AN ANALYSIS OF THE ADMISSIBILITY OF DIGITAL EVIDENCE AND ITS CHALLENGES IN THE AGE OF CYBERCRIME UNDER THE INDIAN LEGAL REGIME

Aswathi P.M., LL.M., Department of Criminal Law, School of Excellence in Law,
The Tamilnadu Dr. Ambedkar Law University, Chennai.

ABSTRACT

This article critically examines the evolving landscape of cybercrime investigations in India, with a particular focus on recent legislative reforms and technological advancements. It underscores the growing inadequacy of conventional investigative approaches in addressing complex cyber offences that often operate across borders and involve transient forms of digital evidence such as deepfakes, encrypted communications, and manipulated data. The Bharatiya Sakshya Adhiniyam, 2023 (BSA) marks a significant shift in evidentiary law by expanding the scope and admissibility of electronic records, while the Bharatiya Nagarik Suraksha Adhiniyam, 2023 (BNSS) introduces procedural innovations including online reporting mechanisms, digital recording of statements, clearer jurisdictional guidelines, and compulsory forensic examination in certain cases. The study also explores the dual role of Artificial Intelligence (AI) in the cyber domain, both as a tool exploited by offenders and as a powerful asset for investigators. At the same time, concerns relating to algorithmic bias, accountability, and ethical use remain significant. The paper emphasizes that strengthening cybercrime response requires not only legal reform but also sustained investment in capacity building, technological integration, public awareness, and international collaboration. The article underscores the importance of capacity building, investment in technological resources, public awareness initiatives, and enhanced international cooperation to effectively combat cyber threats. In conclusion, while the introduction of the BSA and BNSS marks a significant step toward modernizing India's legal and procedural framework, their success ultimately depends on a holistic and integrated approach.

Keywords: Cybercrime investigation, digital evidence, artificial intelligence, Bharatiya Nagarik Suraksha Adhiniyam 2023, Bharatiya Sakshya Adhiniyam 2023, India.

I. INTRODUCTION:

In the contemporary legal landscape, the rapid evolution of the digital world has transformed cybercrime from a peripheral technical concern into a formidable, multi-dimensional threat that transcends geographical boundaries, setting it apart from traditional physical offenses through its use of technology as both a sophisticated weapon and a high-value target. As global society shifts toward an era of total digital dependency, electronic evidence has transitioned into the "silent witness" of modern litigation, providing the objective, granular, and chronological narrative—such as IP logs, system registries, and metadata—necessary to bridge the gap between invisible virtual acts and tangible courtroom convictions. This study's literature review observes a steep upward trajectory in cyber-offenses and a critical need for technical sophistication among legal practitioners to match that of modern offenders who operate in the vacuum of encrypted servers. While existing scholarship from authorities like Karnika Seth and Dr. Prashant Mali has laid the foundational groundwork for understanding cyber laws, there remains a notable and urgent research gap concerning the practical, real-time application of the newly enacted Bharatiya Sakshya Adhiniyam (BSA), 2023, and the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023. Specifically, the discourse lacks a comprehensive analysis of the transition of digital records to "primary evidence" status and how this shift affects the burden of proof in high-stakes cyber trials. Using a doctrinal research methodology that scrutinizes statutory provisions, landmark judicial precedents such as *Anvar P.V. v. P.K. Basheer*, and the latest 2025–2026 threat reports, this paper seeks to address the "forensic gap" where investigators and the judiciary must now navigate a "zero-trust" environment to ensure evidence integrity through rigorous cryptographic hashing and chain-of-custody protocols. The need for this study is underscored by the systemic shift from the lenient standards seen in earlier cases like *Navjot Sandhu* to the strict technical compliance mandated by current laws. Furthermore, the significance of this study lies in its exploration of how the BSA and BNSS move away from traditional paper-based constraints to create a tech-enabled criminal justice system that is agile enough to monitor volatile data, while remains balanced against the fundamental right to privacy and liberty enshrined in Article 21 and reinforced by the *Justice K.S. Puttaswamy* judgment. The academic contribution of this work is to provide a roadmap for interpreting the interplay between technological advancement and human rights within the Indian judicial framework. Ultimately, the aim and objectives of this study are to critically evaluate the efficacy of Section 2(1)(e) and Section 57 of the BSA in validating electronic data, analyze the procedural shifts in digital reporting and mandatory forensic participation under Section 176(3) of the BNSS, and provide a comprehensive framework for staying ahead of emerging threats like AI-

driven phishing, cloud forensics complexities, and the evidentiary challenges posed by blockchain and the Internet of Things.

