FROM INFORMATION EXCHANGE TO OPERATIONAL INTELLIGENCE: EVALUATING INDIA'S EMERGING CYBER-FINANCIAL INTELLIGENCE FUSION ARCHITECTURE

Adv. Ishaan D. Joshi, Forensic and Criminal Intelligence Expert
Founder and Director, Centre for Crime Sciences and Forensic Intelligence

ABSTRACT

India has rapidly constructed a multi-institutional response to cyber-enabled financial fraud through the Indian Cyber Crime Coordination Centre (I4C), the National Cyber Crime Reporting Portal, the 1930 helpline, the Citizen Financial Cyber Fraud Reporting and Management System, the Cyber Fraud Mitigation Centre, the Suspect Registry, Samanvaya, Financial Intelligence Unit-India (FIU-IND), sectoral regulators, banks, payment intermediaries and telecom-derived risk systems. Yet the existence of connected portals, alerts and nodal arrangements does not itself demonstrate intelligence fusion. This article asks whether India's emerging architecture transforms heterogeneous information into coordinated, actionable and accountable intelligence. It develops a six-level continuum from institutional isolation to adaptive and accountable fusion and applies a documentary-evidence maturity index to publicly verifiable Indian mechanisms. The study combines legal and institutional analysis, process mapping, comparative case analysis and socio-technical evaluation. It finds a hybrid and uneven architecture. CFCFRMS, the Cyber Fraud Mitigation Centre, Samanvaya and telecom-financial risk exchange display features of coordinated analysis and operational tasking, particularly for rapid fund interdiction. However, public evidence remains insufficient to establish system-wide joint priority-setting, common source grading, transparent entity resolution, routine feedback, measurable false-positive correction, independent audit or learning across the complaint-investigation-prosecution chain. India therefore sits between structured information sharing and coordinated analysis, with pockets approaching operational fusion. The article proposes a federated Indian Cyber-Financial Intelligence Fusion Model that preserves institutional mandates while creating common intelligence requirements, auditable analytical standards, time-bound tasking, correction mechanisms and outcome-based performance measures.

Keywords: cyber-financial intelligence; intelligence fusion; cyber-enabled fraud; financial intelligence; public-private partnership; inter-agency coordination; mule accounts; India.

1. Introduction

Cyber-enabled financial crime has become a systems problem rather than a collection of isolated complaints. The relevant event is not merely an unauthorised transfer from one victim to one recipient account. A single incident may involve a social-engineering script, a mobile number, a messaging account, an application or website, a device, one or more IP addresses, multiple bank or payment accounts, layers of mule accounts, cash-out points, corporate shells and actors located across several police jurisdictions. Each institution sees only part of this chain. The victim sees the deception; the bank sees transactions and customer records; the payment system sees routing and velocity; the telecom ecosystem sees subscriber and device relationships; a financial intelligence unit sees suspicious transaction reporting; cyber police see complaints, devices and criminal linkages; regulators see sectoral risk; and prosecutors eventually require admissible evidence. The central governance problem is therefore whether these fragments are merely transmitted or converted into intelligence capable of reducing uncertainty and directing action.

India's response has expanded significantly. I4C was created as the national coordination framework for cybercrime and became an attached office of the Ministry of Home Affairs. The National Cyber Crime Reporting Portal (NCRP), helpline 1930 and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) create a rapid complaint and transaction-interdiction pathway. The Cyber Fraud Mitigation Centre (CFMC) co-locates or otherwise brings together representatives of major banks, financial intermediaries, payment aggregators, telecom service providers, information-technology intermediaries and State or Union Territory law-enforcement agencies. The Suspect Registry shares cyber-fraud identifiers and mule-account data, while Samanvaya provides a data repository, management-information function and interstate analytical linkages. As at 31 January 2026, the Government reported that CFCFRMS had helped save more than Rs 8,690 crore across more than 24.65 lakh complaints; the Suspect Registry had received more than 23.05 lakh suspect identifiers from banks, shared 27.37 lakh Layer-1 mule accounts and contributed to declined transactions worth Rs 9,518.91 crore (Ministry of Home Affairs, 2026a).

Parallel developments have broadened the source base. FIU-IND operates the statutory suspicious-transaction-reporting and financial-intelligence architecture under the Prevention of Money Laundering Act 2002, supported by FINNET 2.0, risk-based STR analysis and operational and strategic dissemination (FIU-IND, 2025). The Reserve Bank of India's KYC and fraud-risk directions require regulated entities to detect unusual activity, address money-mule risks and report suspicious transactions (RBI, 2016; RBI, 2024). The Department of Telecommunications (DoT) launched the Digital Intelligence Platform and, in May 2025, the Financial Fraud Risk Indicator (FRI), which categorises mobile numbers as medium, high or very high risk and enables banks and payment actors to apply warnings, delays, declines or restrictions. By the end of 2025, the Digital Intelligence Platform reportedly included more than 850 organisations, including over 800 banks and financial institutions, while FRI-related alerts or interventions covered more than 70 lakh transactions and were reported to have prevented approximately Rs 450 crore in loss (Department of Telecommunications, 2025b). MoUs between DoT and FIU-IND, and later between DoT and SEBI, formalised reciprocal sharing of telecom and financial-fraud risk indicators (Department of Telecommunications and FIU-IND, 2025; Department of Telecommunications and SEBI, 2026).

These developments are institutionally important, but they do not answer the analytical question. A portal can transfer records without producing intelligence. Co-location can accelerate communication without creating shared priorities. A registry can distribute identifiers without disclosing how those identifiers were validated, how false positives are corrected or whether recipients report outcomes. Large volumes of alerts can increase noise and defensive de-risking rather than detection quality, a problem recognised in the literature on suspicious-activity reporting and the 'crying wolf' effect (Takáts, 2011). Conversely, a modest, tightly governed arrangement can constitute fusion if multiple sources are jointly evaluated, uncertainty is expressed, decisions are tasked, action is recorded and results are returned to improve subsequent analysis.

The principal research question is: to what extent does India's emerging cyber-financial crime architecture transform information shared among I4C, FIU-IND, RBI, DoT, SEBI, NPCI, banks, financial institutions and State law-enforcement agencies into coordinated, actionable and accountable intelligence? The unit of analysis is the institutional process by which cyber-financial information is collected, validated, correlated, analysed, disseminated, operationalised and fed back. The article does not assess the overall success of Indian

cybercrime policy, nor does it treat all cybercrime, money laundering or technical cybersecurity as a single field. It concentrates on cyber-enabled financial fraud, mule-account networks, transaction interdiction, telecom-financial indicators, public-private intelligence exchange and the conversion of intelligence into investigation and evidence.

The article makes four contributions. Conceptually, it distinguishes data transfer, information sharing, coordination, collaborative analysis and intelligence fusion through operational indicators. Empirically, it maps the publicly documented Indian architecture and identifies where the complaint-to-action chain displays stronger and weaker fusion characteristics. Comparatively, it evaluates design lessons from the United Kingdom's National Economic Crime Centre (NECC) and Joint Money Laundering Intelligence Taskforce (JMLIT+), Australia's Fintel Alliance, Europol's Financial Intelligence Public Private Partnership (EFIPPP) and United States mechanisms including FinCEN Exchange, Sections 314(a) and 314(b), and the Rapid Response Program. Normatively, it proposes a federated Indian model that seeks to improve operational effectiveness without creating an unaccountable central data lake or a new super-agency.

The central argument is deliberately qualified. India has moved materially beyond institutional isolation and ad hoc bilateral exchange. Certain mechanisms, especially rapid complaint-to-bank action, co-located mitigation, interstate linkage analysis and telecom-financial risk exchange, exhibit features of coordinated analysis and operational fusion. Nevertheless, publicly available evidence does not establish mature fusion across the architecture as a whole. The weakest visible components are common intelligence requirement-setting, standardised source grading, transparent entity resolution, systematic public-to-private feedback, false-positive measurement, correction and appeal, independent audit, and end-to-end learning from interdiction through investigation, prosecution and exoneration. India is best understood as a hybrid network with pockets of operational fusion embedded within a broader system of structured sharing.

2. Information sharing, intelligence and fusion

2.1 Data, information and intelligence

The distinction between data, information and intelligence is functional rather than semantic. Data are recorded elements: an account number, transaction timestamp, UPI virtual payment

address, mobile number, IP address, device identifier, merchant identifier or KYC document. Information exists when data are organised or communicated so that they convey meaning, for example a report that a particular mobile number was linked to several complaints or that a beneficiary account received rapid transfers from geographically dispersed victims. Intelligence is evaluated and contextualised information produced to reduce uncertainty for a decision. It includes a statement of relevance, reliability, confidence and implications. The same account number may therefore be raw data in a complaint, information in a bank alert and intelligence when correlated with a telecom risk indicator, common device, linked mule accounts and an assessed network role.

Financial intelligence is knowledge derived from transactions, customer information, reporting-entity submissions, ownership relationships and other financial records for identifying, understanding, preventing or investigating illicit activity. Cyber-financial intelligence adds cyber, telecom, identity, behavioural, platform and investigative information. Its defining feature is not that a computer was used, but that heterogeneous source types are integrated to explain or disrupt a cyber-enabled financial process. This integration matters because a transaction graph may expose Layer-1 recipient accounts while telecom and device linkages reveal control, recruitment or shared infrastructure at deeper layers. Conversely, over-integration can create spurious associations where recycled mobile numbers, shared IP addresses, family devices, common addresses or inaccurate KYC are treated as guilt by proximity.

Actionable intelligence is sufficiently specific, reliable, timely and relevant to justify a proportionate preventive, regulatory, investigative or operational response. Actionability is contextual. A high-confidence account-and-transaction match may justify a short emergency hold to preserve funds, but not arrest or public designation. A medium-confidence telecom indicator may justify step-up authentication or enhanced monitoring, but not permanent account closure. Intelligence and evidence are therefore related but not interchangeable. Intelligence can prioritise inquiry and preserve opportunities; evidential use requires lawful acquisition, authentication, chain of custody, admissibility and an opportunity for challenge under the Bharatiya Sakshya Adhiniyam 2023 and the Bharatiya Nagarik Suraksha Sanhita 2023.

