International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AN ANALYTICAL STUDY OF CYBER LAW WITH IT'S PROBLEMS AND SOLUTIONS

Dr. Mahendra Kumar Verma[1], **Jai Sharma[2], **Muskan Sharma[3], **Bhavna Jain[4], **Saurabh Kumar[5], **Nitin Singh Raghav [6]

[1] Head of Department Department of Para-medicals
[2] Department of Engineering
[3] Department of Law
[4] Department of Law
[5] Department of Computer Applications
[6] Department of Hotel Management
Vivekananda Global University, Jaipur

ABSTRACT :

This paper delves into cybercrime in India, exploring the legal landscape outlined by the Information Technology Act, 2000, and subsequent revisions. It highlights the multifaceted challenges posed by cyber threats and emphasizes the importance of a comprehensive approach in tackling them. Beyond legislative measures, it underscores the significance of proactive engagement from various sectors, including governmental bodies, businesses, and educational institutions. By fostering a culture of cybersecurity awareness and leveraging technological advancements, the paper seeks to equip stakeholders with the tools needed to safeguard against evolving cyber risks in India's digital ecosystem.

Key Word Cybercrime, Media, Cyber Law , IT ACT, Attacks

INTRODUCTION :

Indians are among the most active users of social media, which is not surprising given how much social media has caught Indian attention. Since users may now access social networks using a variety of apps and devices, the mobile revolution has further ensured the expansion of social networking. People frequently post things on social media without considering the consequences because it's so convenient to do it while on the go. On occasion, people submit content without giving it much thought on various social media platforms like Facebook, Twitter, Pinterest, and so on.

The Information Technology Act 2000 (IT Act 2000) in India is crucial for addressing cybercrime. This legislation makes individuals expressly liable if they post offensive or illegal content online. It goes further by categorizing users as online content providers, content service providers, and network service providers, thereby recognizing them as intermediaries under the law. The IT Act 2000 outlines stringent penalties for a range of cybercrimes, including hacking, identity theft, cyberstalking, and the distribution of obscene material. This law aims to safeguard users and ensure responsible behavior in the digital space, holding offenders accountable for their actions.

BACKGROUND STUDY:

Aim

The primary aim of this study is to analyze the various types of cyber attacks and cyber crimes prevalent in the digital landscape and evaluate the effectiveness of the Information Technology Act 2000 (IT Act 2000) of India in addressing and mitigating these cyber threats. The study seeks to identify gaps, strengths, and areas for improvement within the IT Act 2000 to enhance its efficacy in combating cybercrime.

Scope

1. *Identification and Categorization of Cyber Attacks and Cyber Crimes*:
   - Compile a comprehensive list of different types of cyber attacks, such as phishing, malware, ransomware, Distributed Denial of Service (DDoS) attacks, and hacking.
   - Identify various cyber crimes including identity theft, cyberstalking, online fraud, and distribution of obscene material.
2. *Analysis of the IT Act 2000*:

- Examine the provisions and clauses of the IT Act 2000 related to cybercrime.
- Analyze the legal definitions, penalties, and enforcement mechanisms specified in the Act.

3. *Case Studies and Real-World Examples*:

- Study real-world cases of cyber attacks and cyber crimes in India.
- Evaluate the application of the IT Act 2000 in these cases, including prosecution outcomes and legal precedents.

4. *Comparative Analysis*:

- Compare the IT Act 2000 with international cybercrime laws and frameworks to identify best practices and potential areas for enhancement.

5. *Recommendations for Improvement*:

- Based on the analysis, provide recommendations for amending and updating the IT Act 2000 to better address the evolving landscape of cyber threats.
- Suggest measures for improving enforcement, increasing awareness, and enhancing cooperation between various entities involved in combating cybercrime.

6. *Future Research Directions*:

- Identify areas where further research is needed to continuously adapt and improve the legal and regulatory framework for cybercrime in India.