II. DEFINING DIGITAL EVIDENCE IN THE MODERN LEGAL FRAMEWORK:

Proof is fundamentally established through evidence, which typically consists of records or data pertinent to a specific legal matter. The Information Technology Act of 2008 defines electronic evidence as "Any information with values that is stored or transmitted electronically, and it includes evidence such as computer data, digital audio, digital video, cell phones, and digital fax machines."[1]

The legal structure governing how digital evidence is admitted in court is primarily established under **Section 2(e) of the Bharatiya Sakshya Adhiniyam**. This specific provision serves as the foundational framework for validating electronic data within the Indian judicial system.[2]

Section 32 of the Bharatiya Sakshya Adhiniyam addresses the complexities of electronic evidence when it involves the legal standards or jurisdictions of other nations.

To clarify the evolution of these laws, the following comparison highlights the significant shifts between the previous **Indian Evidence Act of 1872** and the modern **Bharatiya Sakshya Adhiniyam**:

Aspect	Indian Evidence Act, 1872	Bharatiya Sakshya Adhiniyam 2023
Admissibility Standar	Digital evidence was generally categorized as secondary evidence necessitating strict certification under Section 65B.	Elevates it to the status of Prima Evidence under Section 57.
Definition of Primary Evidence	Focused on physical documents submitted for inspection (Section 62).	Modernizes this by including digital records that are created or stored simultaneously as forms o

[1] Information Technology (Amendment) Act, 2008, § 2(1)(t), No. 10, Acts of Parliament, 2009 (India).
[2] Adarsh S., *Digital Evidence Under Bharatiya Sakshya Adhiniyam, 2023: A Procedural Shift*, 14(2) J. Indian L. Inst. 112, 115-118 (2024).

		primary evidence.
Status of Digital Records	Not explicitly grant primary status to electronic data	Explicitly recognizes and trea digital records as primary evidenc
Statutory Detail	Relied on limited and often criticized provisions like Section 65B.	Provides comprehensive a detailed regulations to mana digital evidence effectively.

III. CYBERCRIME AND ITS FORMS:

Cybercrime is an escalating threat in our digital world, defined as any illegal activity involving computers, networks, or connected devices that transcends geographical limits.[3] It takes advantage of digital weaknesses for unlawful purposes or harmful intentions, setting it apart from conventional physical crimes. Recognizing its various forms is crucial for maintaining online security. At its essence, cybercrime employs technology either as a means or a target, ranging from individual fraud to attacks aimed at critical infrastructure, motivated by financial interests, political agendas, espionage, or disruption.

A common manifestation of cybercrime is cyber fraud, which includes tactics like phishing (attempts to steal sensitive information through deception), identity theft (the unauthorized use of personal data), and online scams (fraudulent schemes that exploit trust).[4] Beyond financial misconduct, cybercriminals also compromise data and systems through hacking (unauthorized access aimed at theft or disruption) and malware (such as viruses, worms, ransomware, and spyware that lead to data theft, encryption, or operational hiccups). Ransomware attacks, which demand payment for data restoration, are becoming especially harmful. Furthermore, the digital era has given rise to cyberstalking and online harassment through electronic communication, leading to emotional harm. Disturbingly, social media and messaging applications are often used to facilitate such behaviour.