2.2 A sharing-to-fusion continuum

The word 'fusion' is often used to signal modernity rather than a demonstrable process. To prevent conceptual inflation, this article uses a six-level continuum. Level 0 is institutional isolation: information remains within one organisation and external access occurs only through exceptional formal requests. Level 1 is reactive exchange: bilateral, incident-driven transfer occurs after a complaint or request, without joint analysis. Level 2 is structured sharing: portals, nodal officers, formats, registries and routine alerts exist, but analysis remains institution-specific. Level 3 is coordinated analysis: multiple sources are correlated, analysts communicate directly, and joint threat assessments, typologies or network products are produced. Level 4 is operational intelligence fusion: common priorities and multi-source analysis generate leads that directly inform freezing, disruption, investigation or prevention, with recorded outcomes. Level 5 is adaptive and accountable fusion: the system measures errors and harm, corrects identifiers, revises models and priorities, supports independent oversight and evaluates success through disruption, recovery, evidential outcomes and rights impact rather than data volume.

Table 1. Sharing-to-fusion continuum

Level	Institutional condition	Core indicators	Diagnostic question
0	Institutional isolation	No routine dissemination; access through exceptional formal requests.	Does relevant information remain within one institution?
1	Reactive information exchange	Bilateral, case-specific transfer after a request or incident; no joint analysis.	Is information only sent after a complaint or request?
2	Structured information sharing	Portals, nodal officers, standard formats, registries and routine alerts; analysis remains separate.	Are records connected but analytical responsibility still siloed?
3	Coordinated analysis	Multi-source correlation, direct analyst contact, joint typologies or network products and some feedback.	Are institutions interpreting information together?

4	Operational intelligence fusion	Common priorities; joint products; direct tasking for freezing, disruption, investigation or prevention; outcomes recorded.	Does analysis reliably direct proportionate action?
5	Adaptive and accountable fusion	Measured errors and harm; correction; model recalibration; independent oversight; outcome and rights metrics.	Does the system learn, correct and remain reviewable?

2.3 Intelligence process, network governance and collaborative governance

The conventional intelligence cycle—direction, collection, processing, analysis, dissemination and feedback—offers a useful checklist but an incomplete description (Clark, 2019; Gill and Phythian, 2018; Ratcliffe, 2016). Hulnick (2006) argues that collection and analysis often occur in parallel, decision-makers do not simply wait for finished intelligence, and institutional practice is more iterative than a neat sequence. A cyber-financial architecture should therefore be evaluated as a recursive process: operational action creates new data, which should refine entity resolution, typologies and priorities. Feedback is not an optional final stage; it is the mechanism through which a risk system learns whether an alert was correct, useful, duplicative or harmful.

Network governance theory explains why a single command hierarchy is neither necessary nor always desirable (Agranoff and McGuire, 2003; Powell, 1990; Ostrom, 2010). Provan and Kenis (2008) identify participant-governed networks, lead-organisation networks and network administrative organisations (NAOs). India's cyber-financial field contains autonomous statutory and operational actors whose mandates cannot simply be absorbed into I4C. FIU-IND has a specialised financial-intelligence role; RBI and SEBI regulate different sectors; DoT governs telecom resources; States investigate most offences; banks and payment providers hold private data and operational controls. A viable design therefore requires a coordinating node with authority to convene, set common requirements and maintain standards, while preserving legal ownership and decision competence. This resembles an NAO or hybrid lead-organisation model more than a unitary agency.

Collaborative governance adds attention to starting conditions, institutional design, leadership, trust and shared capacity (Bryson, Crosby and Stone, 2006; Thomson and Perry, 2006). Ansell

and Gash (2008) emphasise face-to-face dialogue, trust-building, commitment and 'small wins'; Emerson, Nabatchi and Balogh (2012) frame collaboration as principled engagement, shared motivation and capacity for joint action. These concepts are directly relevant to public-private intelligence. Banks are not merely sensors feeding the State; they hold expertise in transactions, customers, fraud operations and payment controls. Telecom and platform actors likewise contribute data interpretation and disruption capability. Treating them solely as reporting entities weakens the partnership, while allowing them to exercise opaque quasi-policing power without public safeguards creates a different legitimacy problem.

2.4 Socio-technical fusion, source evaluation and noise

A fusion capability is simultaneously legal, organisational, technological and cognitive (Marrin, 2012; Heuer, 1999). Analysts must determine whether records refer to the same entity, whether a source is reliable, whether an association is causal or coincidental, and whether an apparent pattern reflects a fraud network or ordinary behaviour. Heuer (1999) demonstrates how cognitive biases, anchoring and confirmation can distort analysis. Kahneman, Sibony and Sunstein (2021) add the problem of noise: inconsistent judgements across people and organisations. Common data standards are therefore insufficient without common analytical standards, alternative-hypothesis testing, confidence language and review.

Entity resolution is particularly consequential in India's scale and diversity. Names may be transliterated differently; mobile numbers may be reassigned; addresses may be shared; devices may be used by households or businesses; KYC may be outdated or fraudulently obtained; and mule accounts may be controlled by actors other than the named holder. A mature system should distinguish an identifier 'reported in a complaint' from one 'corroborated across independent sources', one 'assessed as controlled by a network' and one 'judicially established'. Source and information grades should travel with the record so that downstream users do not treat a weak allegation as an established fact.

The volume of suspicious reporting can itself reduce effectiveness (Reuter and Truman, 2004; Ferwerda, 2009). Takáts (2011) models the 'crying wolf' problem in which defensive reporting creates too many low-value alerts for authorities to investigate. Levi and Reuter (2006) and Verhage (2011) similarly show that anti-money-laundering systems can become compliance-intensive and professionalised without proportionate enforcement impact. In cyber-fraud, automated risk flags can shift this problem from suspicious transaction reports to transaction

declines, account restrictions and telecom-linked risk labels. Performance should consequently measure precision, incremental analytical value, network discovery, recovery and error correction—not merely the number of alerts, records or accounts shared.

2.5 Accountability as a component of intelligence quality

Accountability is not external friction imposed after operational design; it is a condition of reliable intelligence (Mittelstadt et al., 2016; Zarsky, 2016). Purpose limitation reduces the temptation to reuse weak indicators for unrelated decisions. Access controls and logs deter curiosity searches and enable audit. Retention rules prevent outdated risk from following an individual indefinitely. Human review can distinguish emergency preservation from long-term exclusion. Correction processes supply valuable negative feedback to analytical models. Puttaswamy establishes privacy as a constitutional right and requires legality, legitimate aim and proportionality for State intrusion (Justice K.S. Puttaswamy (Retd.) v Union of India, 2017). The Digital Personal Data Protection Act 2023 and Rules 2025 add a general data-governance framework, though their application, exemptions and phased implementation require careful institution-specific analysis.

The theoretical expectation is therefore fivefold. First, formal sharing is more likely to produce operational intelligence where common tasking and feedback exist. Secondly, increased volume without source evaluation and entity resolution increases noise. Thirdly, public-private fusion is weakened when private contributors receive little operational feedback. Fourthly, centralisation can reduce duplication but increase opacity, mission creep and single-point failure. Fifthly, fusion depends on trained analysts, trust and institutional capacity as much as technical interoperability. These propositions organise the assessment that follows.

3. Methodology

3.1 Design and scope

The study adopts a multi-method documentary institutional case-study design (Bowen, 2009; George and Bennett, 2005; Yin, 2018). It combines: (1) legal and policy analysis; (2) institutional and process mapping; (3) a structured comparison of foreign public-private financial-intelligence mechanisms; and (4) development of a documentary-evidence Fusion Maturity Index and institutional model. The temporal cut-off is 15 July 2026. The geographic

focus is India, with comparative cases selected for design relevance rather than ranking. The unit of analysis is each mechanism's transformation of multi-source information into decision-support and action.

The documentary corpus includes statutes, subordinate legislation, regulatory directions, official annual reports, parliamentary answers, institutional webpages, public manuals, memoranda and press releases, FATF evaluations and guidance, and peer-reviewed literature on intelligence, collaborative governance, financial-crime information sharing, data systems and accountability. The central Indian sources include I4C and Ministry of Home Affairs material on NCRP, CFCFRMS, CFMC, the Suspect Registry and Samanvaya; FIU-IND publications; RBI KYC and fraud-risk directions; DoT material on the Digital Intelligence Platform and FRI; SEBI's cyber-resilience framework; CERT-In directions; and relevant legislation. Comparative sources include NECC and JMLIT+ reports, AUSTRAC's Fintel Alliance material, Europol and EFIPPP guidance, and FinCEN material on Sections 314, FinCEN Exchange and the Rapid Response Program.

Academic and official sources were screened for direct relevance to six themes, using the logic of transparent review and source selection rather than claiming a statistical meta-analysis (Page et al., 2021): intelligence transformation; public-private financial intelligence; network governance; information-flow design; cyber-enabled fraud and mule accounts; and legal or rights safeguards. Official performance figures were treated as institutional claims unless their method, denominator and validation were publicly available. A press release could establish that a mechanism exists, identify its stated participants or report an official outcome, but could not by itself establish analytical quality, causality or maturity. This rule is important where prevented-loss figures may reflect interventions reported by participating entities rather than independently audited counterfactual estimates.

3.2 Process mapping

The institutional map records each actor's mandate, information inputs, holdings, analytical role, outputs, sharing partners, operational powers, feedback and oversight. The information-flow map then follows a complaint or alert across eight functional stages: intake and collection; validation and deduplication; correlation and entity resolution; joint analysis; dissemination and tasking; disruption and recovery; investigation and evidential development; and feedback, correction and learning. At each stage the analysis asks who acts, under what legal or

administrative authority, what information is created, how quickly it must move, and whether the next actor can understand provenance and confidence.

3.3 Comparative method

The foreign cases were compared using common indicators: lead institution; legal basis; participating sectors; membership; co-location and secondments; shared or federated analytical environment; joint tasking; source evaluation; operational and strategic products; public-to-private and private-to-private sharing; feedback; fund interdiction; privacy and correction safeguards; performance reporting; and transferability. The comparison is functional. It does not assume that a model successful in a unitary or differently regulated system can be transplanted into India's federal policing structure and scale. Features are classified as 'transfer', 'adapt' or 'reject' depending on legal fit, administrative capacity and rights risk.

