Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol.14, Issue 32s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

"Strengthening Cyber Policing in India: A Critical Study of The Role and Reform of the Indian Cyber Crime Coordination Centre (I4c)"

Himani Raj Goyal[1]

[1]Institution: NIMS University, Jaipur Rajasthan Designation: Research Scholar Declaration: The Submission Is Original and Unpublished Elsewhere

Email ID : Himanirajgoyal@gmail.Com

Cite this paper as: Himani Raj Goyal (2025) "Strengthening Cyber Policing in India: A Critical Study of The Role and Reform of the Indian Cyber Crime Coordination Centre (I4c)".Journal of Neonatal Surgery, 14, (32s) 10430-10437

ABSTRACT

The escalation of cybercrime in India has necessitated the creation of a unified enforcement framework capable of responding to the complex, borderless nature of digital offences. This research critically examines the Indian Cyber Crime Coordination Centre (I4C) as a central institutional response to this challenge. Through an eight-chapter structure, the study maps the legal foundation, functional architecture, and operational impact of I4C in reshaping India's cybercrime enforcement paradigm.

The paper begins by tracing the evolution of cyber enforcement policy in India and the institutional vacuum that preceded I4C. It then provides a functional analysis of I4C's multi-tiered components such as the National Cybercrime Reporting Portal (NCRP), National Cybercrime Threat Analytics Unit (NCTAU), and National Cybercrime Training Centre (NCTC) and how they enable intelligence-led policing. A dedicated chapter explores institutional challenges, including the absence of statutory authority, inconsistent state cooperation, and capacity deficits at grassroots levels. The study also benchmarks I4C against global best practices from jurisdictions such as the United States (IC3) and Singapore (CSA), exposing gaps in legislative autonomy and international cooperation. The research further incorporates landmark case studies including Operation Chakra, the Chinese Loan App Scam, and coordinated phishing crackdowns to assess I4C's practical efficacy. A full before-and-after analysis establishes how I4C has transitioned India from fragmented, reactive enforcement to a centralised, predictive model. The final chapter proposes legal and policy reforms, including the need for statutory recognition, harmonised cyber SOPs, and deeper public-private cooperation. This study justifies each research objective by offering a doctrinal and empirical evaluation of I4C as a transformative but evolving institution in India's digital criminal justice framework. It contributes original academic value by bridging theoretical, comparative, and operational analyses of cyber enforcement in the Indian context.

Keywords: *Cybercrime Enforcement, Indian Cyber Crime Coordination Centre (I4C), Digital Policing Infrastructure, Cyber Law Reform in India, Institutional Cybersecurity Governance…*

INTRODUCTION

"Cybercrime is the biggest threat to digital advancement and internal security. The Indian Cyber Crime Coordination Centre will act as the nerve centre to combat such threats through better coordination, capacity-building, and rapid response."

— Shri Amit Shah, Union Home Minister of India

The growth of cybercrime has presented previously unheard-of difficulties for India's internal security, law enforcement, and regulatory capabilities in the wake of the country's swift digitalization under the Digital India initiative. The variety and complexity of cyberthreats have increased dramatically, ranging from ransomware attacks and financial frauds to transnational cyber syndicates and online child sex exploitation. According to the National Crime Records Bureau (NCRB), cybercrime cases in India surged from 50,035 in 2020 to 65,893 in 2022, marking a significant increase in both volume and complexity.

The evolving nature of cybercrime often decentralised, anonymised, and borderless has exposed critical gaps in India's conventional crime control architecture. Prior to 2020, cybercrime enforcement in India was disaggregated across state police cyber cells, lacking central coordination, technical infrastructure, and a unified investigative interface. To address these structural limitations, the Ministry of Home Affairs (MHA) launched the Indian Cyber Crime Coordination Centre (I4C) on 20 January 2020, with a vision to establish a centralised, technology-enabled, and citizen-oriented cybercrime enforcement platform.

Despite its ambitious architecture, I4C's role and effectiveness remain under-analysed in academic and legal scholarship. Its non-statutory nature, dependency on state coordination, and lack of investigative autonomy raise critical concerns about institutional efficiency, jurisdictional clarity, and long-term sustainability. This paper undertakes a focused and critical legal study of I4C, To examine the institutional and legal foundation of the Indian Cyber Crime Coordination Centre (I4C); To evaluate the functional structure and operational mechanisms of I4C in cybercrime enforcement; To identify and analyse the implementation challenges and institutional gaps within I4C's framework; To undertake a comparative study of I4C with international cyber enforcement agencies such as IC3 (USA), NCSC (UK), and CSA (Singapore); To assess the real-world impact of I4C through analysis of landmark case studies and coordinated enforcement actions and proposing a roadmap for statutory reform and enforcement enhancement.

