IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

OPEN ACCESS

Volume: 4

Issue: 3

Month: July

Year: 2025

ISSN: 2583-7117

Published: 18.07.2025

Citation:

P. Santhosh kumar, Dr. Yogesh Wamankar "International Cooperation In Cybercrime Investigations: India's Legal Readiness" International Journal of Innovations in Science Engineering and Management, vol. 4, no. 3, 2025, pp. 123–130.

DOI:

10.69968/ijisem.2025v4i3123-130

International Cooperation In Cybercrime Investigations: India's Legal Readiness

P. Santhosh kumar[1], Dr. Yogesh Wamankar[2]

[1]*Research scholar, Department of Law, Mansarovar Global University M.P.*
[2]*Associate professor, Department of law, Mansarovar Global University M.P.*

Abstract

This research critically examines the inadequacies of India's current legal framework in addressing the rising threat of cybercrime, particularly under the Information Technology Act, 2000. Through in-depth case studies such as the Cosmos Bank cyber heist and the Bulli Bai/Sulli Deals incidents, it reveals systemic flaws in legislation, investigation, and enforcement. A comparative analysis with global cybercrime frameworks specifically those of the United States, United Kingdom, and Singapore underscores the need for India to modernize its laws, enhance cyber forensic capabilities, and foster international cooperation. The study advocates for the enactment of comprehensive cybercrime legislation, establishment of specialized cybercrime units, and increased training for law enforcement and judiciary. Emphasizing public awareness and digital literacy as foundational elements of cyber resilience, the paper concludes that India must adopt a proactive, future-ready approach to protect its digital infrastructure and ensure justice in the cyber age.

Keywords; Cybercrime, Legal Reform, Digital Forensics, International Cooperation, Cyber security.

INTRODUCTION

In the rapidly evolving digital era, the proliferation of internet usage, mobile technology, and digital services has transformed the way individuals, businesses, and governments operate (Chen, 2021). However, this technological advancement has also brought with it a surge in cyber threats, giving rise to a new category of crime cybercrime. Broadly defined, cybercrime refers to criminal activities that involve a computer, networked device, or a digital network. These offenses can range from data breaches, identity theft, and financial fraud to cyber stalking, online harassment, ransom ware attacks, and even cyber terrorism (Goni, 2022). The scope of cybercrime is vast, as it cuts across geographical boundaries and targets individuals, corporations, and state institutions alike.

As we continue to integrate digital tools into every facet of life, cyber security the practice of protecting systems, networks, and programs from digital attacks has become a crucial pillar of national security and economic resilience. In a country like India, which is one of the fastest-growing digital economies in the world, ensuring robust cyber security is not just a technological challenge but also a legal and policy imperative (George, 2023). The rising dependence on digital platforms for banking, governance, education, and communication has significantly widened the attack surface for cybercriminals.

India has witnessed a sharp increase in cybercrime cases over the past decade. According to the National Crime Records Bureau (NCRB), cybercrime cases in India have grown exponentially, with thousands of new complaints registered each year (Kumar, 2021). From high-profile attacks like the Cosmos Bank cyber heist to widespread incidents of online financial scams, fake job portals, and sex-tortion cases, the threat landscape is constantly expanding in complexity and scale. Despite this alarming rise, the legal and investigative mechanisms in place have struggled to match the sophistication and anonymity of cyber offenses.

This research paper aims to critically examine the current legal framework governing cybercrime in India, with a focus on the Information Technology Act, 2000, and related provisions under the Indian Penal Code. It seeks to identify the systemic gaps that hinder effective prevention, investigation, and prosecution of cyber offenses. Additionally, the study explores the need for capacity-building among law enforcement agencies, improved digital forensic capabilities, and stronger international cooperation mechanisms.

The central hypothesis guiding this research is that India's existing cyber laws and enforcement strategies are outdated and insufficient to tackle the challenges posed by today's digital threats. The study contends that urgent legal reforms, specialized training for law enforcement and investment in modern forensic infrastructure are essential to uphold justice and protect citizens in cyberspace. By addressing these gaps, the paper hopes to contribute to the policy discourse on creating a safer and more secure digital ecosystem in India.