3.4 Documentary-evidence Fusion Maturity Index

The index scores nine dimensions from 0 to 4: common direction; breadth and depth of participation; data standardisation; validation and entity resolution; joint analysis; operational tasking; feedback and correction; legal and privacy governance; and performance measurement and learning. A score represents the maturity demonstrable from public evidence, not a confidential capability assessment. Zero indicates no evidence; one indicates ad hoc or reactive practice; two indicates structured but primarily institution-specific practice; three indicates coordinated and repeatable multi-source practice; and four indicates operational, measured and adaptive fusion. Scores are accompanied by confidence judgements and should be revised through interviews, operational documents and anonymised case reconstructions.

The index has two safeguards against false precision. First, no score rests solely on one press release. Secondly, absence of public evidence is not equated with absence of practice. Where a mechanism may possess non-public controls, the score reflects documentary uncertainty. The index is thus diagnostic: it identifies what public evidence establishes and what empirical research must verify.

3.5 Ethics and limitations

No interviews, personal account information, live operational cases or confidential system details were used. The article does not reverse-engineer FRI scoring or disclose methods that

would facilitate evasion. It relies on aggregate and role-based information. The absence of interviews is a substantive limitation because informal coordination, operational workarounds, case ownership and actual feedback may differ from formal design. Nor can public documents reveal how frequently deeper mule layers are identified, how disputed flags are resolved or how intelligence is converted into admissible evidence. These gaps are reported as unknowns rather than filled by assertion.

A subsequent empirical phase should conduct 12–20 role-based expert interviews and four to six anonymised case reconstructions, subject to ethics and access and reported against the COREQ criteria (Tong, Sainsbury and Craig, 2007). Those materials should test the documentary scores, compare successful and unsuccessful cases, measure latency and examine false-positive correction. The present article is therefore a complete documentary and comparative analysis, but not a substitute for internal operational evaluation. Interview coding should combine the deductive maturity dimensions with inductive thematic analysis (Braun and Clarke, 2006).

4. India's emerging cyber-financial intelligence architecture

4.1 I4C, NCRP, 1930 and CFCFRMS

I4C functions as the principal national coordination node for cybercrime (Indian Cyber Crime Coordination Centre, 2026), while constitutional responsibility for police and public order remains primarily with States and Union Territories. This creates a structurally networked system: a central platform can receive, connect and assist, but State agencies ordinarily convert portal complaints into FIRs, investigate, arrest and prosecute (Ministry of Home Affairs, 2026a). The architecture must therefore solve both sectoral fragmentation and federal fragmentation.

NCRP creates a common citizen-reporting interface. For financial fraud, helpline 1930 and CFCFRMS are designed around speed. The critical operational objective is not immediate proof of the entire offence but rapid identification of the transaction path and preservation of funds before they are layered or withdrawn. CFCFRMS therefore demonstrates one of the clearest differences between intelligence and evidence: a complaint and transaction reference can generate time-sensitive operational communication before a completed criminal investigation. Its official scale—more than 24.65 lakh complaints and over Rs 8,690 crore

reportedly saved by 31 January 2026—suggests a repeatable national process rather than isolated bilateral requests (Ministry of Home Affairs, 2026a).

Yet this process can be mature at one stage and weak at another. Rapid bank notification and fund hold may approach Level 4 operational fusion because information directly informs disruption. The subsequent chain—identification of downstream accounts, attribution of control, interstate allocation, investigation, recovery, charge and feedback—may revert to Levels 1 or 2. A saved amount is a valuable outcome, but it does not by itself show that the system identified the network, corrected erroneous holds, generated an intelligence product or improved future detection.

4.2 Cyber Fraud Mitigation Centre

CFMC is the strongest publicly documented institutional candidate for a fusion node. Its membership spans major banks, financial intermediaries, payment aggregators, telecom service providers, IT intermediaries and State or UT law-enforcement representatives working together for immediate action and seamless cooperation (Ministry of Home Affairs, 2026a). Co-presence can reduce the 'request-and-wait' pattern, permit rapid clarification and allow different sectors to interpret their own data. The design resembles foreign public-private operational cells more than a conventional interdepartmental committee.

Nevertheless, the label 'working together' must be unpacked. Mature fusion would require common intelligence requirements, agreed case-selection criteria, a method for grading sources, the ability to resolve conflicting identity and transaction information, joint analytical products, documented tasking, and feedback on whether actions were correct and useful. Public material does not yet reveal whether CFMC maintains dedicated multidisciplinary analysts, whether members are seconded, how access is segmented, how private information is legally shared, how disputed flags are handled or what independent oversight applies. CFMC can therefore be assessed as demonstrating coordinated operational collaboration, while its adaptive and accountable maturity remains unproven.

4.3 Suspect Registry and mule-account intelligence

The Suspect Registry, launched on 10 September 2024 with banks and financial institutions, represents structured reciprocal sharing rather than a one-way law-enforcement list. By January

2026, banks had supplied more than 23.05 lakh suspect identifiers, and 27.37 lakh Layer-1 mule accounts had been shared with participating entities. The Government associated the registry with declined transactions worth more than Rs 9,518 crore (Ministry of Home Affairs, 2026a). This scale gives institutions a common reference point and may reduce repeated victimisation through known identifiers.

The registry also concentrates the central rights and quality problem, particularly where data-driven policing and surveillance categories become durable institutional facts (Brayne, 2021). 'Suspect identifier' can cover information of very different evidential value: a single complaint, repeated independent complaints, a bank's internal fraud classification, a telecom-derived risk, or an analytically assessed network node. Unless provenance, confidence and reason codes travel with the identifier, a downstream institution may overread the label. Layer-1 mule accounts are operationally useful but analytically limited; the named account holder may be complicit, deceived, coerced, negligent or the victim of identity misuse. A mature registry should therefore distinguish reported, corroborated, assessed and confirmed status; record expiry and review dates; propagate corrections; and measure false positives and false negatives.

4.4 Samanvaya and interstate linkage analysis

Samanvaya is publicly described as a management-information system, data repository and coordination platform for law-enforcement agencies, with analytics identifying interstate links among complaints, crimes and criminals. Its Pratibimb module maps locations of criminals and crime infrastructure, while the platform supports techno-legal assistance. By March 2026, the Government attributed more than 21,857 arrests and 149,636 cyber-investigation assistance requests to this environment (Ministry of Home Affairs, 2026a). Unlike a simple complaint portal, Samanvaya therefore claims an analytical function: connecting cases across State boundaries.

This is a significant fusion indicator because cyber-fraud networks exploit jurisdictional fragmentation. A district may see one victim and one recipient account, while national aggregation reveals repeated devices, numbers, accounts, cash-out points or infrastructure. The unresolved questions concern entity-resolution method, source grading, duplication, access, tasking and causality. An arrest associated with platform assistance does not disclose whether

analytics generated the lead, confirmed an existing suspect or simply facilitated communication. Interviews and reconstructed cases are needed to determine how often a Samanvaya linkage becomes a joint intelligence product and whether the originating States receive outcomes.

4.5 FIU-IND and the AML intelligence system

FIU-IND is the established national financial-intelligence unit, receiving, processing, analysing and disseminating reports under the PMLA framework. Reporting entities submit suspicious transaction reports and other prescribed reports; FIU-IND conducts operational and strategic analysis and disseminates intelligence to competent agencies. FINNET 2.0, risk modelling, dashboards and risk-based STR analysis indicate a mature specialised analytical infrastructure (FIU-IND, 2025). The FATF 2024 mutual evaluation found that Indian authorities routinely access and use financial intelligence and that FIU analysis supports competent authorities, while noting uneven use and lower request levels from some law-enforcement bodies (FATF, APG and EAG, 2024).

Cyber-fraud integration is increasingly explicit. FIU-IND and I4C publicised an MoU to combat cyber fraud and financial crime, while DoT and FIU-IND agreed reciprocal sharing: DoT would provide FRI and mobile-number revocation information, and FIU-IND would share mobile numbers linked to suspicious transaction reports involving cyber-fraud or mule activity (FIU-IND, 2025; Department of Telecommunications and FIU-IND, 2025). This creates a potentially powerful loop between financial reporting and telecom risk.

The loop should not collapse distinct statutory purposes. STRs are confidential intelligence reports, not findings of guilt. Telecom risk is an indicator, not proof. FIU dissemination must remain targeted and legally authorised, and reporting entities require enough feedback to improve detection without receiving protected investigative detail. The most important maturity question is whether cyber-fraud complaints, STRs, telecom indicators and police information are jointly analysed or merely cross-referenced through separate institutional workflows.

4.6 RBI, banks, NPCI and payment actors

Banks and payment actors are simultaneously collectors, analysts and operational decision-

makers. They hold KYC, transaction history, authentication events, device and channel data, beneficiary information, internal fraud alerts and customer communications. They can apply step-up authentication, warnings, limits, delays, restrictions or holds; they can report suspicious activity to FIU-IND; and they interact with I4C, police and other banks. RBI's KYC direction specifically recognises money-mule risks and requires suspicious-transaction reporting, while the 2024 fraud-risk directions emphasise early warning, governance and vigilance for unusual or non-KYC activity (RBI, 2016; RBI, 2024).

Private institutions face competing incentives, a recurrent issue in financial information-sharing partnerships (Maxwell and Artingstall, 2017; Maxwell and Artingstall, 2018). Rapid fraud prevention protects customers and reduces loss, but false positives can create service denial, reputational harm and financial exclusion. Defensive compliance may reward over-reporting or broad account closure. Public agencies may demand data without returning outcomes, leaving institutions unable to calibrate rules. Mature partnership consequently requires structured public-to-private feedback: whether an alert linked to a confirmed fraud, a benign explanation, a deeper network or no actionable result.