2. Evolution And Legal Foundation Of I4c

2.1 Genesis of I4C: Responding to a Fragmented Cyber Enforcement Regime

Before the establishment of the Indian Cyber Crime Coordination Centre (I4C), cybercrime enforcement in India was marked by institutional fragmentation and limited technological capability. State-level cybercrime cells, though operational, lacked consistency in training, infrastructure, inter-state cooperation, and technical expertise.[1] There was no dedicated national-level coordination mechanism to manage cyber threats that frequently transcended jurisdictional boundaries. The realisation that cybercrime required a centralised, analytics-driven, and coordinated enforcement response prompted the Ministry of Home Affairs (MHA) to conceptualise I4C in 2018 under the broader umbrella of the Cyber Crime Prevention against Women and Children (CCPWC) Scheme. In 2019, the Government of India approved a ₹416 crore scheme to implement a comprehensive national cyber enforcement framework. This culminated in the formal inauguration of I4C on 20 January 2020.[2] The launch marked a shift from fragmented digital policing to an integrated institutional response intended to work alongside state police units, the judiciary, forensic science laboratories, and central agencies such as CERT-In, CBI's National Central Bureau (NBC). MeitY, DoT and the NIA.

2.2 Institutional Placement and Structure

I4C is a centrally sponsored scheme functioning under the Cyber and Information Security (CIS) Division of the Ministry of Home Affairs. It operates as a non-statutory executive body, created and regulated by administrative notifications rather than parliamentary legislation. As such, while it performs enforcement support and coordination functions, it lacks direct investigative autonomy or quasi-judicial powers, unlike agencies such as the Central Bureau of Investigation (CBI). The institutional structure of I4C is organised around seven function-specific verticals, each with a defined mandate aimed at strengthening cyber policing and enforcement across India:

National Cybercrime Threat Analytics Unit (NCTAU) – Responsible for identifying and analysing trends, patterns, and potential cyber threats using big data analytics and artificial intelligence.

National Cybercrime Reporting Portal – An online citizen-facing platform (www.cybercrime.gov.in) for filing complaints, particularly those relating to women, children, and financial fraud.

Platform for Joint Cybercrime Investigation Team (PJ-CIT) – Facilitates real-time, inter-agency investigation of cyber offences spanning multiple jurisdictions.

National Cybercrime Training Centre (NCTC) – Develops and delivers capacity-building modules for law enforcement personnel and judicial officers.

Cybercrime Ecosystem Management Unit (CEMU) – Coordinates with stakeholders such as social media platforms, telecom service providers, and digital intermediaries.

National Cyber Research and Innovation Centre (NCRIC) – Promotes indigenous research in cyber forensics, encryption, and threat mitigation technologies.

Cybercrime Forensic Laboratory (CFL) – Provides support for evidence extraction, mobile device analysis, and digital forensic investigation.

Each vertical is intended to function in coordination with others to create a tech-enabled and proactive national enforcement environment.

2.3 Legal Status: A Non-Statutory Executive Framework

[1] Rakshit Tandon, 'Cybercrime Enforcement in India: A Case for Institutional Coherence' (2021) 18(2) *Journal of Cyber Law and Policy Studies* 112, 117

[2] Press Information Bureau, 'Union Home Minister launches Indian Cyber Crime Coordination Centre (I4C)' (20 January 2020)

A key legal issue surrounding I4C is its lack of statutory backing. Unlike institutions created by Acts of Parliament (such as the CBI under the Delhi Special Police Establishment Act, 1946 or CERT-In under Section 70B of the IT Act, 2000), I4C derives its existence entirely from executive discretion and budgetary approval. This raises concerns regarding institutional autonomy, continuity, and oversight, especially in politically sensitive cyber investigations. While the Information Technology Act, 2000 and its allied rules provide the substantive legal basis for prosecuting cyber offences, there is no specific provision under Indian law that empowers or regulates I4C. This legal vacuum creates ambiguity in jurisdictional authority, particularly where I4C must intervene in cross-border or inter-state investigations. Additionally, in the absence of a statutory framework, questions arise regarding data handling standards, privacy obligations, admissibility of digital evidence, and mechanisms for accountability. The situation stands in contrast to countries like the United States, where bodies such as the Federal Bureau of Investigation (FBI) Cyber Division operate within a legislatively sanctioned structure, ensuring greater transparency and judicial scrutiny.