Research Hypothesis

The hypotheses of this research are listed below,

- This situation demands urgent reforms in India's legal framework, specialized training for law enforcement, and the establishment of modern forensic capabilities to ensure justice in cybercrime cases.
- The current legal framework in India, including the Information Technology Act, 2000, is inadequate to fully address the evolving and sophisticated nature of cybercrimes.

Research Methodology and Limitations

This research adopts a qualitative approach to explore the complexities of India's cybercrime legal framework and enforcement challenges. A qualitative methodology is suitable for this study as it allows an in-depth understanding of the legal, procedural, and practical issues surrounding cybercrime through analysis of texts and case studies, rather than numerical data alone.

A primary method used in this research is case study analysis, which involves a detailed examination of significant cybercrime incidents in India. These case studies provide insights into how the existing legal provisions and enforcement mechanisms respond to cyber offenses in real-world scenarios. Through this, the study identifies practical gaps and challenges that are often overlooked in purely theoretical discussions.

The study also relies extensively on secondary data sources, including government reports, judicial decisions, legislative documents, and credible news articles. These sources provide a comprehensive backdrop for assessing the evolution, scope, and effectiveness of India's cybercrime laws and enforcement practices.

Despite its strengths, the study has certain limitations. Being qualitative in nature, the findings may not be generalizable across all types of cybercrimes or geographic regions within India. The reliance on secondary data means the research is constrained by the accuracy and completeness of publicly available information. Moreover, some recent cases or ongoing investigations may not be fully accessible, limiting the ability to analyze the latest trends in detail. Finally, the fast-evolving nature of cybercrime and technology means that the legal and technological context may change rapidly, potentially affecting the study's relevance over time.

Acknowledging these limitations, the research nonetheless provides valuable insights into India's cybercrime legal landscape and highlights areas requiring urgent attention.

OVERVIEW OF CYBERCRIME IN INDIA

With the rapid expansion of internet access and digital services across India, cybercrime has emerged as a significant and growing threat to individuals, businesses, and the government (Naha, 2022). Cybercrime encompasses a wide range of illegal activities conducted through or targeting digital systems. Understanding the types, trends, and impacts of cybercrime in India is crucial for framing effective legal and policy responses.

Types of Cybercrimes Prevalent in India

India faces a diverse spectrum of cybercrimes, each with varying degrees of sophistication and impact. Some of the most common types include:

Cyber Fraud: One of the most widespread cyber offenses, cyber fraud involves deceptive practices like phishing, fake online banking websites, and fraudulent e-commerce platforms. These scams often trick victims into revealing sensitive financial information or transferring money to criminals (Ali, 2024).

Identity Theft: Criminals steal personal information such as Aadhaar numbers, PAN cards, or banking credentials to commit unauthorized transactions, open fake accounts, or carry out other illegal activities.

Hacking: Unauthorized access to computer systems and networks is a growing concern, especially targeting government databases, private enterprises, and critical infrastructure. Incidents range from data breaches to ransom ware attacks (Lehto, 2022).

Ransom ware Attacks: These attacks encrypt victims' data and demand ransom payments to restore access. Both private organizations and public institutions in India have faced increasing ransom ware threats, causing operational paralysis and financial losses.

Cyber stalking and Online Harassment: The rise of social media has led to a surge in cyber stalking, trolling, and harassment, disproportionately affecting women and vulnerable groups. These offenses often involve threats, defamation, and invasion of privacy (Chatterjee, 2023).

Trends and Statistics

According to data from the National Crime Records Bureau (NCRB), cybercrime cases in India have shown a consistent upward trend over the last decade (Kumar, 2021). In 2012, around 6,000 cases were reported; by 2022, this number had surged to over 60,000 annually a tenfold increase. The sharp rise reflects not only the growing use of digital platforms but also increased awareness and reporting.

The Indian Computer Emergency Response Team (CERT-IN) reports further highlight the rising volume and complexity of cyber incidents (Sarowa, 2022). CERT-IN's annual reports indicate a steady increase in cyber incidents such as malware infections, website defacements, and ransom ware attacks targeting both government and private sectors. Financial fraud, data breaches, and unauthorized network intrusions top the list of reported cyber threats.