4.7 DoT, the Digital Intelligence Platform and FRI

DoT has become a major cyber-financial intelligence contributor by translating telecom misuse data into risk indicators usable by financial actors. The Digital Intelligence Platform, launched in 2024, shares information concerning misuse of telecom resources among stakeholders. By the end of 2025, more than 850 organisations—including MHA, UIDAI, SEBI, FIU-IND, NPCI, central law-enforcement agencies, more than 800 banks and financial institutions, and police from 35 States or Union Territories—were reportedly onboarded. The platform hosts disconnected mobile connections and reasons for disconnection on a near-real-time basis (Department of Telecommunications, 2025b).

FRI adds prioritisation by classifying mobile numbers as medium, high or very high risk using inputs that include NCRP, Chakshu and stakeholder information. Banks, NBFCs and UPI providers may apply warnings, delays, declines or account restrictions according to their own domain analysis. RBI encouraged integration of FRI into banking systems (Department of Telecommunications, 2025a; RBI, 2025). This is a meaningful form of public-to-private operational intelligence because a telecom-derived assessment directly shapes financial controls.

Its maturity depends on governance that is largely non-public. The system should record source composition, confidence, freshness and reason categories; distinguish disconnected numbers from fraud-controlled numbers; account for recycled numbers and identity misuse; and provide rapid correction. Because financial institutions decide action within their own systems, outcomes should be returned to improve FRI. Without feedback, a high-volume risk indicator can remain static or amplify errors across hundreds of institutions. A reciprocal DoT-SEBI arrangement in 2026 extends the approach to securities-market fraud, increasing both analytical potential and the need for common safeguards (Department of Telecommunications and SEBI, 2026).

4.8 SEBI, CERT-In, State police and investigative bodies

SEBI, exchanges, depositories and intermediaries hold data relevant to investment scams, impersonation, account takeover and fraudulent trading platforms. SEBI's Cybersecurity and Cyber Resilience Framework establishes governance and incident-response expectations for regulated entities (SEBI, 2024). Telecom risk exchange can help identify suspicious numbers associated with market fraud, while SEBI-originated identifiers can enrich telecom and financial systems. CERT-In contributes incident reporting, technical indicators and coordination under section 70B of the Information Technology Act 2000 and its 2022 directions (CERT-In, 2022).

State cyber police, police stations, CIDs and Economic Offences Wings remain central because they conduct enquiries and investigations, register offences, use coercive powers, collect devices and records, arrest suspects and build evidential cases. The Enforcement Directorate may enter where PMLA predicates and proceeds are engaged; the Central Bureau of Investigation or other agencies may act according to jurisdiction; prosecutors and courts determine evidential and legal consequences. The March 2026 parliamentary answer records ED use of SAHYOG, Samanvaya, the Cyber Police Portal and the Inter-operable Criminal Justice System, and information sharing through nodal officers and section 66(2) PMLA (Ministry of Home Affairs, 2026a).

The architecture is therefore not one pipeline but an overlapping network. I4C is the operational coordination node for cybercrime; FIU-IND is the financial-intelligence node; sectoral regulators and DoT govern their domains; private entities control high-speed transaction and account interventions; States own most investigation; and courts govern evidential

consequence. The quality of the system lies in how these roles connect without confusing intelligence, regulatory risk, criminal suspicion and proof.

Table 2. Functional map of India's cyber-financial intelligence architecture

Actor / mechanism	**Principal information or function**	**Analytical / operational role**	**Fusion evidence**	**Principal unresolved issue**
I4C / NCRP / 1930 / CFCFRMS	Victim complaints, transaction identifiers, national coordination and rapid reporting.	Routes time-critical information; supports holds, interdiction and State allocation.	Standard national process with measurable operational outputs.	End-to-end feedback from hold to investigation, prosecution and correction.
Cyber Fraud Mitigation Centre	Banks, intermediaries, payment, telecom, IT and State/UT law-enforcement participation.	Immediate clarification, escalation and multi-sector action.	Direct multi-sector operational collaboration.	Analyst model, legal gateways, access design, correction and audit are not publicly detailed.
Suspect Registry	Identifiers supplied by banks and institutions; Layer-1 mule accounts shared with participants.	Screening, transaction decline and risk controls.	Reciprocal, continuing sharing at scale.	Provenance, status categories, expiry, false-positive correction and deeper-network yield.
Samanvaya / Pratibimb	Cybercrime repository, interstate linkages, mapping and assistance requests.	Cross-case analysis and techno-legal support to police.	Documented analytics and interstate visibility.	Causal contribution to cases, entity-resolution standards and outcome feedback.
FIU-IND	STRs and prescribed reports; operational and strategic financial intelligence.	Risk-based analysis and dissemination to competent agencies.	Established specialist FIU with emerging cyber-fraud MoUs.	Repeatable integration of STR, complaint, telecom and investigative data.

RBI, banks, NPCI and payment actors	KYC, transactions, authentication, fraud monitoring, payment routing and account controls.	Detection, reporting, step-up controls, holds, declines and restrictions.	Private entities are both intelligence contributors and operational actors.	Defensive reporting, feedback, proportionality and accountability for high-impact action.
DoT / DIP / FRI	Telecom misuse, disconnected numbers, subscriber or device-linked risk and stakeholder inputs.	Medium/high/very -high risk indicators used for financial warnings, delays, declines or restrictions.	Cross-domain public-to-private operational intelligence.	Scoring provenance, recycled-number risk, review, correction and model learning.
SEBI / CERT-In / State police / ED	Market surveillance, cyber incidents, investigation, proceeds and evidential material.	Sectoral regulation, technical coordination, investigation, arrest and prosecution support.	Multiple documented sharing and portal routes.	Variable capacity, case ownership, evidential conversion and federal coordination.

5. From complaint to intelligence: process and information-flow findings

5.1 Intake and initial validation

A cyber-financial matter may enter through 1930, NCRP, a bank or UPI application, a police station, a telecom or platform report, an STR, or a regulator. The entry route determines available information and speed. A victim report may contain narrative detail but incomplete transaction identifiers. A bank report may contain precise transaction data but limited knowledge of deception. An STR may identify a broader pattern but not a contemporaneous victim. Consistent with criminal-intelligence guidance, the first analytical requirement is therefore not to force every source into the same format (UNODC, 2011), but to establish a common minimum dataset: reporter, time, transaction reference, channel, beneficiary, amount, mobile or digital identifiers, narrative, supporting material and source status.

Rapid validation should separate authentication from truth. Confirming that a transaction occurred does not establish that the beneficiary controlled the fraud; confirming that a number appeared in a complaint does not establish subscriber complicity. Deduplication is essential

because victims may report through several channels, banks may forward the same event, and a single network may generate thousands of reports. A common event identifier and provenance record would reduce inflated counts and repeated action.

5.2 Transaction interdiction and the 'golden window'

CFCFRMS and 1930 are designed to exploit the short period before funds are dissipated. This is the architecture's clearest operational strength. Information travels from the victim or reporting officer to participating financial entities, beneficiary accounts can be identified, and funds may be placed on hold or transactions interrupted. The process aligns with FATF's emphasis on rapid domestic and international cooperation to preserve and return proceeds of cyber-enabled fraud (FATF, 2026).

The operational need for speed creates a proportionality challenge. Emergency action may rest on incomplete information, but delay can make recovery impossible. The appropriate design is therefore a two-stage decision: a short, logged and reviewable preservation action based on defined minimum criteria, followed promptly by enhanced validation and lawful continuation, release or conversion into an investigative measure. Permanent restrictions should not inherit the low threshold justified by an emergency hold.

5.3 Layering, entity resolution and deeper network analysis

After the first account is identified, analysis must move from transaction tracing to entity resolution. Layer-1 accounts may pass funds to further accounts, cash them out, purchase assets or route them through payment aggregators. Multi-source analysis can connect these accounts through common mobile numbers, devices, IP addresses, KYC introducers, addresses, ATM locations, merchants, timing patterns or communication infrastructure. Samanvaya, the Suspect Registry, FIU analysis, bank monitoring and DoT risk indicators each contribute different portions of this picture.

The public evidence is strongest for identification and sharing of Layer-1 mule accounts, and for interstate linkages. It is weaker on how routinely deeper layers and controlling actors are identified. A system focused mainly on recipient accounts risks producing a high volume of low-level account actions while recruiters, controllers, infrastructure providers and proceeds organisers remain less visible. Performance metrics should therefore distinguish accounts

flagged from networks mapped, control relationships assessed, common infrastructure identified and organisers investigated.

Entity resolution also requires negative evidence. A shared device may be a family device; a common IP may be a public network; a common address may be a hostel or business centre; a recycled number may implicate a new subscriber. Analysts should record alternative hypotheses and corroboration thresholds. The system should not convert probabilistic association into categorical designation through repetition across databases.

5.4 Dissemination and operational tasking

Information sharing becomes intelligence only when a recipient knows what decision is required. An effective product should state the question, source provenance, relevant facts, analytical judgement, confidence, caveats, recommended action, legal basis and urgency. A list of account numbers is not equivalent to a network assessment; a risk label without reason or expiry is difficult to use proportionately.

The Indian architecture contains several tasking pathways: banks can hold or decline transactions; telecom actors can disconnect or disengage resources under applicable processes; police can investigate and seek records; regulators can issue directions or commence supervisory action; FIU-IND can disseminate intelligence; and I4C can coordinate. What remains publicly unclear is who sets cross-sector intelligence priorities and who owns a complex case once it spans States, banks, telecom resources and platforms. Joint Cybercrime Coordination Teams and Samanvaya provide coordination mechanisms, but systematic case ownership and escalation criteria require empirical verification.

5.5 Investigation and evidential conversion

Operational intelligence must eventually be converted into evidence where criminal proceedings are contemplated. This requires lawful requests or production, certified electronic records, witness testimony, chain of custody and attribution. Intelligence databases should therefore be separated from evidential repositories, with a documented process for re-acquiring or certifying material. An analyst's confidence assessment can guide investigation but should not become an evidential shortcut.

The distinction also protects intelligence sharing. Private entities may be willing to exchange

risk insights or typologies within lawful partnerships if those insights are not automatically treated as testimonial proof. Conversely, investigators need clarity on what can be disclosed, relied upon or challenged. The Bharatiya Sakshya Adhiniyam 2023 provides the evidential framework for electronic and digital records; operational protocols must connect intelligence leads to compliant collection rather than assuming that a portal entry is court-ready.

