Journal for Law & Justice (JLJ)
(Volume I | Issue I 2025)

CYBERCRIME AND THE STATE: ASSESSING THE ROLE OF LAW ENFORCEMENT IN THE DIGITAL AGE

Mohneesh Sersia*

***Abstract**: In the context of the rapid expansion of the digital ecosystem and the global rise in cybercrime, this article conducts a doctrinal and comparative analysis of the role of law enforcement authorities in India. It positions cybercrime as a multifaceted, transnational threat that calls for a departure from traditional police paradigms. The article outlines the legal and operational challenges posed by cybercrime, including jurisdictional ambiguities, technological gaps, and evidentiary vulnerabilities. It distinguishes cyber surveillance from traditional enforcement, focusing on proactive surveillance, digital forensics, inter-agency cooperation, and rights-based investigative mechanisms. The article examines the Information Technology Act, 2000, (IT Act), the Bharatiya Nyaya Sanhita, 2023, (BNS), and the Digital Personal Data Protection Act, 2023, (DPDP Act) assessing their adequacy in empowering Law Enforcement Authorities (LEAs) against sophisticated digital crimes. It analyzes institutional mechanisms such as the Indian Cybercrime Coordination Centre (I4C), the Indian Computer Emergency Response Team (CERT-In), and state-level cyber cells, identifying capacity constraints and recommending reforms. A comparative dialogue with the FBI's Cybercrime Division, INTERPOL's Global Cybercrime Strategy, and Europol's EC3 highlights transferable practices for collaboration. Emphasis is placed on the admissibility of electronic evidence, data sovereignty, and private sector cooperation in enhancing resilience. Ultimately, the article argues that Indian LEAs must be reconceptualized as digitally competent actors with prosecutorial power and improved coordination, capable of upholding national security and individual rights. Legal reform, advanced training, cross-border cooperation, and public accountability are essential elements of a future-proof cyber enforcement regime that embodies digital constitutionalism.*

***Keywords:** Cyber policing, digital evidence, law enforcement authorities, cross-border cybercrime, cybersecurity governance.*

I. INTRODUCTION

In the twenty-first century, the main areas of human interaction, trade, governance, and crime have shifted decisively to the digital sphere. Cyberspace is no longer simply an extension of real-world interactions; it is the world itself, an evolving virtual society without borders, where opportunities and threats are intertwined. Among the biggest emerging threats in this area is cybercrime, which has become one of the most widespread and insidious forms of criminal activity. Whether it's ransomware, phishing, cyberterrorism, or deepfake, the modern criminal does not operate in the shadows but on screens, not with weapons but with code.[1] In this rapidly changing landscape, law enforcement authorities, the traditional bulwark of state power, are grappling with profound structural, legal, technological, and jurisdictional challenges. Cybercrime transcends territorial borders, goes beyond regulatory reforms, and evolves faster than policing models can adapt. As India rapidly digitizes,[2] vulnerabilities inherent in its

* 4th Year Law Student at USLLS, GGSIPU, Delhi, India.

[1] Council of Europe, *Convention on Cybercrime ETS No. 185* (Budapest, 2001) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[2] National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs, Government of India, 2024).

infrastructure, citizens, and governance systems are becoming prime targets for cybercriminals. In 2023 alone, India reported more than 2.2 million cases of cybercrime, but conviction rates remained extremely low.[3]

This article critically discusses the role of law enforcement authorities in the fight against cybercrime in India and beyond. It assesses legislative frameworks such as the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 and institutional responses, including the Cybercrime Coordination Centre, the Indian Computer Emergency Response Team (CERT-In), and cyber police stations, and juxtaposes them with international models such as the Budapest Convention, 2001 and agencies such as Europol's EC3 and INTERPOL's Cybercrime Directorate.[4] The central argument of this article is twofold: first, the current framework of cybercrime surveillance in India is reactive, fragmented, and underfunded; second, a holistic approach encompassing legal reform, transnational cooperation, training, and digital skills development is essential for effective law enforcement. The article proposes structural reforms, legal modernization, capacity building, and a rights-sensitive approach that balances law enforcement and digital privacy.