Cybercrime also impacts intellectual property through online piracy and unauthorized sharing of copyrighted content, resulting in financial losses. The effects of cybercrime are widespread,

[3] U.N. Off. on Drugs and Crime, Comprehensive Study on Cybercrime (2013).
[4] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 90 N.Y.U. L. Rev. 1596, 1602-1605 (2015).

causing people to suffer financial losses, identity theft, reputational harm, and emotional distress.[5] Businesses face monetary losses due to fraud and data breaches, as well as damage to their reputation. Moreover, governments and critical infrastructure are at risk, potentially jeopardizing national security and essential services.

To combat cybercrime effectively, a comprehensive strategy is needed, including individual awareness (recognizing scams, using strong passwords, practicing cautious online behaviour, and regularly updating software), organizational security protocols (such as firewalls, intrusion detection systems, anti-malware software, encryption, audits, access controls, and employee training), and government initiatives (including law-making, establishing specialized agencies, and fostering international collaboration).

The fast-paced advancements in technology, including AI, IoT, and blockchain, pose new cybersecurity challenges.[6] Ongoing research, innovative security technologies, and adaptable legal frameworks are crucial for staying ahead of emerging threats.

IV. ROLE OF DIGITAL EVIDENCE IN PROVING CYBERCRIMES:

The role of digital evidence in the modern legal landscape has transitioned from being a peripheral technicality to becoming the "silent witness" that often dictates the outcome of a trial.[7] In the

[5] Nat'l Crime Records Bureau, Ministry of Home Affairs, Crime in India 2022: Statistics Volume III (2023).
[6] *Integrating Blockchain with Artificial Intelligence for Advanced Cyber Defence*, 12(4) Int'l J. Advanced Cyber Stud. 214, 218-220 (2025).
[7] Adv. (Dr.) Prashant Mali, *Trial of Cyber Offences: Admissibility & Appreciation of Digital Evidence Navigating the Bharatiya Sakshya Adhiniyam (BSA), 2023*, Scribd (2024)

practical world, cybercrime is rarely witnessed by the human eye; it occurs in the vacuum of a network or the silence of an encrypted server. Consequently, digital evidence acts as the bridge between an invisible act and a tangible courtroom conviction. It provides an objective, chronological narrative of a crime ranging from the initial unauthorized login to the final exfiltration of data, that human testimony simply cannot replicate. For instance, while a victim may testify that their funds were stolen, the digital evidence, such as IP logs and blockchain transaction histories, provides the "forensic fingerprint" that connects the suspect's device to the specific moment of the theft.

Legally, the strength of this evidence under the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, lies in its newfound status as primary evidence. This shift acknowledges that a digital record is not just a copy, but a direct manifestation of the act itself.[8] By analyzing metadata, file headers, and system registries, investigators can prove "mens rea" or criminal intent, showing that a perpetrator didn't just accidentally stumble into a restricted database but deliberately bypassed security protocols.[9] However, the legal weight of this evidence is entirely dependent on its integrity; the law demands a "zero-trust" approach where every bit of data must be verified through hash values to ensure it hasn't been altered.[10] Ultimately, in a world where physical evidence can be easily wiped clean, the granular details preserved in digital footprints such as, time-stamps and geolocation data which ensure that the digital truth remains resilient against the sophisticated deceptions of the modern cybercriminal.

V. MODERN TRENDS AND CHALLENGES IN DIGITAL EVIDENCE:

The landscape of cybercrime investigations is rapidly changing in our digital age, embracing new technologies and facing increasing complexities associated with digital evidence.

Current Developments: A notable trend is the increasing use of Artificial Intelligence (AI) and Machine Learning (ML) to sift through large datasets, recognize patterns, and identify harmful activities—such as analyzing network traffic in real-time to detect cyberattacks or efficiently spotting phishing campaigns.[11] Proactive threat intelligence is becoming more critical, leveraging

