependency grows, such offenses will become more prevalent, pushing law enforcement deeper into the cyber realm.

Despite its increasing significance, Indian law lacks a precise definition of cybercrime. Even the Information Technology Act of 2000, despite significant amendments, does not explicitly define the

term. Broadly, cybercrime refers to any unlawful activity conducted over the internet or via digital systems.

We do not have a specific definition of cybercrime however the Oxford Dictionary defines cybercrime as follows:

"*Criminal activities committed via computers or the Internet*."[3]

"*Cybercrime can be defined as those species whose genus is a traditional crime and where the computer is either an object or a subject of the criminal conduct*."[4]

3. Various Types of Cybercrime

Child Pornography: One of the most heinous forms of cybercrime, child pornography involves the exploitation and abuse of children through digital platforms. Cybercriminals often utilize the anonymity of the internet to groom and manipulate young victims, luring them into harmful situations. The spread of child pornography poses a severe threat to the safety of minors worldwide, necessitating stringent legal measures and public awareness to combat it.

Hacking: Hacking refers to unauthorized access to computer systems, networks, or devices with the intent to steal, alter, or destroy data. Hackers exploit vulnerabilities in software or hardware to gain entry, often for financial gain or to disrupt services. This illegal activity can lead to significant financial losses and data breaches for individuals and organizations alike.

Denial of Service Attack: Denial of Service (DoS) attacks aim to overwhelm a target system, rendering it inoperable. By flooding a server with excessive requests, hackers can disrupt services, causing downtime for businesses and frustration for users. These attacks can have devastating impacts, especially on online services critical for communication and commerce.

Virus Dissemination: The spread of malicious software, including viruses, worms, and logic bombs, is a common form of cybercrime. These programs can infiltrate systems, corrupt files, and disrupt normal operations. Virus dissemination often occurs through email attachments or infected downloads and can lead to severe data loss and system failures.

Computer Forgery: Computer forgery involves altering digital records or documents to deceive others. This can include the creation of fake documents or the manipulation of existing records. The rise of sophisticated printing technologies has made it easier for criminals to produce convincing forgeries, leading to significant financial fraud and legal repercussions.

Phishing: Phishing scams involve deceptive emails or messages that appear legitimate but are designed to steal sensitive information. Attackers often impersonate reputable organizations to trick individuals into providing personal data, such as passwords or credit card numbers. Awareness and education are key to preventing falling victim to these schemes.

Spoofing: Spoofing involves impersonating another device or user to gain unauthorized access to a network. This technique can be used to steal information, install malware, or conduct fraudulent activities. Spoofing highlights the importance of verifying identities and implementing security measures in digital communications.

Cyberstalking: Cyberstalking is a form of online harassment where individuals use digital means to intimidate or threaten victims. This can include persistent messaging, monitoring social media, or

[3] Oxford by Lexico, https://www.lexico.com/definition/cybercrime (last visited 12th July 2021)

[4] Parthasarathi Pati, Cyber Crime, https://www.naavi.org/pati/pati_cybercrimes_dec03.htm (last visited: 12 July 2021)

spreading false information. The psychological impact of cyberstalking can be severe, affecting victims' mental health

Salami Attack: A salami attack involves making small, inconspicuous changes to financial data that, when aggregated, result in significant theft. For instance, a hacker might deduct tiny amounts from numerous accounts, making it difficult for victims to notice. This method highlights the need for vigilant monitoring of financial statements.

Email Bombing: Email bombing is a tactic used to send massive quantities of emails to a target, overwhelming their inbox and potentially crashing email servers. This disruptive behavior can be used as a form of attack against individuals or organizations, causing significant operational challenges.

Data Diddling: Data diddling refers to the unauthorized alteration of data before or during processing. This manipulation can result in false reports or inaccurate financial statements, leading to significant repercussions for businesses and individuals alike.

Virus Attacks: Viruses attach themselves to files and spread through networks, while worms replicate independently, consuming system resources. Both can lead to extensive damage, including data corruption and loss of functionality. Understanding these threats is vital for maintaining cybersecurity.

Logic Bombs: A logic bomb is a malicious code that executes when specific conditions are met, such as a particular date or event. These hidden threats can cause substantial damage when triggered, emphasizing the importance of regular system monitoring.