Geographic and Demographic Spread

Cybercrime in India is not limited to metropolitan hubs; it has permeated urban, semi-urban, and even rural areas due to the expansion of affordable internet connectivity under initiatives like Digital India. However, the highest concentration of cybercrime cases remains in major cities such as Mumbai, Delhi, Bangalore, and Hyderabad, which have dense populations of internet users and commercial activities.

Demographically, young adults (ages 18-35) are both the most frequent users of digital platforms and, consequently, the most common victims of cybercrime (Dubey, 2023). Women, children, and senior citizens are particularly vulnerable to specific cyber offenses such as online harassment, cyber bullying, and financial scams. The diversity in victims necessitates targeted awareness and protection measures.

Economic and Social Impact

The economic impact of cybercrime on India is substantial. The losses due to cyber fraud and data breaches run into billions of dollars annually, affecting individuals, corporations, and government agencies. Small and medium enterprises (SMEs) suffer disproportionately due to their limited cyber security infrastructure and resources (Chidukwani, 2022). The damage also includes costs related to system recovery, legal penalties, and reputation loss.

Socially, cybercrime erodes trust in digital platforms and online governance. Cyber harassment and stalking contribute to psychological trauma and social alienation, especially among women and marginalized groups. Furthermore, cybercrime threatens national security by exposing critical infrastructure and sensitive government data to malicious actors, including foreign entities.

LEGAL FRAMEWORK GOVERNING CYBERCRIME IN INDIA

India's legal framework addressing cybercrime is primarily built around the Information Technology Act, 2000 (IT Act) and relevant provisions of the Indian Penal Code (IPC). While these laws provide a foundational structure for combating cyber offenses, rapid technological advancements and the increasing complexity of cybercrime have exposed significant gaps and limitations in the current system.

The Information Technology Act, 2000: Structure and Scope

The IT Act was India's first comprehensive legislation aimed at regulating electronic commerce and securing digital communication. It provides legal recognition to electronic records and digital signatures, enabling e-governance and electronic transactions to function smoothly. Over time, the Act was amended most notably in 2008 to include provisions specifically targeting cybercrime and to align with evolving global cyber norms.

The IT Act addresses offenses ranging from hacking, data theft, identity fraud, to obscenity published in electronic form (Madhusudan, 2024). It also empowers authorities to intercept, monitor, or decrypt digital communication in the interest of national security or investigation. Despite its pioneering status, the Act's language and definitions often fail to keep pace with emerging cyber threats.

Key Provisions of the IT Act

Several sections of the IT Act are critical in criminalizing cyber offenses (Mukherjee, 2021):

Section 66: Addresses hacking and wrongful use of computers, defining unauthorized access, damage to computer systems, and tampering with data as punishable offenses. This section forms the backbone for prosecuting many cyber intrusions.

Section 66A (Struck down): Previously criminalized sending offensive messages online but was struck down by the Supreme Court in 2015 for being vague and overly broad.

Section 67: Penalizes the publication or transmission of obscene material in electronic form, covering offenses related to cyber pornography and online obscenity.

Section 69: Grants government agencies the power to intercept and decrypt electronic communications during investigations or for national security, although this power requires procedural safeguards.

Section 72: Protects personal data from unauthorized disclosure by a person in a position of trust, making data breaches punishable.

Despite these provisions, some sections suffer from vague wording, leading to enforcement challenges and judicial inconsistencies.

Relevant Provisions under the Indian Penal Code

The IPC supplements the IT Act by criminalizing offenses that have cyber variants or manifestations. Some key sections include:

Section 419 & 420: Related to cheating and fraud, these sections are often invoked in cases involving online scams and financial fraud conducted through digital platforms.

Section 463, 464, 465: Deal with forgery and falsification of documents, applicable to cyber forgeries such as tampered digital records or fake electronic documents.

Section 499 & 500: Address defamation, increasingly relevant with the rise of online harassment and cyber bullying.

Section 354D: Criminalizes stalking, including cyber stalking.

Section 506: Pertains to criminal intimidation, which extends to threats delivered via electronic means.

The IPC's applicability to cyber offenses depends on judicial interpretation, but it lacks specific cyber-related definitions, leading to challenges in prosecution (Akhter, 2022).