This article argues that India's law enforcement authorities must be reconceptualized as digitally competent and rights-respecting institutions, empowered through legislative harmonisation, specialised investigative mechanisms, and institutionalised public-private cooperation. Specifically, the article contributes in four ways: first, by analysing the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023; second, by evaluating institutional mechanisms such as the Indian Cybercrime Coordination Centre (I4C), the Indian Computer Emergency Response Team (CERT-In), and state cyber cells; third, by engaging in comparative dialogue with models like the FBI Cybercrime Division, INTERPOL's Global Cybercrime Strategy, and Europol's EC3; and fourth, by recommending structural reforms to strengthen capacity while safeguarding constitutional rights.

II. THE LEGAL FRAMEWORK GOVERNING CYBERCRIME IN INDIA

The legal regulation of cybercrime in India is primarily derived from two main laws: the Information Technology Amendment Act, 2008 and the Bharatiya Nyaya Sanhita, 2023. The former defines the substantive and procedural framework for crimes against digital infrastructure, while latter is invoked to punish traditional crime perpetrated using digital means.

A. Information Technology Act, 2000

The Information Technology Act was India's first legislation dedicated to cybercrime and digital transactions. It defines a range of cybercrimes under Sections 43 to 66F, covering unauthorized access (hacking), identity theft, data breaches, cyberterrorism, and posting obscene material online.[5] Particular importance is given to Section 66F, which criminalizes 'cyberterrorism' and

[3] Lok Sabha Unstarred Question No. 3532, Cybercrime Conviction Rate, https://www.mea.gov.in/lok-sabha.htm?dtl/33642/question+no3532+developmental+assistance/
[4] INTERPOL, *Cybercrime*, https://www.interpol.int/en/Crimes/Cybercrime/
[5] Information Technology Act, No. 21, Acts of Parliament, 2000.

introduces strict sanction mechanisms.[6] Despite its status as a foundational, the law suffers from significant deficiencies. Its language is technologically outdated, does not define emerging threats such as deepfakes or synthetic media, and offers limited clarity for prosecutions. In addition, the lack of procedural synchronization with the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) often leads to confusion in investigations and trials.[7]

B. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita applies at the same time as the Information Technology Act, in particular for offenses related to criminal association [Section 61(2)], deception [section 318(4)], defamation [Section 356(1)], criminal intimidation [Section 351(2) and (3)], and obscenity [Section 294]. While the Bharatiya Nyaya Sanhita offers a broader framework for penalizing online harm, it is not digital legislation and does not reflect the technical nuances required by cybercrime.[8]

III. INSTITUTIONAL MECHANISMS AND LAW ENFORCEMENT AGENCIES

A. The Indian Cybercrime Coordination Centre (I4C)

Launched in 2020 under the aegis of the Ministry of Home Affairs, the Indian Cybercrime Coordination Centre is the supreme coordinating agency to facilitate a comprehensive and coordinated approach to the prevention, investigation, and prosecution of cybercrime. It includes seven key components, including the National Cybercrime Reporting Portal, the Cybercrime Investigation Training Modules, and the National Centre for Cybercrime Research and Innovation.[9] While the Indian Cybercrime Coordination Centre is a commendable move, critics say it lacks legal support, real-time surveillance power, and adequate cybersecurity personnel, especially at the state level.

B. National Cybercrime Units

Most Indian states have established cybercrime cells or cyber police stations. However, these units vary greatly in terms of resources, infrastructure, and expertise. A 2022 audit by the National Bureau of Crime Records (NCRB) found that less than 20% of these cells were staffed with personnel trained in digital forensics.[10]

C. Indian Computer Emergency Response Team (CERT-In) and the National Centre for the Protection of Critical Information Infrastructure (NCIIPC)

The Indian Computer Emergency Response Team (CERT-In) and the National Centre for the Protection of Critical Information Infrastructure (NCIIPC) are specialized agencies responsible for protecting national infrastructure and responding to cyber incidents. While CERT-In is under the Ministry of Electronics and Information Technology, NCIIPC operates under the umbrella of