[8] Bharatiya Sakshya Adhiniyam, 2023, § 57, No. 47, Acts of Parliament, 2023 (India).
[9] Ashish Shahi, *Challenges In Digital Forensics And Cyber Evidence In Indian Courts*, 7(5) Int'l J. L. Legal Rep. 1, 4-6 (2025).
[10] Adarsh S., *Evolution of Electronic Evidence: Navigating the Admissibility of the New Criminal Laws in India*, 4(1) Int'l J. Integrated Legal Res. 18, 22-25 (2025).
[11] *Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges*, 12(1) Herald Scholarly Open Access 1, 4-6 (2025).

open-source intelligence (OSINT) and various resources to foresee and mitigate attacks by understanding the strategies of threat actors. The emergence of cloud computing, mobile devices, and the Internet of Things (IoT) has broadened the scope for potential attacks, introducing new and varied sources of digital evidence that necessitate specialized cloud forensics and data extraction tools. Additionally, collaboration across jurisdictions and between public and private sectors is essential, with organizations like Interpol and Europol playing pivotal roles in fostering international cooperation and partnerships with private cybersecurity firms.[12]

Challenges: However, these trends present major challenges for handling digital evidence. The immense amount and speed of digital data make manual examination unfeasible. The fleeting and unstable nature of certain types of digital evidence—like volatile memory and network logs—demands prompt incident response. Data encryption poses a continual challenge, requiring both legal and technical methods for decryption. Maintaining the integrity and authenticity of evidence is critical, necessitating strong chain of custody practices and cryptographic hashing techniques. Legal and jurisdictional issues arise from varying international laws regarding data privacy and cross-border data transfers.[13] The fast pace of technological advancement consistently brings forward new devices and formats, necessitating ongoing updates to forensic tools and skillsets. Finally, it is vital to strike a balance between the privacy implications of collecting digital evidence and the requirement to investigate crimes, which calls for clear legal and ethical frameworks.

Also, the contemporary challenges recognize the importance of digital evidence is essential in investigating cybercrimes. However, it can also endanger people's privacy rights, which are protected under Article 21 of the Constitution, asserting everyone's right to life and liberty. This was further reinforced in the case of Justice **K.S. Puttaswamy vs. Union of India**[14] **(2018).** There is a possibility that this could be misused to undermine individual rights. Monitoring someone's online activities without their consent constitutes a blatant breach of privacy.

VI. COMPARATIVE ANALYSIS OF ADMISSIBILITY OF DIGITAL EVIDENCE ACROSS NATIONS:

[12] Giulio Calcara, *The Role of INTERPOL and Europol in the Fight Against Cybercrime*, 34(2) Liverpool L. Rev. 115, 118-120 (2013).
[13] N. AllahRakha, *Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations*, 16(2) Pak. J. Criminology 119, 122-125 (2024).
[14] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India)

Nations	Primary Legal framewo	Admissibility Standard	Key Characteristics
India	Bharatiya Sakshya Adhiniyam (BSA), 2023	Primary Evidence	Elevates digital records to "primary" status (Section 57), reducing the strict certification hurdles of the previous regime while emphasizing forensic integrity.
United States	Federal Rules of Evidence (FRE)	Rule 901 & 902	Focuses on "Authentication." Evidenc is admitted if there is sufficient proof that the item is what the proponen claims it to be, often using metadata or "self authenticating" electronic records.
United Kingdom	Police and Criminal Evidence Act (PACE) 198	Section 69 (Repealed) Common Law	After repealing strict computer-specific hurdles the UK now presumes tha a computer was operating correctly unless evidence provided to the contrary.
European Union	eIDAS Regulation & Convention on Cybercrim	Harmonized Standard	Focuses on the "Chain of Custody" and cross borde compatibility. Emphasize the reliability of electroni signatures and time stamp as proof of data integrity.
Singapore	Evidence Act (Cap 97)	Presumption of Integr	Similar to the UK, it employs a "presumption o reliability" for electronic records produced by devices used in the ordina course of business, provided the source is verified.