Overlaps and Jurisdictional Challenges

One of the major hurdles in India's cybercrime legal landscape is the overlap between the IT Act and IPC provisions, which sometimes causes confusion over which statute applies to a particular offense. This overlap complicates the charging process and can lead to inconsistent judicial outcomes.

Moreover, cybercrimes often transcend state and national borders, creating jurisdictional challenges. Indian law enforcement agencies frequently struggle with determining jurisdiction, especially when cyber offenses involve perpetrators or servers located abroad (Atrey, 2023). While mutual legal assistance treaties (MLATs) exist, delays and procedural hurdles often hamper cross-border cooperation.

Critique of the Current Framework

Despite these laws, India's cybercrime legal framework faces significant criticism:

Outdated Definitions: Many provisions in the IT Act and IPC were drafted before the explosion of social media, crypto currency, ransom ware, and advanced cyber-espionage techniques. This has resulted in a legal framework that does not adequately capture the nuances of modern cyber offenses.

Weak Enforcement: Law enforcement agencies often lack adequate technical expertise and resources to investigate cybercrimes effectively (Grochmal, 2025). Digital forensics capabilities remain underdeveloped, and police training on cyber laws is inconsistent across states.

Slow Judicial Process: Cybercrime cases tend to get delayed due to lack of specialized cyber courts or trained judges. This contributes to low conviction rates and emboldens cybercriminals.

Inadequate Victim Protection: There is limited legal focus on victim support mechanisms, including data privacy protections and timely relief, which undermines public confidence in the justice system.

Absence of Comprehensive Data Protection Law: The lack of a robust personal data protection regime exacerbates the risks of identity theft, data breaches, and misuse of digital information (Sule, 2021).

While the Information Technology Act, 2000, and the Indian Penal Code provide a foundation for tackling cybercrime, the fast-evolving digital landscape demands urgent reforms. To effectively address cyber threats, India must update its legal definitions, streamline jurisdictional issues, invest in law enforcement training and forensic infrastructure, and establish stronger victim protection frameworks. Without these measures, the country risks remaining vulnerable to increasingly sophisticated cybercriminals.

CASE STUDIES SUPPORTING THE HYPOTHESIS

The following case studies highlight the legal, investigative, and enforcement challenges faced by Indian authorities and reinforce the urgent need for reforms in legislation, policing, and digital forensics.

Cosmos Bank Cyber Heist (2018)

One of the most high-profile cyber attacks in India, the Cosmos Bank cyber heist, occurred in August 2018 and involved the theft of approximately Rs.94 crore. Hackers infiltrated the bank's ATM switch server using sophisticated malware, enabling them to clone debit cards. Over 12,000 unauthorized transactions were conducted across 28 countries in a coordinated operation that lasted merely seven hours. Additionally, around Rs.13.92 crore was siphoned off using the SWIFT international financial messaging system, transferred to an entity in Hong Kong (Deshpande, 2022).

The magnitude and precision of the operation suggested involvement by an international cybercriminal syndicate, possibly backed by state actors. While the Maharashtra Cyber Cell and other agencies managed to arrest and convict 11 individuals involved in the local execution of the attack, the masterminds behind the transnational component remain unidentified and un-apprehended. The case illustrates multiple systemic challenges: weak cyber security protocols in financial institutions, poor coordination between international enforcement bodies, and a lack of preparedness in Indian cyber law enforcement to handle cross-border digital crime.

This case underscores the jurisdictional limitations, inadequate international legal cooperation mechanisms, and absence of cyber-specific investigative capabilities that plague India's current cybercrime enforcement framework.

Bulli Bai and Sulli Deals Cases (2021–2022)

In July 2021, the "Sulli Deals" app was launched on GitHub, showcasing over 100 Muslim women including journalists, scholars, and human rights activists as "deals of the day," using their stolen and doctored photographs (Mishra, 2021). In January 2022, a similar app named "Bulli Bai" repeated the offense, targeting the same demographic with a similarly hateful and misogynistic agenda.