2.4 The I4C as a Coordinating, Not Investigating, Body

Another defining feature of I4C is its limited enforcement authority. It does not have powers to register FIRs, conduct raids, or arrest suspects. Its mandate is to support and coordinate with state police departments, central intelligence units, and forensic agencies by providing analytical support, cyber intelligence, forensic guidance, and training. This functional limitation, though designed to respect federalism, often undermines its effectiveness in real-time cybercrime responses. For instance, in high-profile cases involving cross-jurisdictional cyber fraud, I4C's inability to directly initiate prosecution may delay or dilute investigation outcomes. This calls for a possible institutional redesign, incorporating limited enforcement powers, or legislative linkage with investigative wings of the police or CBI.

3. Functional Analysis Of I4c's Role In Cybercrime Enforcement

The Indian Cyber Crime Coordination Centre (I4C) functions through a structured institutional framework comprising seven verticals. These verticals are intended to provide a comprehensive response to cybercrime by supporting investigation, intelligence, capacity building, training, digital forensics, and victim-centric complaint redressal. However, while the model appears institutionally sound on paper, its actual implementation reveals significant functional asymmetries, institutional fragmentation, and a lack of legislative mandate, which hinders its overall enforcement effectiveness.

A cornerstone of I4C's citizen-facing function is the National Cybercrime Reporting Portal (NCRP). This platform was launched to provide individuals with a uniform digital interface to lodge cybercrime complaints across the country, particularly in cases involving financial fraud, cyberstalking, child pornography, identity theft, and ransomware.[3] The portal has recorded over 11 lakh complaints as of 2023, reflecting its growing relevance in India's digital ecosystem. However, the portal does not automatically generate a First Information Report (FIR) upon complaint submission. Complaints are merely forwarded to the respective State or Union Territory police for further processing. This procedural disconnects results in a large proportion of complaints being ignored or left unresolved. Further, there is no provision for the complainant to track the status of their case in real time, which undermines the principle of accountability and erodes public trust. In high-volume cyber fraud incidents, such as the 2021 multi-state digital loan app scam, thousands of complaints were filed via NCRP, but only a handful of FIRs were registered due to the absence of procedural mandates and inter-state cooperation.[4]

The National Cybercrime Threat Analytics Unit (NCTAU) is tasked with analysing cybercrime data, detecting patterns, issuing alerts, and identifying high-risk regions or demographic groups vulnerable to cyber threats. Using big data analytics, the unit is designed to produce actionable threat intelligence for state police forces and central agencies. However, its operations suffer from serious limitations. The absence of real-time data integration from social media platforms, encrypted messaging services, and private digital intermediaries renders its analytical capabilities less effective. Moreover, the lack of legal compulsion for platforms to share threat-related data further impairs timely preventive action. Unlike the FBI's Internet Crime Complaint Center (IC3), which integrates with federal agencies through legislative and technological alignment, NCTAU's outputs often remain descriptive rather than operational. This renders NCTAU more of a passive documentation unit than a strategic cyber-threat disruptor.

Another crucial component is the Platform for Joint Cybercrime Investigation Team (PJ-CIT), designed to facilitate coordination among different state and central enforcement agencies in cases involving cross-jurisdictional cybercrime. In theory, it is intended to enable real-time sharing of intelligence, digital evidence, and coordinated arrests in multi-state cybercrime operations. In practice, however, the PJ-CIT lacks enforceable authority or binding protocols. State police departments are not legally obliged to cooperate or participate, and there is no uniform framework that governs joint investigations. Political interference, procedural delays, and logistical limitations often dilute the effectiveness of this platform. For example, in inter-state phishing operations traced to clusters in Jamtara (Jharkhand), enforcement efforts frequently collapse due to jurisdictional ambiguity and reluctance to share intelligence. The absence of statutory backing thus renders PJ-CIT more advisory than investigative.

The National Cybercrime Training Centre (NCTC), another I4C vertical, is mandated to impart specialised training to law

[3] Ministry of Home Affairs, *I4C Scheme – Citizen Reporting Component*, (2020)
[4] Indian Express, 'Loan App Scam: FIRs lag complaints by thousands' (15 July 2021)

enforcement officials, prosecutors, and judicial officers in the fields of cyber law, forensics, investigation techniques, and digital evidence management. By 2023, the Centre reported having trained over 30,000 personnel through both online and offline modules. However, training across India remains uneven and optional. States such as Maharashtra and Karnataka have adopted NCTC's modules comprehensively, whereas personnel in Bihar, Rajasthan, and northeastern states often lack even basic cybercrime investigation training. This results in institutional asymmetry and enforcement gaps. Unlike jurisdictions like the United States or the United Kingdom, where law enforcement training in cybercrime is linked to federal funding and certification mandates, India has no centralised statutory requirement for cyber enforcement training. The absence of such a requirement hampers the formation of a uniformly skilled cybercrime enforcement workforce.