Trojan Attacks: Trojans disguise themselves as legitimate software to gain access to systems. Once inside, they can steal information, install malware, or create backdoors for future access. Users must be cautious when downloading software from untrusted sources.

Internet Time Thefts: This type of cybercrime involves unauthorized use of internet hours paid for by someone else, often resulting in financial loss for the victim. Although it may seem less common, it underscores the variety of ways individuals can be exploited online.

Cybersquatting: Cybersquatting occurs when individuals register domain names similar to established brands to sell them at a profit. This practice can lead to legal disputes and damage a company's reputation, highlighting the need for vigilant brand protection online.

Cyber Defamation: Cyber defamation involves spreading false information online to harm someone's reputation. This can occur through social media, blogs, or online reviews, and can have lasting effects on personal and professional lives.

Keystroke Logging: Keystroke logging involves capturing the keystrokes of users to steal sensitive information, such as passwords and personal data. This type of surveillance is often conducted using malicious software and emphasizes the need for robust security measures.

Data-Driven Attack: A data-driven attack uses seemingly harmless data to bypass security systems and initiate malicious activities. This tactic can exploit vulnerabilities in firewalls and security protocols, making it crucial for organizations to stay updated on cybersecurity measures.

DNS Spoofing: DNS spoofing manipulates the Domain Name System to redirect users from legitimate websites to malicious ones. This can lead to phishing attacks or malware infections, emphasizing the importance of secure browsing practices.

Dumpster Diving: Dumpster diving involves scavenging through discarded materials to find sensitive information. This low-tech method can yield significant personal data, highlighting the importance of proper disposal of documents.

s This involves the use of electromagnetic pulses to disrupt or manipulate electronic communications. While less common, it represents a serious threat to sensitive operations and infrastructure.

Digital Arrest: Digital arrest refers to the seizure of digital assets or online accounts, often by authorities. This can impact individuals and organizations, particularly in cases involving allegations of cybercrime.

After AI came onto the scene, some novel cybercrimes have been having a hard time with the authorities, which are as follows:

Voice Cloning: Voice cloning uses artificial intelligence to replicate a person's voice, potentially for malicious purposes, such as fraud or impersonation. As technology advances, so do the methods used by cybercriminals.

Ransom Fraud: Ransom fraud involves encrypting a victim's data and demanding payment for its release. This extortion tactic has become increasingly common, especially among businesses, leading to significant financial losses.

AI-Generated Crime: As artificial intelligence technology evolves, so does its use in cybercrime. AI can be employed to automate attacks, create convincing phishing messages, and exploit vulnerabilities more efficiently.

Deep Fakes: Deep fakes use AI to create realistic fake videos or audio recordings, often leading to misinformation and defamation. The potential for abuse in political, personal, and professional contexts is substantial.

4. Legal Framework on Cyber Security in India

(1) Information Technology Act, 2000: Indian cyber laws are governed by the Information Technology Act, which was implemented in 2000. This Act's major purpose is to provide secure legal protection for e-commerce by making it easy to register real-time records with the government. Several changes were made as cyber criminals got cleverer, as well as the human proclivity to misuse technology e.g., the Jan Vishwas Act, 2023. The IT Act emphasizes the heavy sanctions and penalties that protect the e-governance, e-banking, and e-commerce businesses, which were passed by India's Parliament. ITA's scope has been broadened to encompass all of the most contemporary communication devices.

The IT Act is the most significant; as it directs all Indian legislation to strictly regulate cybercrime:

Section 43 [Penalty and compensation] for damage to computer, computer system, etc.–If any person without the permission of the owner or any other person who is in charge of a computer, computer system, or computer network.

Section 66 [Computer-related offenses] If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to five lakh rupees or with both.