These apps were not commercial platforms, but tools of digital harassment, hate speech, and communal targeting. The perpetrators operated under anonymous identities, leveraging encrypted networks and platforms based outside India to avoid detection. The incidents sparked nationwide outrage and condemnation from civil society and political leaders.

Despite the public pressure, law enforcement agencies took several weeks to trace and arrest the individuals involved, who turned out to be young, tech-savvy individuals with little prior criminal history. The delay in action, combined with the lack of specific legal provisions to prosecute such digitally nuanced crimes, drew widespread criticism.

These incidents exposed several critical gaps:

- Absence of targeted laws to handle gendered cyber harassment and hate speech in digital spaces.
- Slow and reactive investigation, often hindered by insufficient digital forensic capabilities.
- Lack of coordination between state cyber cells and central agencies.
- Inadequate victim protection mechanisms and minimal recourse for those affected.

These cases reaffirm the necessity for a revised legal framework that reflects the realities of internet-based hate crimes and provides faster, victim-sensitive legal remedies.

Conclusion of Case Studies

The Cosmos Bank heist highlights the technical and jurisdictional vulnerabilities in India's approach to cyber financial crimes, while the Bulli Bai and Sulli Deals cases shed light on socially targeted cyber offenses and the limitations of India's legal apparatus in tackling gendered and communal cyber abuse. Together, these examples demonstrate how cybercrime in India is outpacing the capabilities of the current legal and investigative frameworks.

These real-world incidents validate the research hypothesis: India's legal response to cybercrime is outdated, inadequately enforced, and ill-equipped to handle complex, high-tech, and transnational threats. There is a pressing need for comprehensive reform, institutional capacity-building and legislative modernization to ensure justice in the digital age.

COMPARATIVE ANALYSIS WITH GLOBAL FRAMEWORKS

In the face of growing cyber threats, countries worldwide have developed comprehensive legal and institutional mechanisms to detect, prevent, and prosecute cybercrimes. A comparative analysis of cybercrime frameworks in the United States, United Kingdom, and Singapore reveals key strategies and practices that India can adopt to strengthen its own cyber defence infrastructure.

1. United States

The United States has established one of the most sophisticated and layered cybercrime legal frameworks in the world. The Computer Fraud and Abuse Act (CFAA), enacted in 1986 and periodically amended, criminalize unauthorized access to computer systems and the transmission of malicious code. It is complemented by other statutes such as the Electronic Communications Privacy Act (ECPA), which governs surveillance and access to electronic communications.

The Federal Bureau of Investigation (FBI) plays a central role in cybercrime enforcement through its Cyber Division, which works closely with federal, state, and international partners. The FBI also collaborates with the private sector under initiatives like InfraGard and the Internet Crime Complaint Center (IC3) to facilitate public reporting and response to cyber incidents (Choi, 2023).

2. United Kingdom

The UK addresses cybercrime through the Computer Misuse Act 1990, which criminalizes unauthorized access to computer material, denial-of-service attacks, and other malicious cyber activities. The National Crime Agency (NCA), through its National Cyber Crime Unit (NCCU), is tasked with combating serious cyber threats.

The UK also places strong emphasis on international cooperation. As a member of Europol's European Cybercrime Centre (EC3) and INTERPOL, the UK engages in coordinated operations and intelligence sharing. The UK also participates in cyber security drills and cyber diplomacy, ensuring a proactive and collaborative stance on cybercrime.

3. Singapore

Singapore has emerged as a cyber security leader in Asia through the Cyber security Act 2018, which provides legal authority for the protection of critical information infrastructure and mandates incident reporting. The Cyber Security Agency of Singapore (CSA) leads the nation's cyber security efforts, including public awareness campaigns, policy-making, and capacity building (Smith, 2022).

Singapore emphasizes a multi-stakeholder approach, bringing together the government, private sector, and academia to strengthen cyber resilience. Its forward-looking policies, such as mandatory risk assessments and a national incident response framework, offer a model for balancing regulation with innovation.

4. Lessons for India

India can draw several key lessons from these global frameworks:

Enactment of Comprehensive Legislation: While India relies primarily on the IT Act, 2000, a more holistic and updated cybercrime law is needed, akin to Singapore's Cyber security Act or the CFAA in the U.S., to address contemporary digital threats such as ransom ware, AI-generated misinformation, and cyber espionage.