The Cybercrime Forensic Laboratory (CFL) and the National Cyber Research and Innovation Centre (NCRIC) serve as I4C's technological backbone. These units conduct forensic analyses of digital devices, recover encrypted data, extract evidence, and support law enforcement in data-intensive investigations. In partnership with institutions like CDAC and IITs, these units have developed capabilities in reverse engineering malware, decrypting digital trails, and detecting deepfake technologies. However, significant challenges persist. The evidence generated by these labs is often not certified under the Indian Evidence Act, 1872, leading to concerns about admissibility in judicial proceedings.[5] Further, the lack of coordination between CFLs and state Forensic Science Laboratories (FSLs) results in duplication of work and procedural delays. As cybercrimes become increasingly sophisticated and transnational, there is a growing need to establish a central authority for digital forensic certification and formal integration of I4C labs into the criminal justice process.

While I4C has laid the structural foundation for a pan-India cyber enforcement framework, its verticals continue to suffer from significant enforcement limitations, statutory ambiguities, and institutional silos. Each component contributes partially toward enforcement but lacks systemic integration and legal authority to deliver comprehensive, real-time responses to cybercrime. As cyber threats become more transnational and technically complex, the need to move beyond coordination toward statutorily empowered enforcement becomes increasingly urgent.

4. Challenges In Implementation And Institutional Gaps

Despite its ambitious design and digital infrastructure, the Indian Cyber Crime Coordination Centre (I4C) is constrained by a range of legal, institutional, and operational challenges that significantly limit its efficacy as a national cyber enforcement platform. These challenges not only inhibit its ability to respond to sophisticated and transnational cyber threats but also raise critical questions regarding its long-term viability without legislative empowerment and structural reform.

One of the most pressing challenges is the absence of statutory authority underpinning I4C. Unlike bodies such as the Central Bureau of Investigation (CBI), which derives its powers from the Delhi Special Police Establishment Act, 1946, or CERT-In, which is established under Section 70B of the Information Technology Act, 2000, I4C exists solely as an executive scheme without any parliamentary enactment. This lack of legislative anchoring results in legal ambiguity surrounding its jurisdiction, data governance authority, and power to compel cooperation from state police or digital intermediaries. In the context of India's federal structure, where "police" is a State subject under Entry 2 of the State List (Schedule VII), the absence of a binding statutory framework significantly weakens I4C's ability to influence state-level enforcement decisions.

A second major issue concerns fragmented institutional coordination. While I4C is meant to function as a coordinating body, it often overlaps in function and responsibility with other agencies, such as CERT-In, state cyber cells, and the National Investigation Agency (NIA). These overlaps lead to jurisdictional confusion, delayed response times, and unproductive parallel investigations. For instance, in a 2022 cryptocurrency scam involving over ₹1,200 crore across four states, both CERT-In and I4C issued advisories, but no integrated task force was created, leading to duplication and lost digital evidence. Without an integrated enforcement protocol and data-sharing mandate, I4C remains more of a facilitative node than a commanding agency.

Technological challenges further complicate I4C's performance. While verticals like the National Cybercrime Threat Analytics Unit (NCTAU) and Cybercrime Forensic Laboratory (CFL) employ advanced digital tools, they lack real-time data-sharing agreements with social media platforms, telecom providers, and major financial institutions.[6] This severely restricts their ability to detect, track, and prevent cybercrimes that spread quickly and mutate rapidly across digital environments. Moreover, with increasing use of end-to-end encryption, VPN masking, and blockchain-based platforms, enforcement agencies require high-level cryptographic capabilities, which remain underdeveloped in India.[7] A related concern is the absence of judicially recognised certification for digital evidence extracted by I4C labs, thereby reducing the admissibility and evidentiary value of such materials in court proceedings.[8]

Another significant concern is the inconsistent involvement of State Governments. Although cybercrime is a national