Section 66 [Punishment for dishonestly receiving stolen computer resource or communication device] Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C [Punishment for identity theft] Whoever, fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person, shall be

punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh**.**

Section 66D [Punishment for cheating by personation by using computer resource] Whoever, using any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

(2) The Bharatiya Nyaya Sanhita (Act no. 45 of 2023): The Bhartiya Nyaya Sanhita (BNS), which is set to replace the Indian Penal Code (IPC), 1860, also addresses cyber fraud and related offenses. The corresponding sections in the BNS for prosecuting identity theft and cyber-crimes are as follows:

a) Forgery (Section 336 of BNS)
b) False documentation (Section 336(2) of BNS)
c) Forgery pre-planned for cheating (Section 336(3) of BNS)
d) Reputation damage (Section 336(4) of BNS)
e) Presenting a forged document as genuine (Section 340(2) of BNS)

These provisions align with the need to address modern cyber-crimes and identity fraud, with a structured legal framework under the Bhartiya Nyaya Sanhita.

(3) Companies Act of 2013: Corporate stakeholders refer to the Companies Act of 2013 as the legislative necessity for everyday operations optimization. The directive of this Act binds all required techno-legal compliances, putting businesses that are less compliant in a legal bind.

The SFIO (Serious Frauds Investigation Office) was given the jurisdiction to prosecute Indian firms and their directors under the Companies Act of 2013. Following the notice of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs have been considerably more diligent and harsher in this regard.

The bill has adequately addressed all regulatory compliances, including cyber forensics, e-discovery, and cybersecurity vigilance. The Companies (Management and Administration)

Rules, 2014 impose rigorous cybersecurity standards and responsibilities for corporate directors and representatives.

(4) NIST Compliance: The National Institute of Standards and Technology (NIST), the most trusted global certifying organization, has approved the Cybersecurity Framework (NCFS), providing a unified cybersecurity approach.

The *"NIST Cybersecurity Framework*" includes all the guidance, standards, and best practices for safely managing cyber-related risks. The versatility and cost-effectiveness of this system are top priorities. It promotes vital infrastructure stability and security by:

a) Improving cybersecurity risk interpretation, control, and mitigation - to reduce data loss, misuse, and restoration costs.
b) Identifying the most critical jobs and procedures so that protection can be focused on them.
c) Demonstrates the trustworthiness of organizations that safeguard critical assets.
d) Assists in prioritizing investments to optimize cybersecurity ROI.
e) Takes care of regulatory and contractual requirements.
f) Assists in the overall information security program.

Important Cyber Crimes under various Laws one should know

Offenses	**Sections under Acts**
Damage to Computer, Computer System, etc.	Section 43 of IT Act, 2000
Power to issue direction for blocking public access to any information through any computer's resources.	Section 69A of IT Act, 2000
Power to authorize to collection of traffic information or data and to monitor through any computer's resources for cyber security.	Section 69B of IT Act, 2000
Unauthorized entry into a password-protected system.	Section 70[5] of IT Act, 2000
Penalty for misrepresentation	Section 71[6] of IT Act, 2000
Breach of confidentiality and privacy.	Section 72[7] of IT Act, 2000
Publishing False Digital Signature Certificates	Section 73[8] of IT Act, 2000
Publication for fraudulent purposes.	Section 74[9] of IT Act, 2000
Act to apply for contravention or offense that is committed outside India	Section 75[10] of IT Act, 2000
Compensation, confiscation, or penalties for not to interfere with other punishment.	Section 77[11] of IT Act, 2000
Compounding of Offences.	Section 77A[12] of IT Act, 2000
Offenses by Companies.	Section 85 of IT Act, 2000

[5] *Ibid*, S. 70
[6] *Ibid*, S. 71
[7] *Ibid*, S. 72
[8] *Ibid*, S. 73
[9] *Ibid*, S. 74
[10] *Ibid*, S. 75
[11] *Ibid*, S. 77
[12] *Ibid*, S.77A

Sending threatening messages by e-mail.	Section 351 (1)[13] BNS
Sending defamatory messages by e-mail.	Section 356 (1) BNS
Bogus websites, Cyber Frauds.	Section 318 (4) BNS
E-mail Spoofing.	Section 336 (1)[14] BNS
Web Jacking.	Section 308 (1)[15] BNS
E-mail Abuse.	Section 356 (2)[16] BNS
Criminal intimidation by anonymous communications.	Section 351 (4)[17] BNS
Online sale of Drugs.	NDPS Act
Online Sale of Arms	Arms Act

5. Future of Cyber Security Laws

India's rapid digital transformation has led to both tremendous growth and increased exposure to cyber threats like data breaches, identity theft, and cyber fraud. As the country continues to expand its digital infrastructure, the need for comprehensive cyber laws has never been more pressing. The future of India's cyber laws will depend on their ability to keep pace with emerging threats and evolving technologies while ensuring privacy and national security.