5.6 Feedback, correction and closure

Feedback is the least visible stage. The originating bank, telecom provider, platform or analyst should learn whether a supplied identifier was useful, inaccurate, duplicative or linked to a confirmed network. Victims should receive meaningful status information consistent with investigative constraints. Incorrect identifiers should be corrected across downstream systems, not only in the source database. Outcomes should distinguish funds held, funds returned, investigation initiated, network linked, suspect arrested, charge filed, acquittal, closure and correction.

Without feedback, institutions optimise for output rather than accuracy. Banks may continue submitting broad alerts; telecom risk may remain uncalibrated; police may repeat requests; and analysts cannot measure precision. Public reporting currently emphasises complaints, amounts saved, identifiers, accounts, arrests and assistance requests. These are useful but incomplete. Mature reporting should include median latency, percentage of alerts receiving feedback, correction time, deeper-network yield, investigative conversion, recovery, false-positive rate and rights-related complaints.

5.7 Bottlenecks

The principal legal bottlenecks are fragmented gateways, confidentiality, privacy, sector-specific duties and uncertainty about the boundary between voluntary sharing, regulatory obligation and investigative demand. The organisational bottlenecks are competing mandates, variable State capacity, unclear ownership, defensive reporting and uneven trust. Technical bottlenecks include inconsistent identifiers, legacy systems, duplicate records, access controls and the danger of centralising too much sensitive data. Analytical bottlenecks include alert overload, limited source grading, weak alternative-hypothesis testing and insufficient network analysis. Operational bottlenecks include the speed of downstream tracing, interstate handover and conversion from hold to investigation. Accountability bottlenecks include opaque scoring,

uncertain correction, limited public audit and outcome measures dominated by volume.

These problems interact. A legal uncertainty can encourage an organisation to share less or to over-share defensively. Poor feedback can reduce trust and worsen data quality. Weak entity resolution can produce false positives, leading institutions to demand more data, which increases noise. The appropriate response is not simply 'more coordination' but a redesigned cycle with clear requirements, minimum necessary data, confidence labels, decision rights, review and learning.

Figure 1. Current complaint-to-action flow and the principal fusion gaps

Report	**Validate**	**Interdict**	**Trace**	**Analyse**	**Investigate**	**Learn**
1930 / NCRP / bank / STR / telecom	Authenticate, deduplicate, identify transaction	Hold, delay, decline or restrict	Layer-1 and downstream accounts; telecom/ cyber links	Joint network product and confidence	State allocation, evidence, arrest or regulatory action	Outcome feedback, correction and model update
Relatively strong	*Variable source grading*	*Strong time-critical pocket*	*Uneven beyond Layer-1*	*Not consistently visible*	*Variable by jurisdiction and capacity*	*Weakest publicly documented stage*

6. Comparative models and transferability

6.1 United Kingdom: NECC and JMLIT+

The United Kingdom's NECC provides a national system-lead function for economic crime under the wider Economic Crime Plan 2 framework (HM Government, 2023), while JMLIT+ supplies a developed public-private partnership. JMLIT+ includes more than 200 members across law enforcement, regulators, financial institutions, telecommunications, technology, social media, virtual assets, professional services and other sectors. Its Operations Group supports investigations with private-sector information, while public-private threat groups and time-limited cells address defined threats and develop typologies (National Crime Agency, n.d.; National Crime Agency, 2025a).

The transferable lesson is not simply 'create a taskforce'. JMLIT+ combines broad strategic membership with narrower operational groups, allowing participation to vary by problem. The model creates a bridge between threat priorities, specialist expertise and case support. Its reported Data Fusion capability and outcome reporting illustrate the value of targeted datasets and measurable operational outputs. India can adapt the distinction between a permanent strategic partnership, threat groups and time-limited operational cells. It should not transplant UK legal gateways or assume that a central body can direct State police in the same manner.

6.2 Australia: Fintel Alliance

Fintel Alliance is led by AUSTRAC and combines government, law enforcement, national-security, regulatory and private-sector partners. Information sharing is facilitated by staff secondments and partner co-location. Its 2024–25 report describes joint intelligence priorities, working groups and the transition of a Collaborative Analytics Hub from proof of concept to a core function (AUSTRAC, 2025). This is institutionally significant because it embeds private expertise within an intelligence environment rather than treating firms merely as external reporters.

India should transfer the principles of dedicated staffing, secondment, shared project selection and collaborative analytics. Co-location can build trust and accelerate interpretation, but it must be adapted to Indian scale through a national core and accredited State or regional nodes. A model dependent only on physical presence in one city would privilege large institutions and central agencies. Federated virtual collaboration, standard training and rotating secondments are more scalable.

6.3 Europol: EFIPPP

EFIPPP is a transnational public-private mechanism involving Europol, FIUs, investigative authorities and regulated financial institutions. It has historically emphasised structured threat information and typologies, while its 2025 Practical Guide addresses operational cooperation between investigative authorities and financial institutions. The Guide distinguishes strategic sharing from case-specific operational cooperation and identifies legal gateways, governance and trust as prerequisites (Europol, 2025; EFIPPP, 2025).

The principal lesson for India is the need to specify the legal basis and purpose of each sharing

mode. Strategic typologies can often be shared more broadly than personal, case-specific data. Operational exchange requires defined participants, necessity, security and accountability. EFIPPP's cross-border experience also illuminates India's interstate problem: common standards and a trusted coordinating platform can reduce jurisdictional friction without erasing local authority.

6.4 United States: FinCEN, Sections 314 and rapid response

The United States uses several distinct mechanisms rather than one fusion centre. Section 314(a) enables law enforcement, through FinCEN, to ask financial institutions to search for accounts or transactions associated with specified subjects. Section 314(b) provides a voluntary safe harbour for eligible financial institutions to share information with one another to identify and report possible money laundering or terrorist activity, including underlying specified unlawful activity (FinCEN, 2020). FinCEN Exchange convenes public and private actors around priority illicit-finance threats, within a broader financial-intelligence system documented in FinCEN's recent annual reporting (FinCEN, 2026b).

The Rapid Response Program is especially relevant to cyber-enabled fraud because it links victims, financial institutions, US law enforcement, FinCEN and foreign counterparts to interdict and recover funds sent abroad. As at April 2026, FinCEN reported USD 1.8 billion interdicted and more than USD 1 billion recovered for 5,790 victims, across more than 96 foreign jurisdictions (FinCEN, 2026a). The design lesson is a dedicated, time-critical international recovery pathway with clearly defined initiation and counterpart channels.

India can adapt targeted legal gateways and safe-harbour concepts, but broad private-to-private sharing requires caution. A safe harbour should not immunise negligent or discriminatory action, nor permit unrestricted circulation of unverified suspicion. Any Indian mechanism should define eligible entities, permitted purposes, minimum security, provenance, retention, correction and regulatory supervision.

6.5 Comparative synthesis

No model fully resolves accountability. The United States' own fusion-centre guidance therefore treats privacy and civil-liberties capability as foundational rather than optional (Bureau of Justice Assistance, 2006; Department of Homeland Security, 2008). Public-private

intelligence raises questions about democratic control, commercial influence, unequal membership and the movement of State functions into private systems (Petersen and Tjalve, 2017). Fusion centres in the United States have been criticised for mission creep, weak privacy governance and uncertain value (Monahan and Palmer, 2009). India should therefore reject the idea of an unrestricted national data lake, permanent suspicion labels or an opaque central risk score. It should transfer task-focused collaboration, adapt co-location and safe-harbour concepts, and reject governance features that obscure responsibility.

Table 3. Comparative fusion benchmark and transferability

Model	Institutional design	Strong fusion feature	Limitation / safeguard issue	Lesson for India
UK: NECC / JMLIT+	National system lead plus 200+ member public-private partnership; threat groups and time-limited cells.	Defined threat priorities, operational case support and broad sector expertise.	Membership, gateways and central coordination depend on UK legal and administrative conditions.	Adapt permanent strategic partnership plus narrow, time-limited operational cells.
Australia: Fintel Alliance	AUSTRAC-led alliance using co-location, secondments, joint priorities and collaborative analytics.	Private expertise is embedded in analytical work rather than confined to reporting.	Physical co-location and resource intensity may not scale nationally.	Transfer secondments and dedicated analysts; adapt through national and State nodes.
Europol: EFIPPP	Transnational partnership among Europol, FIUs, investigators and regulated financial institutions.	Clear distinction between strategic threat sharing and case-specific operational coperation.	Cross-border legal diversity constrains operational exchange.	Use a legal-gateway matrix and separate typologies from identifiable case data.
US: FinCEN / Sections 314 / RRP	Targeted queries, voluntary safe harbour, public-private exchange and rapid international recovery.	Defined initiation channels and time-critical cross-border interdiction.	Safe harbours can encourage over-sharing unless purpose, eligibility and accountability are narrow.	Adapt rapid-response channels and narrowly tailored safe harbour; reject unrestricted circulation.

7. Is India sharing information or producing intelligence?

7.1 Documentary maturity assessment

The documentary-evidence index places the architecture between structured information sharing and coordinated analysis, with specific mechanisms approaching operational fusion. The overall conclusion is not an arithmetic fact but a synthesis of uneven components. CFMC scores highest because it brings diverse actors into an immediate-action environment. CFCFRMS scores strongly on tasking and disruption but less strongly on downstream feedback and correction. Samanvaya shows analytical and interstate linkage functions. FIU-IND has mature specialised analysis but publicly documented cyber-fraud integration remains emergent. FRI demonstrates cross-domain operational use but limited public detail on validation and correction. The State investigation chain is the least uniform because capacity, latency and case ownership vary.

Table 4. Documentary-evidence Fusion Maturity Index (0–4)

Mechanism	Strongest documented dimensions	Weakest / unknown dimensions	Mean score	Confidence / continuum interpretation
CFCFRMS / 1930	Standardisation, speed, operational tasking and fund preservation.	Downstream analysis, feedback, correction and evidential outcomes.	2.67	Moderate-high; Level 3 with Level 4 interdiction features.
Cyber Fraud Mitigation Centre	Breadth of participation, direct communication and immediate multi-sector action.	Source grading, access design, independent audit and adaptive learning.	2.78	Moderate; strongest candidate for operational fusion.
Suspect Registry	Continuous reciprocal sharing, common identifiers and transaction controls.	Provenance, expiry, false-positive correction and network-depth measures.	2.44	Moderate; strong Level 2, some Level 3 features.
Samanvaya / Pratibimb	Interstate link analysis, mapping and investigative assistance.	Common analytical doctrine, causality, feedback and public audit.	2.67	Moderate; coordinated-analysis capability.