Creation of Specialized Cybercrime Units: Establishing dedicated, well-funded cybercrime units with advanced technical training, similar to the FBI's Cyber Division or the UK's NCCU, would improve investigative capacity and reduce reliance on under-resourced state police forces.

International Cooperation: India's engagement with international conventions, such as the Budapest Convention on Cybercrime, remains limited. Expanding bilateral and multilateral cooperation for cross-border data sharing and prosecution is critical to tackling transnational cyber threats (Buçaj, 2025).

Public-Private Partnerships: Like Singapore, India can strengthen cybersecurity by encouraging collaboration between government agencies and private companies, particularly in sectors like banking, telecom, and critical infrastructure.

The experiences of the U.S., UK, and Singapore illustrate that a strong legal framework, international engagement, specialized enforcement, and cross-sector collaboration are central to addressing cybercrime effectively. India, as a rapidly digitizing economy, must integrate these lessons to build a future-ready cybercrime response mechanism.

THE WAY FORWARD: RECOMMENDATIONS FOR REFORM

To effectively address the escalating threat of cybercrime, India must adopt a multidimensional strategy that includes legal, institutional, and societal reforms. Based on the analysis presented, the following key recommendations are proposed:

Drafting a Comprehensive Cybercrime Law: India requires a new, holistic law that goes beyond the outdated Information Technology Act, 2000. This legislation should clearly define emerging offenses such as ransom ware attacks, cyber bullying, doxxing, phishing, crypto currency fraud, and AI-driven crimes (Ganguli, 2024). The law must provide robust provisions for victim protection, data privacy, and legal remedies.

Modernizing the IT Act: Until a new law is enacted, the IT Act must be amended to incorporate current technological realities. This includes revising obsolete definitions, clarifying penalties, and aligning it with international standards like the Budapest Convention.

Establishing Dedicated Cybercrime Units: There is an urgent need to set up specialized cybercrime cells in every district, staffed with trained personnel and equipped with the latest digital forensic tools. A decentralized structure will ensure faster and more efficient investigation of local cases.

Cyber Training for Law Enforcement and Judiciary: Mandatory, continuous cybercrime training should be institutionalized for police officers, judges, and public prosecutors to bridge the digital knowledge gap and improve prosecution and adjudication of cases (Martin, 2022).

Enhancing Forensic Capabilities: Investments in digital forensic labs, tools, and personnel are essential. Central and state governments must allocate adequate funds to expand forensic infrastructure and reduce investigation backlogs.

International Collaboration: India should enter into more data-sharing treaties, enhance participation in global cybercrime conventions, and establish protocols for transnational cooperation (Callanan, 2022).

Public Awareness and Digital Literacy: Government and private stakeholders must collaborate on nationwide campaigns promoting cyber hygiene, awareness, and digital literacy to empower citizens and reduce victimization.

CONCLUSION

This research began with the hypothesis that India's current legal framework, including the Information Technology Act, 2000, is inadequate to address the complex, evolving nature of cybercrimes. Through an examination of real-world cases, comparative global practices, and legal analysis, the findings clearly support this hypothesis. Cybercrime in India has grown not only in frequency but in sophistication, while the country's legal and investigative apparatus has struggled to keep pace.

The urgent need for reform is evident. Existing laws are outdated and poorly equipped to deal with contemporary threats such as ransom ware, identity theft, cyber stalking, and digital hate crimes. Investigative agencies often lack both the technological expertise and institutional support required to prosecute cyber offenses effectively. Delayed responses and underwhelming conviction rates further weaken public trust in the justice system when it comes to digital crimes.

Addressing this growing crisis requires more than piecemeal adjustments. It calls for a coordinated political, administrative, and societal effort. Lawmakers must prioritize the drafting of comprehensive cybercrime legislation. Government agencies should receive the resources and training needed to enhance cyber policing and forensic investigation. Simultaneously, citizens must be educated on digital safety and cyber awareness to prevent victimization and promote responsible digital behaviour.