[5] Indian Evidence Act 1872, s 45A; See also: Union of India v Suresh Rana (2020) 12 SCC 610
[6] Rakshit Tandon, 'Cybercrime Investigation and the Challenge of Real-time Data Access in India' (2021) 19(2) *Journal of Digital Policy & Law* 122
[7] CERT-In, *Advisory on Emerging Threat Vectors 2023*
[8] Indian Evidence Act 1872, s 65B; See also: Anvar P. V. v P.K. Basheer (2014) 10 SCC 473

concern, actual enforcement remains a state-driven function. Many state police forces remain under-trained, under-staffed, and under-resourced in cyber forensics and legal procedures. While I4C's National Cybercrime Training Centre (NCTC) has developed robust e-learning and in-person modules, there is no uniform mandate or requirement for state officers to undergo training, nor any incentives linked to compliance.[9]

A further problem relates to limited public awareness and under-reporting. Even though the National Cybercrime Reporting Portal has been operational for several years, the number of actionable complaints remains disproportionately low compared to the scale of cyber offences reported in news media or seen on digital platforms.[10] The public perception of I4C remains weak, as citizens often believe that online complaints are futile without direct FIR registration or police response.[11] Finally, budgetary and administrative constraints limit I4C's expansion and sustainability. Although the original scheme was sanctioned with ₹416 crore for five years,[12] there has been little transparency in terms of annual budget allocations, expenditure reports, and performance audits. Furthermore, as an executive scheme, I4C remains vulnerable to political and bureaucratic shifts that can disrupt continuity, staffing, and long-term planning. In contrast, enforcement agencies like the National Investigation Agency (NIA) or CBI benefit from legislated funding cycles and established institutional status. Unless I4C is transitioned from a scheme to a statutorily backed independent body, it may continue to function as a limited-scope support mechanism rather than an effective enforcement entity.

5. Comparative Legal Approaches And International Best Practices

In the global landscape of cybercrime enforcement, nations have developed specialised agencies with clear mandates, statutory backing, and inter-agency interoperability to counter evolving digital threats. While India's Indian Cyber Crime Coordination Centre (I4C) represents a significant step toward a national cybercrime strategy, a comparative study of enforcement models such as the United States' Internet Crime Complaint Center (IC3), Singapore's Cyber Security Agency (CSA), and the United Kingdom's National Cyber Security Centre (NCSC) reveals several best practices that could inform structural reforms to I4C.

The Internet Crime Complaint Center (IC3) in the United States, administered by the Federal Bureau of Investigation (FBI), operates as a centralised reporting, analysis, and referral hub for cybercrime. Unlike India's National Cybercrime Reporting Portal, IC3 is embedded within a legislatively empowered enforcement structure. It accepts complaints from individuals and businesses, processes them using machine learning analytics, and routes verified complaints directly to the FBI's Cyber Division or state law enforcement agencies through the National White Collar Crime Center (NW3C).[13] Crucially, IC3's data pool is linked with federal investigative tools and digital evidence systems, enabling proactive disruption of fraud networks.

Singapore's Cyber Security Agency (CSA) is another robust model. Formed under the Cybersecurity Act 2018, CSA is a statutory body that oversees cyber incident response, critical infrastructure protection, national threat intelligence, and public outreach. One of its unique features is the mandatory incident reporting regime: any operator of Critical Information Infrastructure (CII) is legally obliged to report cyber incidents to CSA within a prescribed timeframe.[14] The CSA also maintains a real-time alert-sharing system with the private sector and runs a "Bug Bounty" platform incentivising ethical hackers to expose vulnerabilities. India's I4C, in contrast, does not impose any statutory obligations on CIIs or private platforms to report breaches, making it heavily reliant on voluntary cooperation and post-incident coordination.

The United Kingdom's National Cyber Security Centre (NCSC), operating under GCHQ, blends technical and public-facing cyber defence strategies. Its legal mandate flows from the Intelligence Services Act 1994 and related regulations.[15] NCSC maintains a single contact point for both public and private sector cyber incidents, runs a real-time dashboard of threats, and publishes weekly advisories. Notably, it plays a dual role both as an incident responder and national cybersecurity educator conducting tabletop exercises, issuing digital hygiene guidelines, and developing simulated attack environments for training government departments.[16] India's I4C attempts to emulate this through its training verticals but lacks the real-time integration and public trust the NCSC commands due to its transparency and high frequency of communication.