Exclusion and Inclusion Criteria

To ensure the relevance and quality of studies included in the research on cybercrime, cyber-attacks, and the effectiveness of the IT Act 2000 in India, the following exclusion and inclusion criteria are established:

Inclusion Criteria

1. *Relevance to Cybercrime and Cyber Attacks*: Studies must focus on cybercrime, cyber-attacks, or related topics such as data breaches, identity theft, phishing, malware, ransomware, and Distributed Denial of Service (DDoS) attacks.
2. *Focus on India*: Studies should specifically examine cybercrime issues in India or the application of the IT Act 2000 in addressing cybercrime.
3. *Recent and Peer-Reviewed*: Preference will be given to studies published within the last 10 years (2012 onwards) in peer-reviewed journals, conference proceedings, or reputable academic sources.
4. *Empirical Research and Case Studies*: Empirical studies, case studies, and qualitative or quantitative research articles provide insights into cybercrime trends, legal frameworks, enforcement practices, or cybersecurity measures in India.
5. *Policy and Legal Analysis*: Studies that analyze the effectiveness of legal frameworks, including the IT Act 2000, in combating cybercrime in India and propose recommendations for improvement.
6. *Comparative Analysis*: Comparative studies with international cybercrime laws and frameworks that offer insights into best practices and potential enhancements to the Indian legal framework.

Exclusion Criteria

1. Irrelevant Topics: Studies not related to cybercrime, cyber-attacks, or the IT Act 2000 in India.
2. Non-English Language: Studies published in languages other than English, unless translations are available or summaries in English are provided.
3. Outdated Studies: Studies published before 2012, unless they provide significant historical context or background information relevant to the topic.
4. Non-Academic Sources: Non-peer-reviewed articles, opinion pieces, news articles, and blogs without empirical evidence or academic rigor.
5. Non-Indian Context: Studies that primarily focus on cybercrime issues in other countries without comparative analysis or relevance to the Indian context.
6. Incomplete Data or Studies: Studies lacking comprehensive data, methodology, or detailed analysis that are necessary for a rigorous academic review.

CYBERCRIME

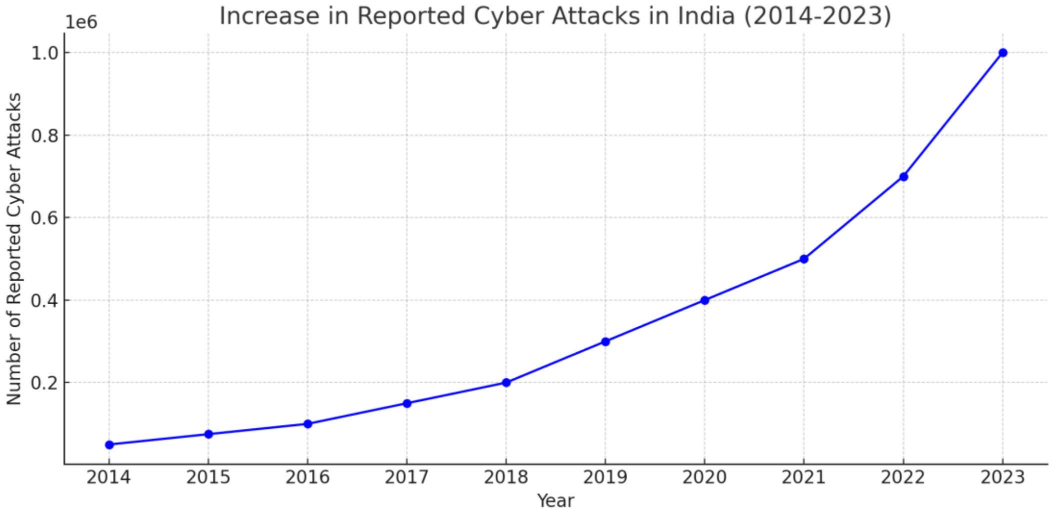
Introduction, methods, and types

What is Cyber Crime

The way we live has altered as a result of the Internet culture shift that has occurred in the new millennium. Our everyday lives now wouldn't be the same without the Internet, which we use for new forms of e-commerce, social networking connections, messaging, gaming, news, and opinion exchange, chatting, talking, sending messages, and making new friends. Cybercrime, defined as crimes committed with or through computers in cyberspace, has emerged as a result of increased Internet use. Examples of such crimes include:

- Damaging computer systems or networks
- Stealing computer software and data
- Gaining unauthorized access to computer data
- Blackmailing
- Giving threats, committing defamation, extortion, and intimidation through social media chats and by emailing
- Illegal gambling
- Cyberstalking
- Cyber espionage

Statistics



The NCRB (National Crime Records Bureau) reported a total of 11,28,265 cases of cyber-crime complaints on record with 7,48,863 (in Lacs) rupees in damages during the period 1st January 2023 to 31st December 2023.

"Cybercrime is growing at the rate of 15-20% annually in our country and more than 80,000 plus complaints have been received from West Bengal in the current year till November end in the national cybercrime reporting portal", Hari Kishore Kusumakar, Additional Director General (ADG) & IGP-Cyber Cell told The India Times on 15th December 2023.

Common methods to gain unauthorized access to devices

1. **Phishing:**

   - **Email Phishing**: Deceptive emails appear legitimate and trick users into revealing personal information or downloading malware.
   - **Spear Phishing**: Targeted phishing aimed at a specific individual or organization.
   - **Whaling**: Phishing attacks targeting high-profile individuals such as executives or senior management.

2. **Social Engineering**:

   - **Pretexting**: Attackers create a fabricated scenario to steal sensitive information.
   - **Baiting**: Offering something enticing to users (like a free download) to trick them into providing information or downloading malware.
   - **Tailgating/Piggybacking**: Gaining physical access to restricted areas by following someone with proper access.

3. **Malware**:

- **Viruses**: Malicious code that attaches to legitimate files and spreads when those files are shared.
- **Worms**: Self-replicating malware that spreads without user intervention.
- **Trojans**: Malicious software disguised as legitimate software.
- **Ransomware**: Encrypts files and demands a ransom for the decryption key.
- **Spyware**: Secretly monitors user activity and gathers information.

4. **Exploiting Vulnerabilities**:

   - **Zero-Day Exploits**: Attacks targeting previously unknown vulnerabilities.
   - **SQL Injection**: Inserting malicious SQL queries into input fields to manipulate databases.
   - **Cross-Site Scripting (XSS)**: Injecting malicious scripts into web pages viewed by others.

5. **Man-in-the-Middle (MITM) Attacks**:

   - **Eavesdropping**: Intercepting and listening to private communications.
   - **Session Hijacking**: Taking over a session between a user and a web application.

6. **Denial of Service (DoS) and Distributed Denial of Service (DDoS)**:

   - **DoS Attack**: Overloading a system with requests to make it unavailable to users.
   - **DDoS Attack**: Using multiple compromised systems to launch a large-scale attack.

7. **Password Attacks**:

   - **Brute Force**: Trying all possible password combinations until the correct one is found.
   - **Dictionary Attacks**: Using a precompiled list of likely passwords.
   - **Credential Stuffing**: Using leaked credentials from one breach to access other accounts.

8. **Insider Threats**:

   - **Malicious Insider**: An employee or contractor who intentionally exploits their access to harm the organization.
   - **Accidental Insider**: An employee who unintentionally causes harm through negligence or error.

Common types of Cyber-Attacks

1. **Advanced Persistent Threats (APTs)**: Long-term targeted attacks where attackers gain and maintain access to a network over time.
2. **Botnets**: Networks of infected devices controlled remotely by attackers to carry out various attacks, such as DDoS.
3. **Ransomware**: Malware that encrypts files and demands payment for the decryption key.
4. **Spyware and Adware**: Malicious software that secretly monitors user activity or displays unwanted advertisements.
5. **Rootkits**: Malware designed to gain root or administrative access to a system and hide its presence.
6. **Keyloggers**: Programs that record keystrokes to capture sensitive information like passwords and credit card numbers.
7. **Drive-by Downloads**: Automatically downloading and installing malware when a user visits a compromised or malicious website.
8. **Watering Hole Attacks**: Compromising websites frequently visited by a targeted group to infect visitors with malware.
9. **DNS Spoofing/Poisoning**: Altering DNS records to redirect traffic from legitimate websites to malicious ones.
10. 10.**Crypto-jacking**: Using a victim's computing resources to mine cryptocurrency without their knowledge.