[6] Cyber Law Committee, *Expert Recommendations on Amendments to the IT Act* (MeitY, 2023) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268#:~:text=Information%20Technology%20(Intermediary%20Guidelines%20and,be%20prosecuted%20under%20section%20111/

[7] Ministry of Home Affairs, *Indian Cybercrime Coordination Centre (I4C)* (2023), https://cybercrime.gov.in/

[8] DSCI, *Cybercrime Training Gaps in State Police* (2022), https://www.dsci.in/events/content/12th-cybercrime-awareness-workshop/

[9] NCRB Report, Cyber Infrastructure Audit (2022), https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf

[10] *Id.*

the National Technical Research Organisation (NTRO). These agencies are primarily focused on cyber threat intelligence and responding to privacy breaches, but they are not investigative agencies *per se*.[11]

IV. CHALLENGES FACED BY LAW ENFORCEMENT IN CYBERCRIME CASES

A. Jurisdictional Complexity and Territorial Ambiguity

One of the main legal challenges is the question of jurisdiction. Cybercrimes often involve cross-border data streams, foreign-based servers, and anonymous perpetrators operating via VPNs or the darknet. In such cases, the traditional notions of territorial jurisdiction in Indian criminal law (Sections 197 and 199 of the BNSS) become inadequate.[12] Mutual legal assistance treaties are often slow, non-transparent, and inadequate to request real-time data.[13]

B. Capacity Shortfalls and Technical Delays

A 2021 report by the Parliamentary Standing Committee on Information Technology highlighted that more than 90% of police personnel had not received formal training on cybercrime.[14] Law enforcement continues to rely heavily on outsourced forensic expertise, leading to delays, compromised chains of evidence, and poor prosecution outcomes.[15]

Digital evidence, especially metadata, IP logs, encryption keys, and timestamps, requires rapid collection and processing. However, police officers at police stations are often ill-equipped to handle cybersecurity complaints, resulting in low FIR registration rates.[16]

C. Legislative Fragmentation and Procedural Gaps

Despite the existence of the Information Technology Act, there remains a procedural disharmony with the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the BNSS, and the BNS. For example, Sections 62 and 63 of the Bharatiya Sakshya Adhiniyam, relating to electronic evidence remain poorly understood and poorly implemented, especially after the landmark decision of the Hon'ble Supreme Court in the case of *Anvar P.V. v. P.K. Basheer.*[17] In addition, while the Digital Personal Data Protection Act, 2023 has since been enacted, its procedural integration is still a developing area, leaving law enforcement agencies without clear procedural safeguards to manage digital privacy.

D. Privacy, Conflicts of Interest, and Excessive Scrutiny

Law enforcement's reliance on mass surveillance tools, such as facial recognition and predictive policing software, has raised concerns among privacy advocates. The Pegasus spyware scandal revealed how state surveillance could evade judicial oversight, in violation of Article 21 of the

[11] Ministry of Electronics and Information Technology (MeitY), *CERT-In Functions*, Notification (April 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
[12] Bharatiya Nagarik Suraksha Sanhita, 2023, § 197-199, No. 46, Act of Parliament, 2023.
[13] Ministry of Foreign Affairs, *Manual of the Mutual Legal Assistance Treaty (MLAT)* (2021) https://legalaffairs.gov.in/documents/mlat/
[14] Standing Committee on Information Technology, *Cyber Surveillance and Capacity Building* (2021) https://sansad.in/getFile/lsscommittee/Communications%20and%20Information%20Technology/18_Communications_and_Information_Technology_5.pdf?source=loksabhadocs/
[15] Comptroller and Auditor General of India, Cyber Crimes, Vol II (2020) https://cag.gov.in/uploads/media/Vol-II-Cyber-Crimes-20200528155403.pdf
[16] *Id.*
[17] Anwar P.V. v. P.K. Bashir, (2014) 10 SC 473.