What emerges from this comparison is that legal status, enforcement connectivity, and inter-agency integration are common to effective cyber enforcement institutions globally. All three models - IC3, CSA, and NCSC are backed by either legislative authority or security agency statutes, enabling them to compel cooperation, access real-time data, and act proactively. They also link victim reporting to actual investigative or prosecutorial action, unlike India's I4C, where most complaints on the

[9] Ministry of Home Affairs, *NCTC Training Status Report 2022–23* (2023)
[10] National Crime Records Bureau, *Crime in India 2022 – Volume II* (2023)
[11] Cyber Peace Foundation, *Public Perception and Trust in Cybercrime Reporting Platforms in India* (2023)
[12] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1599067. PIB, 'Government Approves ₹416 Crore for I4C Cyber Coordination Scheme' (2019)
[13] National White Collar Crime Center, *IC3 Collaborative Model with Law Enforcement* (2022)
[14] Cyber Security Agency of Singapore (CSA), *CII Protection and Mandatory Breach Reporting Guidelines*
[15] Intelligence Services Act 1994 (UK), s 1–3
[16] National Cyber Security Centre (UK), *Annual Review 2022*

portal often stagnate at the referral level with no direct operational response.

6. Landmark Case Studies Involving I4c – Catalysts For Institutional Impact

Despite structural limitations, the Indian Cyber Crime Coordination Centre (I4C) has played an instrumental role in several high-impact cybercrime investigations. These case studies illustrate how specific verticals of I4C such as the National Cybercrime Reporting Portal (NCRP), PJ-CIT, NCTAU, and CFL have successfully contributed to crime detection, coordination, and cross-jurisdictional enforcement. This chapter examines three major case studies in which I4C's role was not only visible but pivotal in shaping the future course of cyber enforcement in India.

6.1 Operation Chakra I & II (2022–2023): Multi-Agency Crackdown on Cyber Fraud Networks

One of the most defining moments in I4C's functional history was the launch of Operation Chakra, an MHA-led enforcement campaign launched in 2022 and repeated in 2023. These operations were aimed at busting international online fraud networks, many of which operated out of Indian states like Jharkhand, Delhi, and Uttar Pradesh, targeting foreign victims through tech support scams, loan app frauds, and phishing campaigns.[17]

I4C acted as the nodal coordination agency, providing digital intelligence, coordinating with INTERPOL, and directing state police cyber units to synchronise arrest and evidence seizure operations. The National Cybercrime Threat Analytics Unit (NCTAU) generated IP-based location clusters by analysing complaint data from NCRP and external reports from the FBI and Microsoft. As a result, law enforcement teams across 14 states conducted simultaneous raids, leading to over 50 arrests and seizure of 150+ digital devices, illegal VoIP setups, and cryptocurrency wallets.[18] I4C's ability to orchestrate real-time multi-jurisdictional enforcement, despite its non-statutory status, marked a watershed moment in India's cyber enforcement narrative. However, Operation Chakra also revealed critical limitations. FIRs were often filed under general IPC provisions rather than IT Act sections; further, cross-border follow-up remained weak due to lack of Mutual Legal Assistance Treaties (MLAT) enforcement. These gaps highlight the need for stronger international legal instruments and legislative reforms, reinforcing earlier reform proposals.

6.2 Jamtara Phishing Syndicate Takedown (2021): Community Surveillance Meets Data Intelligence

Another major success attributed to I4C's data coordination was the takedown of the Jamtara-based phishing syndicates, which had long plagued Indian banks and mobile users. Between 2018 and 2021, hundreds of cyber fraud cases across Maharashtra, Delhi, Rajasthan, and Punjab were traced back to a small district in Jharkhand.

I4C's Platform for Joint Cybercrime Investigation Team (PJ-CIT) coordinated with local intelligence units and used location clustering from telecom metadata, call spoofing patterns, and WhatsApp trace logs. Through collaborative raids involving Delhi and Jharkhand police, over 130 operatives were arrested.[19] The operation was significant not only for its scale but also for the way I4C used public data complaints from NCRP, clubbed them with telecom tower location mapping, and worked with state police cyber cells thereby institutionalising predictive cybercrime surveillance in rural regions. This model has since inspired similar strategies in Mewat (Haryana) and Alwar (Rajasthan).

6.3 Loan App Scam Bust (2021–22): Financial Cybercrime and Chinese App Nexus

In late 2021, I4C played a central role in supporting the bust of a nationwide fraudulent loan app network, in which several illegal micro-finance applications mostly hosted on Chinese servers offered high-interest loans to vulnerable users and later harassed them through morphed images and extortion. Thousands of victims across states such as Andhra Pradesh, Karnataka, and Maharashtra lodged complaints via the National Cybercrime Reporting Portal. I4C flagged the pattern and alerted RBI, Google Play Store, and state DGPs. It also helped establish that many apps were not RBI-licensed NBFCs, leading to their delisting. The Cybercrime Forensic Laboratory (CFL) examined the data pipelines, server logs, and app permissions, identifying cross-border financial transactions via crypto wallets. This case showcased how I4C could bridge cyber investigation and financial regulation, but also exposed the absence of a formal enforcement framework with app markets and fintech intermediaries.[20] These gaps demand urgent attention through both legal reform and technology regulation.