FIU-IND cyber integration	Specialist financial analysis, statutory reporting and dissemination.	Degree of routine joint cyber-financial analysis and feedback to contributors.	2.67	Moderate; mature FIU, emerging cross-domain fusion.
DoT FRI / DIP	Large participation, cross-domain indicators and direct preventive use.	Scoring transparency, correction, feedback, drift and rights metrics.	2.67	Moderate; operational intelligence, accountability not yet demonstrable.
State investigation chain	Formal jurisdiction, investigative powers and access to national platforms.	Uniform capacity, case ownership, latency, deeper-layer tracing and closure feedback.	1.78	Low-moderate; reactive to structured sharing, variable by State.
Architecture overall	National intake, shared registries, specialised nodes, analytics and tasking.	System-wide feedback, correction, common doctrine, oversight and learning.	2.53	Moderate; boundary of Levels 2 and 3, with pockets at Level 4.

The aggregate mean of the illustrative scores is approximately 2.53 on a four-point dimensional scale. This should be read as 'repeatable structured sharing with material coordinated-analysis capability', not as a league-table grade. On the six-level continuum, India lies around the boundary between Level 2 and Level 3, with pockets at Level 4. Confidence is moderate because the existence, membership and outputs of major mechanisms are documented, while internal analytical processes and rights controls are not.

7.2 Where India has moved beyond exchange

India has moved beyond reactive exchange in at least five respects. First, 1930 and CFCFRMS create a standard national process for rapid reporting and fund preservation. Secondly, CFMC brings financial, telecom, technology and policing actors into a common operational setting. Thirdly, the Suspect Registry establishes continuous reciprocal sharing with private entities. Fourthly, Samanvaya performs analytics across complaints and States rather than merely storing records. Fifthly, FRI converts telecom-derived risk into financial decision-support at scale. These are meaningful institutional innovations and should not be dismissed because the system is incomplete.

The architecture also displays network-governance adaptation. I4C does not formally replace FIU-IND, regulators, banks or State police; it provides a coordination layer. MoUs connect domains without attempting a wholesale merger. This is appropriate because expertise and legal authority remain distributed. The direction of development is therefore towards a hybrid network administrative organisation with sectoral analytical nodes.

7.3 Where fragmentation remains

The architecture remains fragmented where the output of one mechanism becomes the input of another without a shared analytical frame. A complaint may generate a hold, but the bank, I4C and State police may retain different case identifiers. A telecom risk may influence a bank decision without disclosing sufficient provenance for proportional action. An STR may reach a competent agency without linking to victim complaints or portal data in a repeatable way. A State may investigate one fragment without visibility of related cases or without resources to pursue deeper layers.

The constitutional distribution of policing makes this more than a technical problem. State ownership is necessary for lawful investigation and local accountability, yet national networks require cross-jurisdictional prioritisation. The solution is not central takeover but common case identifiers, escalation thresholds, joint analytical support, lead-State or joint-team protocols and reciprocal reporting.

7.4 Analytical capacity and source quality

Public material demonstrates analytics but not a common analytical doctrine. There is little public evidence of a national source-grading system, standard confidence language, alternative-hypothesis requirements or common entity-resolution thresholds. Different institutions may use sophisticated internal methods, but their outputs can lose context when shared. A ‘high-risk’ mobile number, a ‘suspect’ identifier, an STR subject and an accused person are not equivalent categories. Fusion should preserve these distinctions.

Analytical capacity is also a workforce issue. Technology can surface connections, but trained analysts must interpret them, identify bias, understand financial products and telecom systems, and communicate uncertainty. India’s scale requires a professional cyber-financial intelligence analyst cadre spanning I4C, FIU-IND, State nodes and seconded sector experts. Training

should include transaction and network analysis, digital evidence, intelligence writing, privacy, and the difference between investigative lead and proof.

7.5 Feedback and private-sector partnership

The architecture's public-private participation is substantial, but partnership maturity depends on feedback. Banks and telecom actors appear to supply large volumes of identifiers and act on government risk information. Public evidence is less clear on whether they receive case outcomes, precision measures or reasons for correction. One-way extraction can erode trust and encourage defensive compliance. Foreign models show that joint threat groups, secondments and operational cells provide a richer form of participation than periodic reporting.

India should therefore classify feedback into operational, analytical and governance layers. Operational feedback tells a contributor whether action was taken. Analytical feedback indicates whether an alert was accurate and what additional pattern was found. Governance feedback publishes aggregate precision, correction, latency and outcome data. Each layer can protect sensitive investigations while improving the system.

7.6 Accountability maturity

The Digital Personal Data Protection framework, sectoral regulation, criminal procedure, constitutional privacy and internal controls supply a legal environment, but the specific governance of cross-sector risk indicators remains underdeveloped in public documentation. Key questions include retention, downstream deletion, access logs, independent audit, challenge and whether an institution can make a high-impact decision solely from a shared label. The absence of public answers does not prove absence of controls, but it prevents a Level 5 assessment.

The system's own operational interests support stronger accountability. A corrected false positive is labelled data for model improvement. An audit trail enables incident response and attribution of misuse. Time-limited designations reduce stale risk. Published aggregate metrics build legitimacy and allow Parliament, regulators and researchers to distinguish harm reduction from activity counts.

8. An Indian Cyber-Financial Intelligence Fusion Model

8.1 Institutional form

The proposed model is a federated network administrative organisation led operationally by I4C for cyber-fraud coordination, with FIU-IND retaining statutory authority and analytical control over financial-intelligence reporting. It also reflects global guidance favouring lawful, risk-based and protected public-private information sharing rather than indiscriminate pooling (FATF, 2017; FATF, 2021; FATF, 2022). It does not create a new agency. Instead, it formalises a permanent Cyber-Financial Intelligence Fusion Board, a national analytical and operational core, accredited State fusion nodes and time-limited threat or case cells. RBI, DoT, SEBI, NPCI or relevant payment-system operators, CERT-In, designated banks and financial institutions, major payment intermediaries, State police representatives and other competent agencies participate according to role and case need.

The Board should approve intelligence priorities, minimum standards, legal gateways, safeguards and performance measures. The national core should maintain common case identifiers, coordination tools, standards and network-level analysis. Sectoral data should remain federated wherever possible. Institutions would expose verified attributes, query responses or derived risk information through controlled interfaces rather than contributing unrestricted copies to a central lake. Case cells would receive only the data necessary for an approved purpose.

8.2 Eight-stage fusion cycle

The first stage is direction and intelligence requirements. The Board should publish classified and unclassified priorities, such as digital-arrest fraud, investment scams, business email compromise, mule recruitment or high-risk cash-out corridors. Each priority should identify questions, decision-makers, collection gaps and review dates. Direction prevents the system from becoming a passive accumulation of all available data.

The second stage is collection and reporting. Inputs include victim complaints, STRs, bank fraud alerts, transaction and payment records, telecom indicators, market surveillance, cyber incident indicators and investigative information. Every record should carry source, time, legal basis, purpose, quality status and retention category. A common event identifier should link

duplicate reports without erasing source differences.

The third stage is validation and source evaluation. Automated checks should verify format, timestamps and duplicates; human or institution-led checks should assess source reliability. A standard matrix could grade the source and the information separately. Records should use confidence bands such as confirmed, highly probable, probable, possible, unverified or contradicted. A reported identifier should not become 'confirmed' through mere repetition of the same source.

The fourth stage is correlation and entity resolution. Privacy-preserving matching should connect accounts, mobile numbers, devices, IPs, merchants, companies, beneficial owners, addresses and cash-out points. Matching rules should account for recycled numbers, shared infrastructure, transliteration and identity theft. High-impact associations should require independent corroboration or documented review.

The fifth stage is joint analysis. Multidisciplinary teams should produce transaction graphs, network assessments, typologies, geographic analysis and threat reports. Products should identify alternative hypotheses, gaps and confidence. Strategic products can be distributed broadly; operational products should be compartmented to authorised participants.

The sixth stage is dissemination and operational tasking. Each product should specify the recipient, requested decision, urgency, authority and review period. Possible actions include transaction delay or hold, enhanced authentication, account restriction, telecom intervention, police investigation, regulatory action or international request. A RACI matrix should identify who is responsible, accountable, consulted and informed. I4C should coordinate, not silently exercise powers belonging to banks, regulators or police.

The seventh stage is disruption, recovery and evidential development. Emergency actions should be time-bound and reviewed. Investigators should convert intelligence into lawfully acquired and authenticated evidence. Cross-border cases should use a dedicated rapid-response channel through FIU and law-enforcement counterparts. Outcomes should distinguish preservation, return, asset tracing, arrest, charge, conviction and acquittal.

The eighth stage is feedback, correction and learning. Every operational product should generate a closure code and feedback record. Incorrect identifiers should be corrected at source

and propagated to recipients. Detection rules and priorities should be recalibrated using verified outcomes. Analysts should receive case lessons; institutions should receive typology and precision feedback; the public should receive aggregate reporting; and an independent oversight mechanism should review access, error and rights impact.