PREVENTIVE MEASURES FROM CYBERCRIME

Preventions

1. **Education and Training**:

   - Regularly train employees on cybersecurity best practices and how to recognize phishing and social engineering attacks.
   - Conduct simulated phishing attacks to assess and improve employee awareness.

2. **Strong Password Policies**:

   - Enforce the use of complex passwords and regular password changes.
   - Encourage the use of password managers to generate and store strong, unique passwords.

3. **Multi-Factor Authentication (MFA)**:

   - Implement MFA to add a layer of security beyond just passwords.

4. **Regular Software Updates**:

- Keep all software, including operating systems and applications, up to date with the latest security patches.

5. **Data Backup and Recovery Plans**:
   - Regularly back up important data and ensure that backups are stored securely.
   - Develop and test disaster recovery plans to ensure quick restoration of data and services.

Technologies

1. **Firewalls**:
   - Deploy firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules.
2. **Intrusion Detection and Prevention Systems (IDPS)**:
   - Use IDPS to detect and prevent potential security breaches by monitoring network and system activities for malicious activities.
3. **Antivirus and Anti-Malware Software**:
   - Install and regularly update antivirus and anti-malware software to detect and remove malicious software.
4. **Endpoint Protection**:
   - Implement endpoint protection solutions to secure all devices connected to the network, including desktops, laptops, and mobile devices.
5. **Encryption**:
   - Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.
   - Use secure communication protocols like HTTPS, SSL/TLS, and VPNs.
6. **Secure Email Gateways**:
   - Deploy secure email gateways to filter out malicious emails and attachments before they reach users.
7. **Network Segmentation**:
   - Divide the network into segments to limit the spread of malware and restrict access to sensitive information.
8. **Security Information and Event Management (SIEM)**:
   - Use SIEM systems to collect, analyze, and respond to security incidents in real time.
9. **Threat Intelligence**:
   - Utilize threat intelligence services to stay informed about emerging threats and vulnerabilities.
10. **Behavioral Analytics**:
    - Implement solutions that use machine learning and AI to detect unusual behavior that may indicate a security breach.

Best Practices to Control Cybercrime

1. **Access Control**:
   - Implement the principle of least privilege, granting users only the access necessary for their roles.
   - Use role-based access control (RBAC) to manage permissions.
2. **Regular Security Audits and Assessments**:
   - Conduct regular security audits, vulnerability assessments, and penetration testing to identify and address security weaknesses.
3. **Incident Response Planning**:
   - Develop and maintain an incident response plan to quickly and effectively respond to security incidents.
   - Conduct regular drills and update the plan based on lessons learned.
4. **Secure Software Development**:
   - Follow secure coding practices and conduct regular code reviews to minimize vulnerabilities in software development.
5. **Physical Security**:

- Ensure physical security measures are in place to protect hardware and sensitive information from unauthorized access.

INDIAN LAWS RELATING TO CYBERCRIME

Information Technology Act, 2000

On October 17, 2000, the Indian Parliament enacted the IT Act, 2000. Pramod Mahajan, who was the minister of information technology at the time, signed it. It was constructed to uphold regulations about cybercrime and the online economy. The proposed Model Law on International Commercial Arbitration by UNCITRAL serves as its foundation. It was approved by the UN. There were 94 articles in the prior law. The Information Technology Act encourages digital identification, e-commerce, and commerce. After the Information Technology Act was introduced, India's cyber law underwent changes. Section 66A was inserted by an amendment in 2008. According to this provision, sending "offensive messages" is illegal. He proposed legislation against cyberterrorism, voyeurism, and child pornography. Section 69 was also implemented, giving the authorities the power to monitor and decrypt any information using any computer device. Everyone should behave responsibly on the Internet and be careful. Cybercrime laws in India aim to keep us safe on the web and to develop a healthy online society.