Constitution.[18] The lack of a legal framework for surveillance mechanisms left agencies operating in legal grey areas, undermining trust in LEAs.

E. Low Conviction Rates and a Lack Of Prosecution

Despite the increase in cybercrime reports, conviction rates remain below 3%.[19] Reasons include poor prosecution, lack of clarity on the admissibility of digital evidence, delays in retrieving data from intermediaries, and insufficient coordination with judicial officials who are unfamiliar with digital concepts.[20]

VI. COMPARATIVE INTERNATIONAL APPROACHES

A. The Budapest Convention on Cybercrime

The Council of Europe Convention on Cybercrime, 2001 also known as the Budapest Convention, remains the only binding international instrument dedicated to cybercrime. It harmonizes national laws, promotes international cooperation, and facilitates criminal investigations into crimes ranging from data interference to content-related crimes.[21] Although India has refused to sign the treaty, citing sovereignty issues,[22] the Convention's procedural and research models have been adopted globally. Article 32 allows cross-border access to data stored with the consent of the legitimate user, while Articles 16 to 21 prescribe expedited protocols for data retention and retrieval. The Convention, therefore, serves as a procedural reference for international cooperation.[23]

B. INTERPOL and Europol

INTERPOL's Cybercrime Directorate serves as a global hub, coordinating 194 member countries for information sharing, operations and the issuance of Purple Cyber Threat Notices.[24] The Directorate's Digital Crime Centre in Singapore has played a key role in dismantling ransomware networks, credit card fraud schemes, and darknet operations.[25] Europol's European Cybercrime Centre (EC3), established in 2013, supports EU states in the fight against organized cybercrime, child exploitation and dark web activities.[26] In particular, EC3's Joint Cybercrime Action Working Group (J-CAT) operates through a multinational liaison model, which builds trust and speed between agencies.[27]

C. United States

In the United States, agencies such as the FBI's Cyber Division, Homeland Security

[18] Pegasus Spyware Case, SC Writ Petition (Civil) No. 314 of 2021.
[19] Law Commission of India, *Report No. 277, Prosecution Failures in Cybercrime Cases* (2023), https://static.pib.gov.in/WriteReadData/userfiles/Report%20No.%20277%20Wrongful%20Prosecution.pdf
[20] *Id.*
[21] Council of Europe, *Explanatory Report on the Convention on Cybercrime* (2001), https://rm.coe.int/16800cce5b#:~:text=The%20Convention%20aims%20principally%20at,well%20as%20other%20offences%20committed/
[22] *Id.*
[23] *Id.*
[24] INTERPOL, *Cybercrime Directorate Annual Report* (2023), https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.interpol.int/content/download/22267/file/
[25] *Id.*
[26] Europol EC3, *Joint Cybercrime Action Group (J-CAT) Overview* (2024), https://www.europol.europa.eu/how-we-work/services-support/joint-cybercrime-action-taskforce/
[27] *Id.*

Investigations (HSI), and the Cybersecurity and Infrastructure Security Agency (CISA) lead enforcement against cybercrime. The Computer Fraud and Abuse Act, 1986 (CFAA) provides substantial grounds for prosecution, while initiatives such as the National Cyber Investigation Joint Task Force (NCIJTF) promote collaboration between agencies.[28] The U.S. model demonstrates a high degree of institutional integration and real-time response capabilities, particularly in counterterrorism cyber operations and election interference monitoring.[29]

D. United Kingdom

The UK's approach is based on the National Crime Agency (NCA) and its National Cybercrime Unit (NCCU), backed by the Computer Misuse Act, 1990.[30] The Cyber Aware program, a public-private partnership, focuses on training and raising awareness among citizens.[31] Unlike India, the UK deploys Regional Organized Crime Units (RCUs) to decentralize expertise and improve local response capacity.[32]

E. Estonia: A Model of Cyber Resilience

Following the 2007 cyberattacks on its infrastructure, Estonia undertook structural reforms that transformed it into a model of cyber resilience. Its NATO-affiliated Centre of Excellence for Cooperative Cyber Defense (CCDCOE) organizes the annual Locked Shields exercise, which simulates real-world cyber incidents for law enforcement in all jurisdictions.[33] Estonia's experience highlights the fundamental value of preventive planning, digital literacy and inter-agency exercises.[34]

