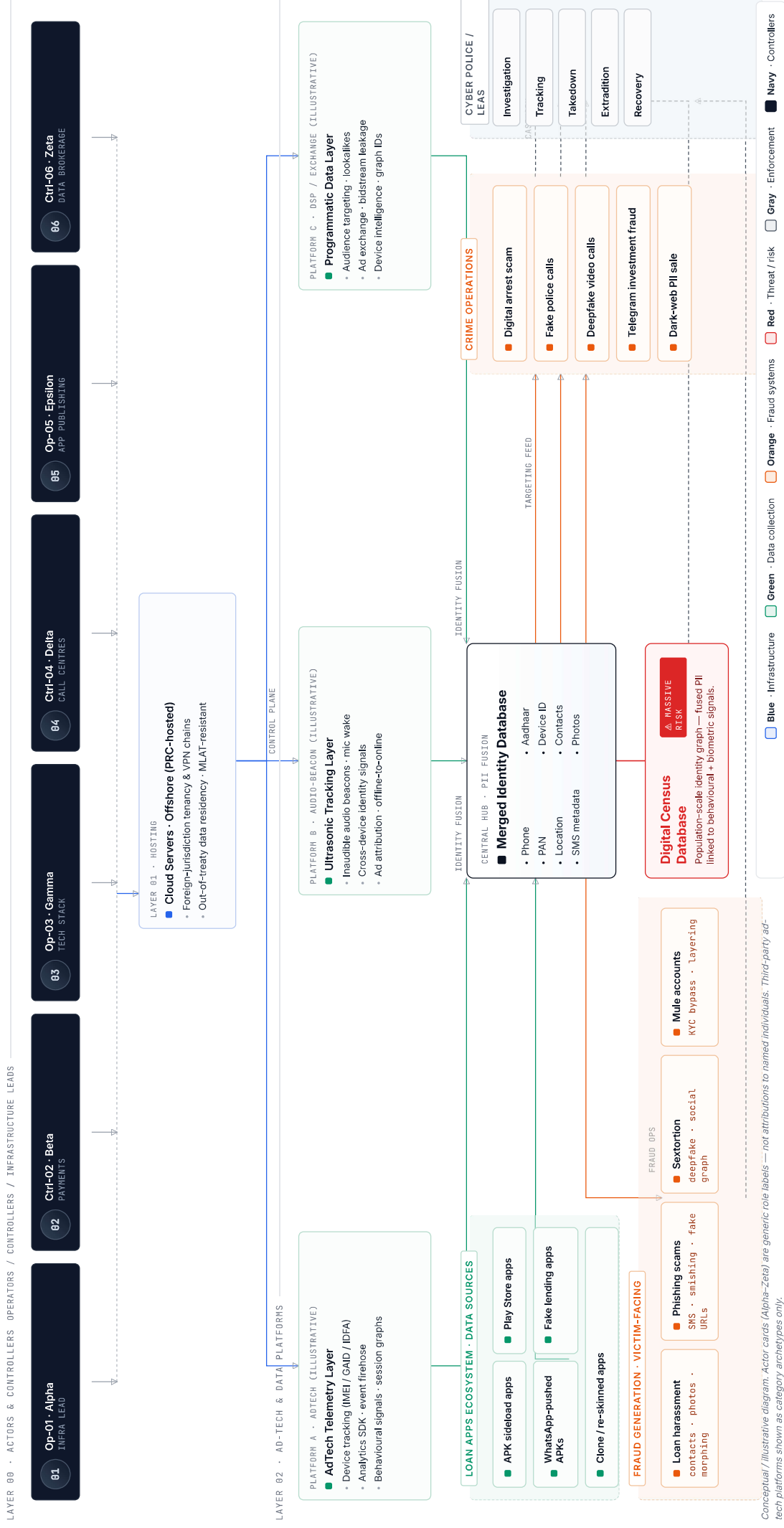


Comprehensive Digital Crime Architecture



Agency Mandates, Coverage & Structural Gaps

LAYER A · AGENCIES & MANDATES · MHA · MEITY · RBI · DOT

A-01 · MODAL
I4C — Indian Cyber Crime Coordination Centre
Ministry of Home Affairs
Nodal body for cybercrime; runs NCRP portal & 1930 helpline; coordinates State LEAs.

A-02 · CRIME DATA
NCRB — National Crime Records Bureau
Ministry of Home Affairs
Cybercrime statistics, CCTNS integration, central fingerprint & ICJS linkage.

A-03 · TECHNICAL
CERT-In — Computer Emergency Response Team
MeitY
Incident response, advisories; 6-hour breach reporting; tech takedowns.

A-04 · INVESTIGATION
CBI Cyber Division & ED
DoPT / MoF
Cross-state & cross-border cyber-financial crime; PMLA attachment, extradition.

A-05 · FINANCIAL
RBI & FIU-IND
MoF
Mule-account monitoring, STRs, digital-lending norms, PA/PG licensing.

A-06 · STATE
State Cyber Cells + DOT & TRAI
States · DOT · MIB
FIR registration, subscriber-data requests, SIM-card takedown, app blocking.

LAYER B · THREAT-TO-AGENCY COVERAGE MATRIX · FULL / PARTIAL / GAP

THREAT VECTOR	I4C	NCRB	CERT-IN	CBI / ED	RBI / FIU	STATE + DOT
Digital arrest / impersonation	FULL	PARTIAL	N/A	PARTIAL	GAP	FULL
Loan-app harassment	FULL	PARTIAL	PARTIAL	GAP	FULL	PARTIAL
Mule a/c & fund layering	PARTIAL	GAP	N/A	FULL	FULL	PARTIAL
Deepfake / AI-generated fraud	PARTIAL	GAP	PARTIAL	GAP	N/A	GAP
Cross-border ad-tech data exfil	GAP	GAP	PARTIAL	GAP	N/A	GAP
Dark-web PII / Aadhaar leaks	PARTIAL	PARTIAL	FULL	PARTIAL	N/A	GAP
Telegram / offshore investment fraud	FULL	PARTIAL	GAP	PARTIAL	PARTIAL	PARTIAL

LAYER C · STRUCTURAL GAPS · CROSS-CUTTING · PRIORITY REMEDIATIONS

GAP 01 · LEGAL
No cross-border ad-tech data-flow regime
DDP Act lacks teeth on SDK-level exfiltration; no MLAT-equivalent for biostream data.

GAP 02 · JURISDICTIONAL
State vs. central FIR tennis
Victim in State A, mule a/c in State B, server in State C — no default routing, cases stall on Zero-FIR.

GAP 03 · TECHNICAL
Deepfake detection unfunded
No standing forensic capability at I4C / CFSUs; no ingestion pipeline for synthetic-media tips.

GAP 04 · FINANCIAL
Mule-account remediation lag
Freeze requests cross 4+ entities (bank → PA/PG → RBI → FIU); median lag exceeds the layering window.

GAP 05 · CAPACITY
State cyber cells under-resourced
Sub-district training & tooling absent; SIM-box & APK takedowns wait on DOT escalation.

GAP 06 · DATA
No unified cyber-crime telemetry
NCRP → CCTNS → bank → CERT-in data rarely joined; no single identity-graph view of repeat offenders.

Full coverage Partial Gap Not in remit