Table 5. Proposed eight-stage Indian Cyber-Financial Intelligence Fusion Cycle

Stage	**Principal activity**	**Mandatory governance control**	**Illustrative performance measure**
1. Direction	Set threat priorities, intelligence requirements, gaps and decision owners.	Board approval, defined purpose and review date.	Priority coverage; unanswered intelligence gaps.
2. Collection	Receive complaints, STRs, bank, payment, telecom, cyber, market and investigative inputs.	Common event ID, provenance, legal basis and minimisation.	Completeness; duplicate rate; reporting latency.
3. Validation	Authenticate records, deduplicate and grade source and information.	Separate source and information confidence; record contradictions.	Validation time; verified-error rate.
4. Correlation	Resolve accounts, phones, devices, IPs, merchants, companies and ownership.	Independent corroboration for high-impact associations.	Entity-resolution precision; network-depth yield.
5. Joint analysis	Produce graphs, typologies, threat assessments and case products.	Alternative hypotheses, caveats, compartmentation and analyst accreditation.	Actionable product rate; analytical review score.
6. Tasking	Direct holds, authentication, telecom, regulatory, investigative or international action.	Named decision-maker, authority, urgency and review period.	Dissemination-to-action latency; action completion.
7. Disruption and evidence	Preserve and recover funds, investigate networks and lawfully acquire evidence.	Time-bound emergency action; separate intelligence and evidence stores.	Funds preserved/returned; investigation and prosecution conversion.
8. Feedback and learning	Close outcomes, correct errors, recalibrate rules and publish aggregate metrics.	Correction propagation, independent audit and rights-impact review.	Feedback completion; correction time; repeat failure reduced.

8.3 Legal gateways and data-access hierarchy

The model should use a legal-gateway matrix rather than a blanket 'sharing authority'. Each flow should identify origin, recipient, information category, purpose, legal basis, necessity, retention and review. Four access tiers are appropriate. Tier 1 contains strategic and anonymised typologies. Tier 2 contains pseudonymised or tokenised attributes for matching. Tier 3 contains identifiable operational intelligence for a defined case or threat. Tier 4 contains evidential material acquired under criminal procedure or regulatory authority. Movement between tiers should be logged and justified.

A carefully drafted statutory or regulatory safe harbour may be required for limited private-to-private cyber-fraud sharing, especially for common mule networks. It should protect good-faith, standards-compliant sharing while preserving liability for misuse, discrimination, gross negligence and security failure. Participation should be limited to regulated entities, approved purposes and audited channels. Nothing in the safe harbour should make a shared alert conclusive proof or authorise permanent exclusion without review.

8.4 Human review and challenge

High-impact action should use a 'human review plus recorded reason' rule, consistent with the broader administrative-law concern that consequential automated classifications remain reviewable and explainable (Zarsky, 2016). Automation may prioritise and temporarily protect funds, but continued restriction, account exit or cross-sector designation should require review proportionate to impact. The reviewer should see provenance and confidence, not only a risk score. An emergency action can precede notice where notice would frustrate the purpose, but prompt review and a grievance route should follow where legally and operationally possible.

The correction mechanism should allow individuals and institutions to contest inaccurate identifiers without demanding disclosure of sensitive methods. A specialised review unit could verify identity misuse, recycled numbers, mistaken account linkage or resolved cases. Corrections must propagate through the registry and participating systems. The model should record both the original decision and correction for audit, while preventing continued operational use of invalidated data.

8.5 Performance measurement

The model should replace record-volume success with a balanced scorecard. Input measures include participating institutions, trained analysts and usable data sources. Process measures include complaint-to-bank latency, data completeness, duplicate rate, entity-resolution rate, product time and feedback completion. Output measures include actionable leads, linked accounts, mapped networks, disrupted transactions and investigative referrals. Outcome measures include funds preserved and returned, repeat victimisation reduced, networks dismantled, prosecutions supported and controls improved.

Quality and rights measures are equally important: false-positive rate, correction time, unauthorised access, audit findings, retention compliance, complaints, disparate impact and financial-exclusion effects. Learning measures include typologies revised, detection rules changed, training issued and repeat failures reduced. Metrics should be disaggregated by mechanism and fraud type, because a single national average can conceal weak stages or vulnerable groups.

8.6 Implementation roadmap

Implementation should occur in four phases. Phase 1 should standardise vocabulary, common case identifiers, provenance, confidence labels, closure codes and a legal-gateway matrix across existing mechanisms. Phase 2 should create secondments, analyst accreditation, State-node pilots and structured feedback for selected fraud types. Phase 3 should deploy federated entity-resolution services, audited case cells and a correction portal. Phase 4 should establish independent audit, publish aggregate performance and rights metrics, and consider any narrowly tailored legislative safe harbour based on pilot evidence.

The roadmap is deliberately incremental. India already possesses substantial infrastructure; the principal need is to connect direction, analytical doctrine, tasking and learning. A new central agency would create delay, duplication and institutional resistance. Strengthening I4C as a governed coordination node while preserving FIU-IND, regulator and State powers is more feasible and consistent with network-governance theory.

9. Risks, safeguards and research limitations

The first risk is false positive and financial exclusion. Cyber-fraud controls operate at speed

and can affect persons who are victims of identity misuse, unwitting mule recruitment or inaccurate linkage. A permanent or widely distributed 'suspect' label can restrict banking, telecom and market access without a criminal finding. Safeguards must therefore include confidence labels, time limits, independent corroboration for high-impact action, human review, correction and aggregate error reporting.

The second risk is mission creep. Data collected to stop an urgent fraud may later be used for unrelated surveillance, credit decisions, employment screening or broad law-enforcement fishing. Purpose limitation, role-based access, query auditing and tiered gateways should be technically enforced. Strategic analysis should favour anonymised or aggregated data; identifiable case information should be accessed only for approved requirements.

The third risk is security concentration. A central repository of linked financial, telecom, identity and cyber data would be an exceptionally valuable target. Federated design, tokenisation, data minimisation, segmentation, zero-trust access, security testing and incident reporting reduce this risk. Access logs should be immutable and reviewed by an independent function.

The fourth risk is institutional capture and unequal partnership. Large banks and technology firms may have greater capacity to shape priorities than smaller entities, while private risk models may become embedded in public decisions without scrutiny. Governance should include transparent membership criteria, rotating representation, conflict declarations and regulator-led standards. Private partners should contribute expertise but should not determine criminal priorities or evidential conclusions.

The fifth risk is analytical opacity. Machine-learning or rules-based systems may encode proxy discrimination, historical reporting bias or self-reinforcing feedback. A number heavily reported because it was previously flagged may appear increasingly risky even if the original flag was weak. Models should be tested for calibration, drift and disparate impact. Analysts should be able to explain the material factors behind an operational recommendation.

The sixth risk is confusing interdiction with justice. Declining a transaction or holding an account can prevent harm, but it does not identify the controller, establish mens rea or support conviction. Performance incentives should not encourage mass account closure at the expense of network investigation. Intelligence and evidence systems should remain separate, with

explicit conversion and disclosure processes.

The study's own limits are significant. Public sources cannot reveal classified or protected procedures, internal case data, precise access controls or all informal coordination. Official figures may use different methodologies and are not uniformly independently audited. The maturity scores are therefore transparent hypotheses based on documentary evidence, not definitive institutional ratings. Interviews with police, I4C, FIU, banks, telecom, payment actors, regulators, prosecutors and digital-forensics professionals are required. Anonymised case reconstructions should compare successful interdictions, delayed cases, false positives and deeper-network investigations.

Future research should also examine State variation, rural and linguistic access, the experience of small financial institutions, cross-border recovery, market and crypto-related fraud, and the relationship between cyber-fraud intelligence and PMLA investigation. A longitudinal study should test whether the January 2026 SOP for NCRP-CFCFRMS improves uniformity, feedback and victim outcomes.

10. Conclusion

India possesses more than a collection of disconnected databases. It has created national reporting and fund-interdiction processes, a multi-sector mitigation centre, reciprocal suspect and mule-account sharing, interstate analytical platforms, a mature financial-intelligence unit, telecom-financial risk indicators and growing sectoral MoUs. These mechanisms demonstrate a substantive transition from institutional isolation and reactive requests towards structured sharing and coordinated analysis. In time-sensitive parts of the system, particularly transaction preservation and multi-sector immediate action, the architecture contains pockets of operational fusion.

It does not yet amount, on publicly available evidence, to a uniformly mature cyber-financial intelligence fusion system. The missing or insufficiently documented features are common intelligence requirements, standard provenance and confidence, transparent entity resolution, repeatable joint intelligence products across all major domains, case ownership, downstream feedback, false-positive correction, independent audit and learning from investigation and adjudication. The overall architecture therefore lies near the boundary between structured sharing and coordinated analysis rather than at adaptive and accountable fusion.

The proposed Indian Cyber-Financial Intelligence Fusion Model builds on existing institutions rather than replacing them. It treats I4C as the network administrative and operational coordination node, FIU-IND as the statutory financial-intelligence node, State police as principal investigators, regulators and sector actors as domain authorities, and private institutions as governed analytical partners. It uses federated data access, common intelligence requirements, accredited analysts, time-limited cells, tiered legal gateways, source grading, human review, correction and a balanced performance scorecard.

Three immediate reforms are feasible without creating a new agency: a common provenance-confidence-closure standard across I4C-connected mechanisms; mandatory structured feedback and correction for shared identifiers; and publication of aggregate latency, precision, recovery, deeper-network and rights metrics. The next empirical phase should validate the documentary maturity scores through expert interviews and anonymised case reconstruction. The decisive question for 2026–2030 is no longer whether Indian institutions can exchange information. It is whether they can transform that exchange into intelligence that is timely enough to prevent harm, precise enough to direct investigation, and accountable enough to deserve trust.

Research transparency statement. *This manuscript reports a documentary, legal and comparative assessment. It does not claim that interviews or confidential case reconstructions were conducted. All maturity scores are evidence-bounded and expressly provisional pending field validation.*

References

1. Agranoff, R. and McGuire, M. (2003) *Collaborative Public Management: New Strategies for Local Governments*. Washington, DC: Georgetown University Press.

2. Ansell, C. and Gash, A. (2008) 'Collaborative governance in theory and practice', *Journal of Public Administration Research and Theory*, 18(4), pp. 543–571. doi:10.1093/jopart/mum032.

3. AUSTRAC (2025) *Fintel Alliance Annual Report Extract 2024–25*. Canberra: Australian Transaction Reports and Analysis Centre. Accessed 15 July 2026.

4. Bowen, G.A. (2009) 'Document analysis as a qualitative research method', *Qualitative Research Journal*, 9(2), pp. 27–40. doi:10.3316/QRJ0902027.

5. Brayne, S. (2021) *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York: Oxford University Press.

6. Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101. doi:10.1191/1478088706qp063oa.