Chapter XI of this act deals with offenses or crimes along with certain other provisions. The various offenses which are provided under this chapter are shown in the following table:

OFFENCE SECTIONS UNDER IT ACT

- Tampering with computer source documents sec.65
- Hacking with a computer system, Data alteration sec.66
- Publishing obscene information sec.67
- Publishing false digital signature certificates sec.73
- Breach of confidentiality and privacy sec.72

Problem With Indian Cyber Law

The absence of comprehensive rules worldwide is one of the largest gaps in the cybercrime industry. The issue is made worse by the internet's and cybersecurity laws' unbalanced expansion. Cybercrime-related problems still exist, despite the IT Act and the Indian Penal Code Act and Amendment having made a start.

1. There is intense disagreement over jurisdiction about the viability of every case that has been filed. Nowadays, it appears as though national borders are vanishing due to the expanding reach of online. Therefore, an alternate mechanism of resolving disputes will have to take the place of the concept of geographical jurisdiction as envisioned in S.16 of the CPC and S.2 by the I.P.C.

2. Evidence loss is a frequent issue that might arise from the regular destruction of all data. Additionally, the criminal investigation system is severely hampered by the gathering of data from outside the region.

3. Cyber Army: Another requirement is to establish a sophisticated infrastructure for investigating crimes and employing highly technological personnel on the other end.

4. Although this law's section 75 addresses extraterritorial actions, it cannot have any real significance unless it is combined with a clause that acknowledges informational orders and warranties from authorities with the necessary authority. enacted outside of their purview and cooperative mechanisms for law enforcement authorities to exchange documents and evidence of cybercrime.

5. Cybercrime-aware judges are a must nowadays. Legislation on the agenda is formulated in large part by the judiciary.
   The P.I.L. (Public Interest Litigation) is one such case that deserves recognition and was accepted by email by the Supreme Court.

The word "perfect" is relative. There is nothing flawless in this world. Regulators and legislators are also fallible. As a result, the laws that they pass cannot be flawless. From the womb of globalization, cyber law was born. He is about to make a development. It will eventually deal with a wide range of intricate problems and be incorporated into the law.

Other Countries On Cybercrime And Their Cyber Laws

Computer-related theft, fraud, forgery, and hacking are all considered cybercrimes in Australia.

Cybercrimes in Belgium include electronic sabotage, fraud, forgery, and hacking involving computer systems.

The courts in Canada appear to be utilizing the current legislation about electronic sabotage, forgery, fraud, intrusion, and theft to update the law to include cybercrime.

If the website in question can be accessed from Chile, Chilean courts appear to have the authority to examine cases regarding any cybercrime involving child pornography.

While hacking itself may not be considered a criminal in the Czech Republic, what you do with the information you obtain may.

Theft and fraud involving computer systems are considered cybercrimes in Ireland.
6) Cybercrimes in Japan include electronic sabotage, forgery, fraud, hacking, and intrusion using a computer system.
7) Cybercrimes in Peru might include electronic sabotage, forgeries, and computer system infiltration.
8) Computer-related theft and fraud are considered cybercrimes in Spain.
9) In the United Arab Emirates, it appears that using electronics to offend any religion can be combined with other cybercrimes such as forgery, fraud, hacking, and theft involving a computer system.
10) Establishing and running a botnet is now considered a federal offense in the United States. Cybercrime may also include electronic sabotage, forgery, fraud, hacking, impersonation, and computer system penetration.

Result of the Research

The human mind is infinitely capable of things. Cybercriminals cannot be eliminated from cyberspace. Testing them is a feasible option. History demonstrates that no legislation has ever been able to completely eradicate crime from the earth. The only thing that can be done to reduce crime is to increase public awareness of rights and responsibilities (denouncing criminal activity is a communal duty to society) and to strictly enforce the law. France is unquestionably a historic advance in cyberspace. Moreover, I concede that alterations to the Information Technology Act are imperative to enhance its efficacy in combating cybercrime. I'd want to conclude by reminding the pro-law school that cyber law rules are not often strictly enforced, which can hamper company growth and backfire. A variety of media outlets have been used to raise awareness and knowledge about it. As a result, the notion of social cognitive communication was born. Social awareness communication is a critical approach for informing the public about social issues and keeping key social topics on the public agenda.