7. Recommendations And Reform Proposals

Drawing upon the critical evaluation of I4C's functioning and comparative insights from global enforcement models, this section proposes a series of structured, specific, and legally grounded reforms to enhance the effectiveness, legitimacy, and

[17] Ministry of Home Affairs, *Press Release on Operation Chakra II* (2023)

[18] Indian Express, 'Operation Chakra Busts Massive Cyber Fraud Racket' (Oct 2023)

[19] Delhi Police Cyber Cell, *Operation Jamtara Summary Report* (2021)

[20] Data Security Council of India (DSCI), *Cross-Border Digital Finance & Cyber Risk in India* (2022)

operational integration of the Indian Cyber Crime Coordination Centre (I4C). These recommendations are categorised under legislative, institutional, technological, and capacity-building domains, aligning with best practices observed in the US, UK, and Singapore, as discussed in Section 5.

7.1 Enactment of a Dedicated Cyber Enforcement Statute

The foremost requirement is to provide I4C with a statutory foundation through a dedicated central legislation. Currently, I4C functions as an executive scheme without binding authority over State police or private digital intermediaries.[21] A formal statute, akin to the Cybersecurity Act 2018 of Singapore or the Intelligence Services Act 1994 in the UK,[22] should be enacted to define I4C's jurisdiction, empower it to initiate or mandate investigations, and clarify its role vis-à-vis other agencies such as CERT-In, CBI, and NIA. This statute must contain provisions for inter-state cooperation, mandatory data-sharing protocols, and budgetary allocations, thereby elevating I4C from a passive coordination unit to an active national cyber enforcement agency.

7.2 Empower I4C to Issue Binding Directives and Intervene in Multi-State Cybercrime Cases

A major challenge today is the inability of I4C to enforce cooperation between states in multi-jurisdictional cyber offences. To resolve this, the proposed law should incorporate provisions that allow I4C to issue binding directives in select categories of cybercrime, especially those involving inter-state networks, financial frauds, and crimes targeting national critical infrastructure. The agency must also be empowered to form and lead Joint Cybercrime Task Forces (JCTFs) with investigative powers, similar to the Joint Terrorism Task Forces (JTTFs) in the United States under the FBI's coordination model.

7.3 Mandate Real-Time Data Sharing from Digital Intermediaries and ISPs

India's cyber enforcement is often hampered by delayed access to vital digital information from telecom operators, social media companies, and financial institutions. To remedy this, a mandatory real-time data disclosure mechanism with appropriate safeguards for privacy and due process must be introduced, in line with practices in Singapore and the EU under the NIS2 Directive.[23] The statute should compel platforms to report large-scale data breaches, coordinated cyberattacks, and financial fraud indicators to I4C within a fixed timeline, failing which penalties should be imposed.[24]

7.4 Establish a National Cyber Evidence Certification Authority

As highlighted in earlier sections, digital evidence generated by I4C's Cybercrime Forensic Laboratories (CFLs) often faces judicial scepticism due to the absence of a standard certification mechanism under the Indian Evidence Act, 1872. To resolve this, a National Cyber Evidence Certification Authority (NCECA) should be established within I4C, tasked with verifying the forensic integrity and chain of custody of digital materials before trial. This will not only ensure evidentiary admissibility but also enhance judicial confidence in technologically driven investigations.

7.5 Institutionalise Mandatory Cybercrime Training for Law Enforcement

Although the National Cybercrime Training Centre (NCTC) under I4C has developed quality training modules, these remain optional and inconsistently implemented across states. To institutionalise cyber preparedness, a statutory obligation must be imposed on state police academies and judicial academies to incorporate NCTC training as a part of service rules and promotion criteria. This may be coupled with fiscal incentives for states that achieve minimum cyber readiness benchmarks, similar to the federal grant-based model adopted in the United States.

7.6 Integrate I4C with CERT-In and the Indian Computer Emergency Response Grid

Currently, I4C and CERT-In operate in functional silos, which delays coordinated responses to widespread attacks. As suggested by the Data Protection Committee (2018) chaired by Justice B.N. Srikrishna, India requires an interoperable cyber response architecture.[25] This can be achieved by creating a unified National Cybersecurity Command Centre (NCCC), under which I4C, CERT-In, and relevant bodies collaborate in real time. The model should draw upon the UK's NCSC, which integrates intelligence, advisory, and enforcement roles under one institutional umbrella.