VII. JUDICIAL PRONOUNCEMENTS ON DIGITAL EVIDENCE:

The evolution of how Indian courts handle digital evidence is marked by a series of landmark judicial shifts, moving from leniency to strict technical compliance and back again. Below is a rephrased analysis of these pivotal cases:

The Judicial Evolution of Electronic Admissibility

State (N.C.T of Delhi) v. Navjot Sandhu (2001)[15] [The Parliament Attack Case] In the high-stakes trial following the terrorist attack on the Indian Parliament, a critical debate arose regarding the use of mobile phone records as evidence.

The defense argued these records were inadmissible because they lacked the mandatory certificate required by Section 65B(4) of the Indian Evidence Act.

However, the Supreme Court took a flexible stance, ruling that electronic documents could be admitted even without this certificate. This verdict effectively relaxed the rules, suggesting that if an original record was unavailable, a copy could still be presented under the general provisions of secondary evidence. While this simplified the prosecution's task, this lenient approach was eventually reconsidered and overruled a decade later.

Anver P.V. v. P.K. Basheer & Ors (2014) This case fundamentally changed the landscape by restoring the mandatory nature of the Section 65B certificate. Arising from an election dispute involving allegations of corruption and the use of recorded CDs and pamphlets, the court had to decide if uncertified digital media could be used to prove a case. The Supreme Court took a firm stand, declaring that Section 65B is a self-contained code. It ruled that electronic records are inadmissible as secondary evidence unless accompanied by the specific statutory certificate.[16] This judgment essentially closed the door on the "relaxed" era of *Navjot Sandhu*, making technical compliance a non-negotiable requirement for digital proof.

Tomaso Bruno & Anr v. State of U.P. (2015) In a case involving the tragic murder of a foreign tourist in Varanasi, the Supreme Court highlighted the dangers of forensic negligence. The court observed that the prosecution had failed to properly present CCTV footage and essential technical documentation during the trial.[17] Interestingly, while the court did not directly reference the *Anvar v. Basheer* precedent, it emphasized that criminal convictions must rest on compelling, beyond-a-reasonable-doubt evidence. Because the digital evidence was mishandled and created significant gaps in the investigation, the court acquitted the accused, reinforcing the principle that the law favors the accused when the integrity of digital evidence is in question.

[15] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 S.C.C. 600 (India)
[16] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
[17] *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 S.C.C. 178 (India).

Shafhi Mahommad v. The State of Himachal Pradesh (2018) This ruling introduced a practical exception to the strict certification rule. The court addressed a common dilemma: what happens when a party wants to submit digital evidence but does not own or have access to the device that created it? The Supreme Court clarified that the requirement for a Section 65B (4) certificate is not meant to be an impossible barrier.

It ruled that if the person providing the evidence is not in possession of the original device, the court can admit the electronic evidence even without a certificate.[18] This provided a necessary balance, ensuring that the search for truth is not stalled by technicalities when a party acts in good faith.

VIII. CONCLUSION AND SUGGESTIONS:

The transition from the traditional Indian Evidence Act of 1872 to the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, marks a historic pivot in how our legal system perceives truth in the digital age. By formally elevating electronic records to the status of **primary evidence**, Parliament has acknowledged that a digital footprint is no longer just a "copy" of a document—it is the document itself. However, as our lives generate more data, the risk of technological abuse and sophisticated criminality grows, making it essential for lawyers, judges, and investigators to move beyond basic legal knowledge and master the technical nuances of digital proof.

Suggestions:

Training Programs and Regulatory Standards

Empowering legal and law enforcement professionals through specialized training is vital for navigating modern digital complexities. By mastering forensic software and investigative techniques, personnel can ensure that gathered evidence is both accurate and resilient under judicial scrutiny. Furthermore, establishing clear, standardized regulations for the collection and storage of digital data is essential to maintain procedural integrity and ensure that forensic tools are used ethically and effectively.

Inter-Departmental Collaboration

Effectively tackling cybercrime requires a unified front between the police, legal counsel, and IT

[18] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).

specialists. This collaborative synergy allows experts from different fields to align on new technologies and courtroom standards, ensuring that evidence is not "lost in translation." By sharing insights into forensic specifics and legal requirements, these teams can overcome technical hurdles and streamline the transition of evidence from the digital crime scene to the trial.