SUGGESTIONS

1. Create clear policies: Governments and platforms should work together to create transparent policies that address legal concerns including privacy, content moderation, and data protection.
2. Educate users through camps: Promote digital literacy to provide users with a better awareness of the legal ramifications of their actions on social media.
3. Strengthen cybersecurity measures: Put in place strong cybersecurity rules to protect user data and reduce the risk of breaches and illegal access.
4. Quick legal reactions: Create agile legal frameworks that can adapt to the constantly changing social media world, ensuring fast solutions to emergent concerns.
5. International cooperation: Encourage states to work together to develop cohesive global norms that address cross-border legal challenges related to social media platforms.
6. Regular updates: Periodically review and update existing laws to keep pace with technological advancements, guaranteeing relevance and effectiveness in the digital age.

REVIEW OF LITERATURE

A LITERATURE REVIEW OF SOCIAL MEDIA CAPABILITIES FOR COUNTER-TERRORISM
“BY JAMIE BARTLETT AND CARL MILLER NOVEMBER 2013”
LAWFUL ACCESS OF SOCIAL MEDIA BY INTELLIGENCE AGENCIES
“The legal frameworks that govern the gathering and use of private information are common in OECD countries, and SOCMINT (Social Media Intelligence) activities must abide by them. These rules guarantee that state agencies have appropriate, lawful access to citizen data, together with supervision procedures to guard against power abuses. Every nation has a unique legal system with varying guiding ideas.
In the UK, for example, obtaining potentially "private" information necessitates a rigorous licensing process and oversight by authorized authorities. Navigating the legal authority needed for certain data gathering, which is usually dictated by the idea of a "reasonable expectation" of privacy, is the main problem facing law enforcement. In the UK, even if the material comes from a public source, RIPA authorization is required if there is a possibility of getting "private information".”
CHILD SEXUAL ABUSE AND THE INTERNET—A SYSTEMATIC REVIEW
“BY SANA ALI, HIBA ABOU HAYKAL, ENAAM YOUSSEF, MOHAMMED YOUSSEF 2023”
CHILD SEXUAL ABUSE ON THE INTERNET
“The OECD's legal principles must be followed for SOCMINT (Social Media Intelligence) operations in order to guarantee proportionate, legal access to citizens' private information together with supervision procedures. Different countries have different legal systems; in the UK, gathering potentially private information requires rigorous authorization and control. Determining the legal authorization required for certain data gathering, which is based on the idea of a "reasonable expectation" of privacy, is the primary difficulty facing law enforcement.
On a different subject, there is increasing worry over child sexual abuse, especially when it occurs online. The paper emphasizes how digital platforms contribute to the global epidemic of child sexual abuse occurring online. A thorough analysis of the literature (N=42 publications) shows how frequently child pornography is used for both profit and non-profit endeavors. Online platforms hold regular abuse sessions that are frequently difficult for law authorities to locate. Predators employ a range of tactics, including extortion, to exploit victims in non-commercial ways. The study emphasizes the need

for coordinated efforts, particularly in poor countries, to decrease abuses of children's rights and offers helpful advice to mitigate online child sexual exploitation."

SOCIAL MEDIA, STUDENTS, AND THE LAW

"BY MARTHA MCCARTHY OCTOBER 2021"

CYBERBULLYING AND THE LAW

"The line separating expression on and off campus has become more hazy as the internet becomes more and more significant. Applying Tinker's criteria becomes more complicated due to the permeable barrier separating both domains, particularly in cases where student posts can be viewed on campus. The Mahanoy ruling from the Supreme Court did not provide teachers and pupils with enough direction while navigating the digital world. Students would have enjoyed strong protection if the court had applied Tinker to both in-school and off-campus speech unless their speech posed a risk of disrupting the classroom. Regretfully, there is still uncertainty in the verdict about when kids can face consequences for their speech outside of school. Schools are urged to take proactive measures to stop cruel speech in order to address this, highlighting education as a vital tool in the fight against the rising incidence of cyberbullying among young people in America."