Looking ahead, India's position as a global digital powerhouse hinges on its ability to create a secure cyber ecosystem. Reforms must be future-ready, grounded in international best practices, and adaptable to rapid technological changes. Only through a robust, forward-looking, and inclusive framework can India ensure justice, protect its digital economy, and uphold the fundamental rights of its citizens in the cyber age.

REFERENCES

[1] Akhter, F. (2022). Department of Law. *Doctoral dissertation, Department of Law, University of Dhaka* .

[2] Ali, M. a. (2024). Phishing—A cyber fraud: The types, implications and governance. *International Journal of Educational Reform, 33(1)* , pp.101-121.

[3] Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews* .

[4] Buçaj, E. a. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews, 8(1)* , pp.2025024-2025024.

[5] Callanan, C. C. (2022). Enhancing global cybersecurity cooperation: European and Indian perspectives. *Observer Research Foundation (ORF)* , pp.1-29.

[6] Chatterjee, S. (2023). Cybercrime against Women with Special Emphasis on Cyberbullying, Sextortion and Right to Privacy. *Issue 2 Indian JL & Legal Rsch., 5* , p.1.

[7] Chen, C. L. (2021). Role of government to enhance digital transformation in small service business. *Sustainability, 13(3)* , p.1028.

[8] Chidukwani, A. Z. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEe Access, 10* , pp.85701-85719.

[9] Choi, J. a. (2023). Techno-crime prevention: the role of the private sector and its partnerships with the public sector. *In Handbook on Crime and Technology. Edward Elgar Publishing.* , pp. 359-374.

[10] Deshpande, K. D. (2022). Cyberattack at cosmos bank: Regaining customer trust. *SAGE Publications: SAGE Business Cases Originals* .

[11] Dubey, P. a. (2023). Social Media and Cybercrime: A Sociodemographic Study of Awareness Level Among Indian Youth. *In Cybercrime in Social Media. Chapman and Hall/CRC* , pp. 23-40.

[12] Ganguli, P. (2024). The Rise of Cybercrime-as-a-Service: Implications and Countermeasures. *Available at SSRN 4959188* .

[13] George, A. (2023). Evaluating India's economic growth: challenges and opportunities on the path to 5 trillion dollars. *Partners Universal International Innovation Journal, 1(6)* , pp.85-109.

[14] Goni, O. (2022). Cyber crime and its classification. *Int. J. of Electronics Engineering and Applications, 10(1)* , p.17.

[15] Grochmal, A. (2025). Challenges Faced by Law Enforcement Collecting and Using Digital Evidence in Cybercrime Investigations. *Doctoral dissertation, Marymount University* .

[16] Kumar, S. a. (2021). Cyber crimes in India: Trends and Prevention. *GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ) ISSN (E), 9(5)* , pp.2347-6915.

[17] Lehto, M. (2022). Cyber-attacks against critical infrastructure. *In Cyber security: Critical infrastructure protection. Cham: Springer International Publishing* , pp. 3-42.

[18] Madhusudan, V. (2024). A Critical Analysis of Information Technology Act, 2000 with Reference to Cyber Offence and Cyber Security. *Issue 2 Int'l JL Mgmt. & Human., 7* , p.2529.

[19] Martin, E. (2022). The Evolving Challenges, Issues of Cybercrime, Law Enforcement Personnel, Preparedness, and Training. *Doctoral dissertation, Walden University* .

[20] Mishra, S. (2021). Cyberbullying of Women. *Jus Corpus LJ, 2* , p.627.

[21] Mukherjee, I. (2021). A Critical Analysis of Section 67 of the Information Technology Act, 2000. *Indian JL & Legal Rsch., 3* , p.1.

[22] Naha, A. (2022). Emerging cyber security threats: India's concerns and options. *International Journal of Politics and Security, 4(1)* , pp.170-200.

[23] Sarowa, S. B. (2022). Analysis of Cyber Attacks and Cyber Incident Patterns over APCERT Member Countries. *In 2022 4th International Conference on Artificial Intelligence and Speech Technology (AIST)* (pp. pp. 1-6). IEEE.

[24] Smith, J. (2022). Sheltering from cyber insecurity? A comparative analysis of New Zealand and Singapore. *Doctoral dissertation, The University of Waikato* .

[25] Sule, M. Z. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technology in Society, 67* , p.101734.