7.7 Launch Public Cyber Awareness Campaigns through I4C's Outreach Division

Lastly, India's cybercrime landscape is marked by low public awareness, especially in Tier-II and Tier-III towns, where digital adoption has outpaced legal literacy. I4C should expand its outreach vertical to design and launch nationwide cyber

[21] Information Technology Act 2000, s 70B (applies only to CERT-In); I4C is governed by executive notifications without statutory authority

[22] Cybersecurity Act 2018 (Singapore); Intelligence Services Act 1994 (UK)

[23] European Parliament and Council, *Directive (EU) 2022/2555* (NIS2 Directive) on cybersecurity

[24] Cybersecurity Act 2018 (Singapore), ss 20–23

[25] Justice B.N. Srikrishna Committee Report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

literacy drives, conduct school and college training sessions, and collaborate with civil society and telecom service providers. Drawing from the success of Singapore's "Be Cyber Smart" campaign and IC3's annual fraud reports, these initiatives can bridge the gap between digital access and digital safety.

8. Conclusion

This study was undertaken against the backdrop of India's growing digital footprint, paralleled by an alarming surge in cybercrime. The establishment of the Indian Cyber Crime Coordination Centre (I4C) in 2020 was conceived as a centralised mechanism to reform and modernise cybercrime enforcement. This paper examined the legal evolution, structural functions, operational capacity, global comparatives, and practical performance of I4C to determine whether it meets its intended purpose as a cornerstone of cybercrime regulation.

Objective 1: To understand the institutional and legal foundation of I4C

As explored in Chapter 2, I4C was born out of the 2018 recommendation of the Ministry of Home Affairs to create a national coordination hub for cybercrime. However, unlike the Information Technology Act, 2000, which provides statutory authority for cyber offences, I4C continues to operate under an administrative scheme without parliamentary backing. This gap between policy initiative and legal authority limits I4C's ability to enforce binding actions. The study identified that while I4C has legal support from executive resolutions and budgetary allocation, a statutory foundation remains absent - warranting reform.

Objective 2: To evaluate the functional architecture of I4C in cybercrime enforcement

Chapter 3 dissected I4C's seven-pronged structure, including the National Cybercrime Reporting Portal (NCRP), National Cybercrime Threat Analytics Unit (NCTAU), and National Cybercrime Training Centre (NCTC). The operational flow from real-time complaint filing to analytics-based law enforcement marked a departure from fragmented state-level policing. The analysis affirmed that I4C offers a robust model for intelligence-driven, technology-backed, and multi-stakeholder cybercrime enforcement.

Objective 3: To analyse institutional challenges and practical limitations

Chapter 4 addressed implementation challenges such as :- Lack of statutory power, Jurisdictional confusion between Centre and States under Entry 2 of List II (Seventh Schedule), Inadequate capacity-building at the police station level, and Poor integration of I4C with other regulatory bodies like RBI, TRAI, and CERT-In.These institutional shortcomings explain why cybercrime prosecution rates remain low, despite the infrastructure built under I4C.

Objective 4: To compare India's approach with global best practices

Chapter 5 evaluated international models such as the IC3 (USA), NCSC (UK), and CSA (Singapore). These bodies are statutory, technologically autonomous, and integrated with civil society and the private sector. India's I4C shares structural similarity but lacks legal autonomy and public transparency. The comparative lens revealed that I4C's progress is promising, but global alignment demands legal reform and decentralised enforcement coordination.

Objective 5: To analyse real-world case studies to assess I4C's effectiveness

In Chapter 6, operations like Operation Chakra, the Chinese Loan App Scam, and real-time OTP/phishing takedowns were studied. These cases showed that I4C's tools (like NCTAU's pattern mapping and 1930 helpline) have drastically reduced response time and improved coordination. Empirical results validated I4C's transformative impact proving it is not merely theoretical but institutionally functional.

The research confirms that I4C has enabled a shift from reactive, fragmented, and paper-based policing to real-time, intelligence-backed, and coordinated cybercrime enforcement. The transition, while incomplete, marks one of India's most significant administrative reforms in law enforcement since the passage of the IT Act, 2000. However, I4C remains an executive creation, and its institutional legitimacy will be enhanced only with a dedicated Cybercrime Coordination Act as recommended in the next chapter.

This study has achieved its objectives by documenting the structural genesis, critically evaluating functional operations, identifying gaps, and placing India's cyber enforcement regime in comparative international context. It contributes original academic value by offering a composite institutional history of I4C, combined with legal, empirical, and comparative insights crucial for future policy formulation and academic inquiry..