HISTORICIZING INTERNET REGULATION IN CHINA: A META-ANALYSIS OF CHINESE INTERNET POLICIES

"BY *WEISHAN MIAO, MIN JIANG, YUNXIA PANG 2021*"

LAWS TO LIMIT POLITICAL RAMIFICATIONS OF SOCIAL MEDIA IN CHINA

"China has enacted hundreds of laws and regulations in the last 20 years to control the Internet and lessen its political implications (F. Yang & Mueller, 2014). Chinese Internet rules are composed of multiple tiers of legal restrictions that are a component of the Chinese legal system. According to the Legislation Law of the PRC, Chinese laws and regulations include laws, judicial interpretations, administrative regulations, local decrees, autonomous decrees, special decrees, and rules. The Constitution governs all laws and regulations, with laws making up the majority of legal documents and administrative rules and local decrees acting as their auxiliary forms (State Council Information Office, 2011). Few laws have a strong legal standing, even though many target the Internet. Just four of them were made into law by the National People's Congress between 1994 and 2017. The remaining ones are expressed as "rule," "decision," "decree," "administrative measure," "opinion," and even "notice." Because there isn't much high-level legislation about the Internet, authorities have released a lot of ad hoc regulations to address issues. The primary features of Chinese legislation, as identified by Tian (2008), are agency-based power, interest-driven agency, and law-sanctioned interest. Consequently, these policies aim to optimize the authority of their respective regulatory bodies."

References and Citations:

1. Jenifer Stella, S., and S. Ambika Kumari. "Cyber Space-A Critical Analysis On The Feminine Facet." (2022).

2. Mambi, Adam J. *ICT law book: A source book for information and communication technologies & cyber law in Tanzania & East African community*. African Books Collective, 2010.

3. Sahoo, Ms Deepali Rani, and Pooja Kapoor. "An Analytical Study Relating to the Legal Dimensions against Cyberviolence in India." *Computers in Human Behavior* 25.5: 1089- 1101.

4. Sarmah, Animesh, Roshmi Sarmah, and Amlan Jyoti Baruah. "A brief study on cyber crime and cyber laws of India." *International Research Journal of Engineering and Technology (IRJET)* 4.6 (2017): 1633-1640.

5. Brenner, Susan W. "US cybercrime law: Defining offenses." *Information Systems Frontiers* 6.2 (2004): 115.

6. Karnika Seth, Computer, internet and new technology laws, (2016), Lexis Nexis, New Delhi.

7. Castañeda, J. Alberto, Francisco J. Montoso, and Teodoro Luque. & quot;The dimensionality of

8. Customer privacy concerns on the internet.& quot; Online Information Review (2007). 9. Shilpa Dongre (2015), Cyberlaw and its applications, Current Publication, Mumbai.

10. https://www.thelawcodes.com/cyber-crime-social-media-and- information-technology act/

11. https://economictimes.indiatimes.com/definition/socialmedia

12. Https://pib.gov.in/pressreleaseiframepage.aspx?PRID=2003158

13. Https://m.economictimes.com/news/india/cyber-crime-growing-at-the-rate-15-20-annually-in-india-west-bengal-igp-cyber-cell/articleshow/106030543.cms

14. A literature review of social media capabilities for counter-terrorism "*by Jamie Bartlett and Carl Miller November 2013*"

15. Child sexual abuse and the internet—a systematic review "*by Sana Ali, Hiba Abou Haykal, Enaam Youssef, Mohammed Youssef 2023*"

16. Social media, students, and the law "*by Martha McCarthy October 2021*"

17. Historicizing internet regulation in china: a meta-analysis of Chinese Internet Policies "*by Weishan Miao, Min Jiang, and Yunxia Pang 2021*"