VII. CYBER POLICING CASE STUDIES: INDIA AND ABROAD

A. India: The Cosmos Bank Cyber Heist (2018)

In August 2018, hackers diverted around ₹94 crore from the Pune-based Cosmos Bank through a malware attack on its ATM switching server.[35] The perpetrators used cloned debit cards in 28 countries in two days. The incident highlighted the deep vulnerabilities of the cooperative banking infrastructure and the deficiencies in incident response.[36] The Maharashtra Cyber Cell collaborated with INTERPOL and multiple foreign agencies, but no arrests were made for more than a year.[37] Despite traces of evidence, legal hurdles involving server jurisdictions and lack of intermediary cooperation hampered prosecutions. This case has highlighted the urgent need for

[28] Federal Bureau of Investigation (FBI), *Attribution of WannaCry to the Lazarus Group* (2018), https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and/

[29] U.S. Department of Justice, *Operation Disruptor Results* (October 2020), https://www.justice.gov/archives/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170/

[30] UK Home Office, *Cybersecurity Strategy 2022-2030,* https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/

[31] National Crime Agency (UK), *Annual Cybercrime Threat Report* (2023), https://assets.publishing.service.gov.uk/media/66b627400808eaf43b50dfd0/NCA+Annual+Report+2023-24.pdf

[32] *Id.*

[33] NATO CCDCOE, *Locked Shields Cyber Defence Exercise* 2023, https://ccdcoe.org/news/2023/6016/

[34] *Id.*

[35] Cosmos Bank FIR Case No. 456/2018.

[36] *Id.*

[37] *Id.*

international treaties and real-time data sharing.[38]

B. India: The Case of the Bulli Bai and Sulley Agreements

In 2021-22, two major cases of online harassment involved uploading manipulated images of Muslim women to fictitious auction apps hosted on GitHub.[39] The FIRs were registered under Sections 78, 79 of the BNS and 66E of the Information Technology Act. Mumbai and Delhi police, in coordination with Indian Computer Emergency Response Team (CERT-In) located the defendants using digital fingerprints. The cases demonstrated how digital forensics and rapid interstate cooperation can produce results, though they also highlighted GitHub's initial delay in providing user data due to jurisdictional hurdles.[40]

C. International: WannaCry Ransomware Attack (2017)

WannaCry affected more than 300,000 systems in 150 countries, focusing on healthcare, banking, and government infrastructure.[41] The National Health Service (NHS) in the UK was severely affected.[42] The investigations have been traced back to North Korean state-sponsored hackers, though attribution has been diplomatically sensitive.[43] The response included collaboration between the FBI, Microsoft, and Europol. The Indian Computer Emergency Response Team (CERT-In) in all jurisdictions have released decryption tools and patches. This case illustrated the need for global cooperation and a multi-stakeholder cybersecurity apparatus.[44]

D. International: Operation Disruptor (2020)

A joint effort by the U.S. Department of Justice, Europol, and law enforcement agencies from nine countries, Operation Disruptor dismantled darknet markets, including Alpha Bay and Wall Street Market.[45] More than 170 arrests were made, and crypto seizures totalled more than $6.5 million.[46] This operation is a model of cross-border collaboration, forensic tracking of cryptocurrencies, and proactive law enforcement through cyber patrols and undercover digital agents.[47]

VII. THE ROLE OF PUBLIC-PRIVATE PARTNERSHIPS AND DIGITAL LITERACY

A. Industry Collaboration and Cyber Surveillance

The private sector, which includes ISPs, social media platforms, fintech services, and cybersecurity firms, has an unprecedented technology infrastructure and real-time monitoring capabilities. Law enforcement authorities rely heavily on these entities for data retention, log