Currently, India's cyber legal framework is built around the Information Technology Act, 2000**.** Key sections address unauthorized access to systems, government surveillance powers, and liability protection for intermediaries like social media platforms. Despite updates, the IT Act has limitations in dealing with sophisticated cybercrimes and emerging technology trends.

India's Digital Personal Data Protection Act (DPDP) 2023 aims to protect personal data, influenced by international standards like GDPR. Future laws will strengthen individual data rights, corporate accountability, and clarify regulations around data storage and cross-border data flows. As AI and blockchain technologies gain traction, new cyber regulations will be needed to prevent misuse. India's reliance on digital infrastructure heightens the risk of cyberattacks, necessitating stringent cybersecurity measures and rapid response protocols. Balancing national security interests with individual privacy rights is a challenge.

[13] The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), Section 351 (1)
[14] *Ibid*, S. 336 (1)
[15] *Ibid*, S. 308 (1)
[16] *Ibid,* S. 356 (2)
[17] *Ibid,* S. 351 (4)

India's future cyber laws should prioritize data localization, specialized courts, and enhanced law enforcement capacity to combat cyber threats. Cyber literacy programs and public-private partnerships will enhance cybersecurity infrastructure, fostering collaboration and innovation to build a resilient digital ecosystem that protects national interests and individual rights.

6. Cybercrime Statistics in India (2020–2023)

India has witnessed a significant surge in cybercrime, with reported complaints rising from 1.15 million in 2020 to 1.56 million in 2023. Financial fraud, sextortion, and job-related scams, particularly KYC (Know Your Customer) expiry fraud, have been among the most prevalent offenses. The country incurred economic losses exceeding ₹10,319 crore ($1.24 billion), though some funds were recovered through initiatives like the Citizen Financial Cyber Fraud Reporting and Management System.

The rise in cyberattacks, including ransomware and Distributed Denial-of-Service (DDoS) attacks, has been fueled by both domestic and international actors, with nearly 50% of cases linked to foreign entities, particularly from China and Cambodia. Rapid digitization, combined with increasing phishing and malware incidents, has exposed critical technological vulnerabilities. In response, the Indian government has strengthened cybercrime reporting mechanisms, such as the National Cybercrime Reporting Portal, and enhanced legal frameworks. However, continuous vigilance and proactive measures remain essential.

Telangana: A Cybercrime Hotspot

Among Indian states, Telangana has emerged as a leader in cybercrime reporting, with over 23,000 First Information Reports (FIRs) filed for various cyber offenses. Most cases fall under the Information Technology Act, encompassing financial fraud, identity theft, and cyber-based sexual exploitation.

The surge in cybercrime is driven by rapid digital expansion, increasing internet penetration, and the state's growing tech ecosystem. While Telangana's government and law enforcement agencies have been proactive in strengthening cyber vigilance and encouraging public reporting, cyber threats continue to escalate. Addressing these challenges requires sustained efforts to enhance cybersecurity awareness, improve digital literacy, and reinforce legal frameworks to better protect citizens from evolving online threats.

Uttar Pradesh: Lagging in the Fight Against Cybercrime

Uttar Pradesh, India's most populous state, faces mounting challenges in combating cybercrime. Despite rapid technological growth, the state struggles with rising digital threats, including financial fraud, online harassment, and identity theft. Limited awareness, inadequate infrastructure, and a lack of trained personnel have left Uttar Pradesh vulnerable to cybercriminals.

7. Measures to prevent Cyber Crimes

Due to the borderless nature of Cybercrimes, innovative measures are required to curb the issue of *hi-tech crime*. Therefore, apart from the Cyber Laws, one should keep the following points in mind for safety in Cyberspace while surfing the Internet:

1. Cyber literacy and awareness at grassroots levels are crucial in combating cybercrime. Educational institutions can play a vital role in spreading awareness about online safety, digital hygiene, and responsible internet usage. Organizing Cyber Law awareness programs at these centers can provide students with a foundational understanding of the internet's risks and security practices.