Two-Factor Authentication and System Security

Robust security habits are the first line of defence against unauthorized intrusions. Utilizing strong, unique passwords alongside **Two-Factor Authentication (2FA)**—which adds a second layer of verification via mobile codes—significantly bolsters account safety. Additionally, maintaining a schedule of regular updates for software and operating systems is critical; these patches close security loopholes and provide the latest defences against evolving hacking attempts.

Safeguarding Sensitive and Volatile Data

Protecting data integrity involves both proactive monitoring and strategic recovery plans. Implementing firewalls and Intrusion Detection Systems (IDS) helps control network traffic, while active backup systems ensure data can be restored following an attack. Crucially, investigators must prioritize **volatile evidence**—transient data stored in RAM that vanishes when power is lost. Adhering to the "order of volatility" by collecting the most fragile data first is essential to preserving the digital truth before it is permanently erased.

REFERENCES:

Books & Scholarly Articles

1. Karnika Seth, Computers, Internet and New Technology L aws: A Comprehensive Reference Work with Special Focus on Developments In India (2nd ed. 2016).

2. Adv. (D R.) Prashant Mali, Cyber L Aw & Cyber C Rimes: Simplified for Law Students & Professionals (2024).

3. Adarsh S., *Digital Evidence Under Bharatiya Sakshya Adhiniyam, 2023: A Procedural Shift*, 14(2) J. INDIAN L. INST. 112 (2024) - https://www.google.com/search?q=https://www.ijilr.com/wp-content/uploads/2025/01/EVOLUTION-OF-ELECTRONIC-EVIDENCE-NAVIGATING-THE-ADMISSIBILITY-OF-THE-NEW-CRIMINAL-LAWS-IN-INDIA.pdf

4. G.S. Bajpai & Ankit Kaushik, *The New Code of Criminal Procedure: Evaluating the Bharatiya Nagarik Suraksha Sanhita, 2023*, 58(4) ECON. & POL. WKLY. 14 (2024).

5. Ram Prakash Chaubey, *An Analysis of Digital Evidence and its Role in Proving Cybercrimes*, 7(3) INT'L J. L. 38 (2025) - https://www.lawjournals.net/assets/archives/2025/vol7issue3/7067.pdf

6. Sadhna Gupta & Meghali Das, *Criminal Investigation of Electronic Evidence: Challenges Faced with Digital Forensics*, 2(2) NFSU J. FORENSIC JUST. 1 (2023) - https://jfj.nfsu.ac.in/Uploads/EJournal/2/3/(1-16)%20CRIMINAL%20INVESTIGATION%20OF%20ELECTRONIC%20EVIDENCE%20CHALLENGES%20FACED%20WITH%20DIGITAL%20FORENSICS%20v1.pdf

Statutes & Authorities

1. Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India).

2. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).

3. Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

4. India Const. Art. 21.

5. Convention on Cybercrime (Budapest Convention), Nov. 23, 2001, E.T.S. No. 185.

Cases Referred:

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

2. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

3. *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 S.C.C. 801 (India).

4. *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 S.C.C. 600 (India).

5. *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 S.C.C. 178 (India).

Reports & Online Sources

1. Nat'l Crime Records Bureau, Ministry of Home Affairs, Crime in India 2022: Statistics Volume III (2023) - https://www.google.com/search?q=https://ncrb.gov.in/sites/default/files/CII-2022/CII_2022_Volume%25203.pdf

2. U.N. Off. on Drugs and Crime, Comprehensive Study on Cybercrime (2013) - https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

3. PwC, Annual Threat Dynamics 2026: Cyber Threats in Motion (Apr. 12, 2026) - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/annual-threat-dynamics.html

4. PIB: Curbing Cyber Frauds in Digital India (2025) - https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3

5. PIB: Year End Review-2025: Ministry of Home Affairs - https://www.google.com/search?q=https://www.pib.gov.in/PressReleaseDetail.aspx%3FPRID%3D2219070