[38] *Id.*
[39] *GitHub Response Disclosure under MLAT*, Mumbai Police Case File (2022).
[40] *Id.*
[41] Europol and FBI, *WannaCry Coordinated Investigation* (2017), https://www.europol.europa.eu/media-press/newsroom/news/2017-year-when-cybercrime-hit-close-to-home/
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] U.S. Department of Justice and Europol, *AlphaBay Takedown and Evidence Seizure Report* (2020), https://www.justice.gov/archives/opa/pr/alphabay-largest-online-dark-market-shut-down/
[46] *Id.*
[47] UK Cabinet Office, *Cyber Aware Evaluation* (2023), https://www.gov.uk/government/publications/information-security-review-2023-final-report/information-security-review-2023-final-report-html/

analysis, and IP address tracking. In accordance with Section 79 of the Information Technology Act, intermediaries are obliged to exercise due diligence and provide the necessary assistance. However, a 2020 report by the Data Security Council of India (DSCI) found that intermediary response times ranged from 10 to 45 days, making investigations severely difficult.[48] To address this problem, some jurisdictions, such as the United Kingdom, have formalized public-private coordination units within law enforcement structures. In India, this integration remains informal and inconsistently enforced.[49] Joint working groups, cybersecurity simulation exercises, and information-sharing mechanisms between the Indian Computer Emergency Response Team (CERT-In) and big tech companies (such as Google, Meta, and Microsoft) have shown promise, but they need to be institutionalized.[50] The Reserve Bank of India (RBI)[51] and the Securities and Exchange Board of India (SEBI)[52] has also issued industry notices requiring regular cyber audits, thereby incentivizing compliance.

B. Capacity Building and Digital Literacy

India's digital penetration rate exceeds 850 million users, but digital literacy remains alarming, especially in rural and Tier 2 and Tier 3 regions. According to a 2023 survey conducted by Internet and Mobile Association of India (IAMAI), less than 30% of users were able to identify phishing or scam attempts.[53] This lack of knowledge makes citizens vulnerable to cyber fraud and undermines trust in reporting mechanisms. The training programs of National Association of Software and Service Companies (NASSCOM), National Institute of Criminology and Forensic Sciences (NICFS) and police academies are nascent but growing.[54] Initiatives such as Cyber Dost[55] (a Twitter-based outreach platform by MHA) and CBSE's cyber wellness program are examples of state-backed efforts to promote awareness.[56] Despite this, there is no consolidated national policy on cyber hygiene for students, seniors, and small business owners. A 360-degree approach is needed combining basic awareness, school curricula and platform accountability.

C. The Role of Academia and Civil Society

Academia and civil society organizations play a key role in analyzing state surveillance, formulating rights-based critiques and suggesting ethical frameworks for law enforcement

[48] DSCI and MeitY, *Public-Private Cybersecurity Frameworks in India* (2022), https://www.dsci.in/files/content/knowledge-centre/2023/India-Cybersecurity-Industry.pdf
[49] *Id.*
[50] CERT-In, *Annual Report on the Coordination of Cyber Threat Intelligence* (2024), https://www.cert-in.org.in/PDF/Digital_Threat_Report_2024.pdf
[51] Reserve Bank of India (RBI), *Cyber Security Framework for Banks*, Circular (2016), https://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=1721/
[52] Securities and Exchange Board of India (SEBI), *Cyber Security and Cyber Resilience Framework for Market Infrastructure Institutions* (2018), https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html
[53] Internet and Mobile Association of India (IAMAI) and Nielsen, *India Internet Report* (2023), https://uat.indiadigitalsummit.in/sites/default/files/thoughtleadership/pdf/Kantar_iamai_Report_20_Page_V3_FINAL_web_0.pdf
[54] NASSCOM and NICFS, *Digital Forensic Capability Survey* (2021), https://community.nasscom.in/communities/cyber-security-privacy/digital-forensics-solving-legal-and-regulatory-issues.html
[55] Ministry of Home Affairs, *CyberDost Campaign Review* (2023), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2065959/
[56] Central Board of Secondary Education (CBSE), *Cyber Wellbeing Curriculum* (2022), https://www.cbse.gov.in/cbsenew/documents/Cyber%20Safety.pdf

conduct.[57] Collaborations have emerged between law schools and state cyber cells for legal assistance, research, and capacity building, but they require more institutional support.[58]