7. Bryson, J.M., Crosby, B.C. and Stone, M.M. (2006) 'The design and implementation of cross-sector collaborations', *Public Administration Review*, 66(s1), pp. 44–55. doi:10.1111/j.1540-6210.2006.00665.x.

8. Bureau of Justice Assistance (2006) *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: US Department of Justice.

9. CERT-In (2022) *Directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents under section 70B(6) of the Information Technology Act, 2000*, 28 April. New Delhi: Indian Computer Emergency Response Team.

10. Clark, R.M. (2019) *Intelligence Analysis: A Target-Centric Approach*. 6th edn. Thousand Oaks, CA: CQ Press.

11. Department of Homeland Security (2008) *Baseline Capabilities for State and Major Urban Area Fusion Centers*. Washington, DC: US Department of Homeland Security.

12. Department of Telecommunications (2025a) 'Financial Fraud Risk Indicator: a new tool to curb cyber fraud', 21 May. New Delhi: Ministry of Communications. Accessed 15 July 2026.

13. Department of Telecommunications (2025b) *2025 Year End Review for Department of Telecommunications*, 19 December. New Delhi: Ministry of Communications. Accessed 15 July 2026.

14. Department of Telecommunications and FIU-IND (2025) 'DoT and Financial Intelligence Unit-India sign MoU to strengthen efforts against telecom-enabled cybercrime and financial fraud', 25 September. New Delhi: Government of India.

15. Department of Telecommunications and SEBI (2026) 'DoT and SEBI sign MoU for exchange of telecom and securities-market fraud intelligence', 15 April. New Delhi: Government of India.

16. EFIPPP (2025) *EFIPPP Annual Report 2024*. The Hague: Europol Financial Intelligence Public Private Partnership. Accessed 15 July 2026.

17. Emerson, K., Nabatchi, T. and Balogh, S. (2012) 'An integrative framework for collaborative governance', *Journal of Public Administration Research and Theory*, 22(1), pp. 1–29. doi:10.1093/jopart/mur011.

18. Europol (2025) *EFIPPP Practical Guide for Operational Cooperation between Investigative Authorities and Financial Institutions*. The Hague: Europol. Accessed 15 July 2026.

19. FATF (2017) *Private Sector Information Sharing: Role of Financial Institutions and Law Enforcement*. Paris: Financial Action Task Force.

20. FATF (2021) *Stocktake on Data Pooling, Collaborative Analytics and Data Protection*. Paris: Financial Action Task Force.

21. FATF (2022) *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*. Paris: Financial Action Task Force.

22. FATF, APG and EAG (2024) *Anti-Money Laundering and Counter-Terrorist Financing Measures: India Mutual Evaluation Report*. Paris: Financial Action Task Force.

23. FATF (2026) *Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks*. Paris: Financial Action Task Force.

24. Ferwerda, J. (2009) 'The economics of crime and money laundering: does anti-money laundering policy reduce crime?', *Review of Law & Economics*, 5(2), pp. 903–929. doi:10.2202/1555-5879.1421.

25. Financial Crimes Enforcement Network (2020) *Section 314(b) Fact Sheet*. Washington, DC: US Department of the Treasury.

26. Financial Crimes Enforcement Network (2026a) *Rapid Response Program Fact Sheet*, 15 April. Washington, DC: US Department of the Treasury.

27. Financial Crimes Enforcement Network (2026b) *Year in Review: Fiscal Year 2025*. Washington, DC: US Department of the Treasury.

28. Financial Crimes Enforcement Network (n.d.) *FinCEN Exchange*. Washington, DC: US Department of the Treasury. Accessed 15 July 2026.

29. Financial Intelligence Unit-India (2025) *Annual Report 2024–25*. New Delhi: Department of Revenue, Ministry of Finance.

30. George, A.L. and Bennett, A. (2005) *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

31. Gill, P. and Phythian, M. (2018) *Intelligence in an Insecure World*. 3rd edn. Cambridge: Polity.

32. Government of India (2000) *Information Technology Act 2000*. New Delhi: Government of India.

33. Government of India (2002) *Prevention of Money Laundering Act 2002*. New Delhi: Government of India.

34. Government of India (2023a) *Digital Personal Data Protection Act 2023*. New Delhi: Government of India.

35. Government of India (2023b) *Bharatiya Sakshya Adhiniyam 2023*. New Delhi: Government of India.

36. Government of India (2023c) *Bharatiya Nagarik Suraksha Sanhita 2023*. New Delhi: Government of India.

37. Government of India (2025) *Digital Personal Data Protection Rules 2025*. *Gazette of India*, 13 November. New Delhi: Government of India.

38. Heuer, R.J. Jr (1999) *Psychology of Intelligence Analysis*. Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence.

39. HM Government (2023) *Economic Crime Plan 2: 2023–2026*. London: HM Government.

40. Hulnick, A.S. (2006) 'What's wrong with the intelligence cycle', *Intelligence and National Security*, 21(6), pp. 959–979. doi:10.1080/02684520601046291.

41. Indian Cyber Crime Coordination Centre (2026) *About I4C*. New Delhi: Ministry of Home Affairs. Accessed 15 July 2026.

42. *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1 (Supreme Court of India).

43. Kahneman, D., Sibony, O. and Sunstein, C.R. (2021) *Noise: A Flaw in Human Judgment*. New York: Little, Brown Spark.

44. Levi, M. and Reuter, P. (2006) 'Money laundering', *Crime and Justice*, 34(1), pp. 289–375. doi:10.1086/501508.

45. Marrin, S. (2012) 'Is intelligence analysis an art or a science?', *International Journal of Intelligence and CounterIntelligence*, 25(3), pp. 529–545. doi:10.1080/08850607.2012.678690.

46. Maxwell, N.J. and Artingstall, D. (2017) *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*. London: Royal United Services Institute.

47. Maxwell, N.J. and Artingstall, D. (2018) *Expanding the Capability of Financial Information-Sharing Partnerships*. London: Royal United Services Institute.

48. Ministry of Home Affairs (2026a) *Lok Sabha Unstarred Question No. 5184: Measures to Combat Cyber Fraud*, answered 24 March 2026. New Delhi: Government of India.

49. Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L. (2016) 'The ethics of algorithms: mapping the debate', *Big Data & Society*, 3(2), pp. 1–21. doi:10.1177/2053951716679679.

50. Monahan, T. and Palmer, N.A. (2009) 'The emerging politics of DHS fusion centers', *Security Dialogue*, 40(6), pp. 617–636. doi:10.1177/0967010609350314.

51. National Crime Agency (2025a) *National Economic Crime Centre Annual Report 2024–25*. London: National Crime Agency.

52. National Crime Agency (n.d.) *National Economic Crime Centre and Joint Money Laundering Intelligence Taskforce*. London: National Crime Agency. Accessed 15 July 2026.

53. National Payments Corporation of India (n.d.) *Unified Payments Interface: Product and Participant Information*. Mumbai: NPCI. Accessed 15 July 2026.

54. Ostrom, E. (2010) 'Beyond markets and states: polycentric governance of complex economic systems', *American Economic Review*, 100(3), pp. 641–672. doi:10.1257/aer.100.3.641.

55. Page, M.J. et al. (2021) 'The PRISMA 2020 statement: an updated guideline for reporting systematic reviews', *BMJ*, 372, n71. doi:10.1136/bmj.n71.

56. Petersen, K.L. and Tjalve, V.S. (2017) 'Intelligence expertise in the age of information sharing: public–private "collection" and its challenges to democratic control and accountability', *Intelligence and National Security*, 32(1), pp. 21–35. doi:10.1080/02684527.2017.1316956.

57. Powell, W.W. (1990) 'Neither market nor hierarchy: network forms of organization', *Research in Organizational Behavior*, 12, pp. 295–336.

58. Provan, K.G. and Kenis, P. (2008) 'Modes of network governance: structure, management, and effectiveness', *Journal of Public Administration Research and Theory*, 18(2), pp. 229–252. doi:10.1093/jopart/mum015.

59. Ratcliffe, J.H. (2016) *Intelligence-Led Policing*. 2nd edn. London: Routledge.

60. Reserve Bank of India (2016, updated 2025) *Master Direction – Know Your Customer (KYC) Direction*. Mumbai: RBI.

61. Reserve Bank of India (2024) *Master Directions on Fraud Risk Management in Commercial Banks (including Regional Rural Banks) and All India Financial Institutions*. Mumbai: RBI.

62. Reserve Bank of India (2025) *Advisory on integration of the Department of Telecommunications Financial Fraud Risk Indicator into regulated entities' systems*, 2 July. Mumbai: RBI.

63. Reuter, P. and Truman, E.M. (2004) *Chasing Dirty Money: The Fight Against Money Laundering*. Washington, DC: Peterson Institute for International Economics.

64. SEBI (2024) *Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities*. Mumbai: Securities and Exchange Board of India.

65. Takáts, E. (2011) 'A theory of "crying wolf": the economics of money laundering enforcement', *Journal of Law, Economics, & Organization*, 27(1), pp. 32–78. doi:10.1093/jleo/ewp018.

66. Thomson, A.M. and Perry, J.L. (2006) 'Collaboration processes: inside the black box', *Public Administration Review*, 66(s1), pp. 20–32. doi:10.1111/j.1540-6210.2006.00663.x.

67. Tong, A., Sainsbury, P. and Craig, J. (2007) 'Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups', *International Journal for Quality in Health Care*, 19(6), pp. 349–357. doi:10.1093/intqhc/mzm042.

68. UNODC (2011) *Criminal Intelligence: Manual for Analysts*. New York: United Nations Office on Drugs and Crime.

69. Verhage, A. (2011) *The Anti Money Laundering Complex and the Compliance Industry*. London: Routledge.

70. Yin, R.K. (2018) *Case Study Research and Applications: Design and Methods*. 6th edn. Thousand Oaks, CA: Sage.

71. Zarsky, T. (2016) 'The trouble with algorithmic decisions: an analytic road map to examine efficiency and fairness in automated and opaque decision making', *Science, Technology, & Human Values*, 41(1), pp. 118–132. doi:10.1177/0162243915605575.