2. Regular monitoring of financial statements is essential to reduce the risk and impact of cybercriminals targeting personal and financial information for identity theft, online fraud, and other malicious activities. By keeping track of financial activities, individuals can avoid falling victim to identity theft or other crimes that involve their sensitive financial data being compromised online.
3. Keeping operating systems up to date is another effective way to protect your computer and online accounts. Software developers frequently release updates to patch security vulnerabilities that hackers may exploit. Regularly updating your operating system and applications minimizes the chances of cybercriminals exploiting weaknesses in your software.
4. Using strong and unique passwords for online activities is another crucial defense against cybercrime. A strong password should be at least eight characters long and include a combination of symbols, letters, and numbers. Avoid using easily identifiable information, such as email ID, birth date, or name, as these can be easily traced by hackers.
5. Implementing two-step authentication on webmail and social media accounts is a critical step to safeguarding personal data from unauthorized access.
6. Installing reliable security software, such as antivirus and firewall programs, is essential for protecting your computer from malware, viruses, and unauthorized access. Integrating security suites like Norton Internet Security, which combines antivirus, antispyware, firewall, and other protection tools, can offer comprehensive protection for online activities.
7. Phishing scams often involve emails or messages requesting personal information or clicking on fraudulent links. It's crucial to avoid responding to such emails or providing sensitive information online. Legitimate companies don't ask for personal information via email. Verify the sender's authenticity and read website privacy policies before submitting any information. Being cautious with email communications and recognizing phishing attempts can help prevent falling victim to scams stealing personal and financial information.
8. Use AI Measures: AI is a new addition to the realm of cybersecurity. It can tackle and even predict the information and patterns of cybercrime. Many companies are looking forward to it.

8. Concluding Remark

What appears impeccably secure and impenetrable today may not remain so tomorrow. As a global phenomenon, the internet inevitably attracts various forms of criminal activity. With the enactment of the Information Technology Act and the empowerment of law enforcement agencies to combat cybercrime, India has taken a significant step toward reducing digital threats.

The human mind possesses boundless ingenuity, making it impossible to eliminate cybercrime. However, it can be analyzed, mitigated, and controlled. History has shown that no policy has ever completely eradicated crime; the most effective approach lies in public awareness, education, and stringent law enforcement. Educating individuals about their rights and responsibilities—such as reporting cybercrime as a collective duty—remains crucial in curbing these offenses.

Undoubtedly, the Act marks a watershed moment in the evolution of cyberspace regulations. However, necessary amendments should continue to refine its effectiveness. That said, a word of caution for proponents of stringent legislation: cyber laws must strike a balance between security and innovation. Excessive restrictions could hinder industry growth, ultimately proving counterproductive.

BIBLIOGRAPHY

1. Dennis, Michael Aaron, *Cybercrime*, Encyclopedia Britannica, (19 Sep. 2019), https://www.britannica.com/topic/cybercrime.
2. Henry et al, *Countering the Cyber Threat*, 3 no. 1 The Cyber Defense Review, 47–56 (2018).
3. *India: Promoting internet safety amongst 'netizens',* UNODC (United Nations Office on Drugs and Crimes), https://www.unodc.org/southasia/frontpage/2012/May/india_addressing-the-rise-of-cybercrime-amongst-children.html
4. Jigar Shah, *A Study of Awareness About Cyber Laws for Indian Youth*, 1(1) International Journal of Trend in Scientific Research and Development, (2016).
5. Joshua B. Hill, *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*, PSI Textbook (2016)
6. Kshetri, Nir, *Diffusion and Effects of Cyber-Crime in Developing Economies*, 31 no. 7 Third World Quarterly, 1057–1079 (2010).
7. NITIN DESAI et al. INDIA'S CYBER SECURITY CHALLENGE, (Institute for Defense Studies & Analysis, 2012)
8. Prof. Dr. Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, Telecommunication Development Sector (ITU, 2014).
9. Shubham Kumar et al, *Present scenario of cybercrime in INDIA and its preventions*, 6 no. 4 International Journal of Scientific & Engineering Research, 1971 (2015).