VIII. RECOMMENDATIONS FOR REFORM AND THE WAY FORWARD

A. Legislative Review and Harmonization

India needs to enact a comprehensive cybercrime code that consolidates the scattered provisions of the Information Technology Act, the Bharatiya Nyaya Sanhita, and the Bharatiya Sakshya Adhiniyam. The harmonization of procedural law is essential, especially with regard to the collection of digital evidence, the admissibility of data under the Bharatiya Sakshya Adhiniyam, and integration with global protocols such as the Budapest Convention. The recently enacted Digital Personal Data Protection Act must be effectively implemented to provide legal guarantees to citizens and clarity for the application of the law.

B. Establishment of Specialized Courts For Cybercrime

To address procedural backlogs and low conviction rates in cybercrime cases, India needs to establish specialized cybercrime courts at the district and higher court levels. Judges and prosecutors should receive mandatory training in digital forensics, blockchain, data preservation, and cyber law. In addition, case management systems should incorporate electronic filing, virtual testimony, and secure discovery portals to ensure procedural efficiency and chain of custody integrity.

C. Capacity-Building and Training Of The Police

The current police training curriculum needs to be updated to include modules on Open Source Intelligence (OSINT), cyber forensics, cryptocurrency tracing, and darknet monitoring. Cyber cells in all districts should be equipped with modern digital laboratories, and their performance indicators should be linked to the success of prosecutions and not just to the number of FIRs registered. Mandatory certifications from National Institute of Electronics and Information Technology (NIELIT) or National Institute of Criminology and Forensic Science (NICFS) help standardise cyber surveillance credentials. Judicial oversight mechanisms, independent audits and whistleblower protection must be institutionalised to ensure accountability. Public confidence in law enforcement cannot be the result of mere efficiency; it must be based on legitimacy. As digital policing tools become more invasive, ethical and rights-based frameworks must evolve simultaneously.

IX. CONCLUSION

As the frontier of crime shifts into cyberspace, the response of law enforcement authorities must transcend conventional paradigms. The nature of cybercrime is borderless, anonymous and rapidly evolving, requiring a rethink of jurisprudence on crimes, evidence and sanctions. India, with its booming digital population and expanding e-governance, is at a critical juncture. The

[57] University Grants Commission (UGC), *Model Law Curriculum - Cyber Law Module* (2024), https://ugcmoocs.inflibnet.ac.in/index.php/courses/view_ug/185#:~:text=UGC%20MOOCs:%20A%20Vertical%20of,About%20UGC%2DMOOCs/

[58] NICFS, *Cybercrime Investigation Curriculum* (2023) https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://cytrain.ncrb.gov.in/&ved=2ahUKEwj3-ej7mtaPAxX0T2wGHXhaCWYQFnoECBoQAQ&usg=AOvVaw2JvWDUfY7v2KxDNxTj6cZq/

current legal and institutional framework, while laudably evolving, remains fragmented, under-resourced and procedurally inadequate to address the complex cyber threat architecture. While initiatives like Indian Cybercrime Coordination Centre (I4C) and the Indian Computer Emergency Response Team (CERT-In) are structurally promising, they must be backed by legal legitimacy, advanced training, and collaborative ethics. International models reveal the need for transnational cooperation, decentralised law enforcement and multi-stakeholder participation. Case studies, both national and global, highlight not only the vulnerabilities but also the resilience that coordinated law enforcement can bring. Ultimately, the legitimacy of cyber policing lies in its ability to guarantee digital rights without compromising civil liberties. A digital Leviathan must remain chained to constitutional morality. Vigilance should not be a substitute for evidence, and technological prowess should not silence procedural fairness. For the rule of law to prevail, India must invest not only in infrastructure but also in imagination, re-engineering its law enforcement agencies not just with better tools but with a new philosophy, one that is as agile, borderless, and technologically fluent as the threat it seeks to contain.