



National Cyber Trust Infrastructure

Keshav Bhardwaj

Center for Digital Public Goods, Indian Institute of Management Bangalore

keshav.bhardwaj@iimb.ac.in | cdpg@iimb.ac.in

www.iimb.ac.in/cdpd

Context

~ 1.48 Billion
Indians

1.09 Billion
Internet
Subscribers

As of March 2026

1.31 B
Telecom
Subscribers

As of December 2025

24.5 B
Monthly UPI
Txns

As in August 2026

1.45 B
Aadhaars
Enrolled

As on 08 October 2026

One of the world's largest and most interconnected digital societies

The Problem

The Digital Footprint is growing. So is the harm.

FINANCIAL-FRAUD COMPLAINTS

2.63 LAKH → 24.03 LAKH
(2021) (2025)

≈9× Growth

LOSS REPORTED

₹551 Cr → ₹22,495 Cr
(2021) (2025)

≈41× Growth

THE SCALE OF THE PROBLEM HAS CHANGED MASSIVELY.
HAS THE RESPONSE ADAPTED?

Modern cybercrime operates across organised networks

A single cyber-fraud incident:

- Begins with a phone call or digital platform
- Moves through an identity and a payment
- Crosses multiple banks and jurisdictions
- Involves telecom and technology intermediaries
- Requires law enforcement, forensics, prosecutors and courts

However, what appear to be separate incidents are often connected parts of the same criminal network.
Criminals reuse identities, mule accounts, devices, infrastructure and successful fraud patterns across incidents.

India's Cyber-Response Capability

01	Reporting & Response	• NCRP & 1930 • CFCFRMS • Money Recovery Module
02	Intelligence & Coordination	• I4C • National Cybercrime Threat Analytics Unit • Joint Cyber Crime Coordination Team • National Cybercrime Ecosystem Management Unit
03	Financial Systems	• RBI - MuleHunter.ai • Digital Payments Intelligence Platform • RBI Sachet Portal
04	Investigation & Forensics	• State Police • National Cyber Forensic Laboratory
05	Judiciary	• eCourts • National Cybercrime Training Centre / CyTrain

We keep adding
portals, databases,
units, and platforms.

But cybercrime
keeps moving
across them.

The criminal network vs. the institutional response

NETWORKED CRIMINAL ENTERPRISE

- Coordinated
- Technology-enabled
- Cross-jurisdictional
- Multi-platform
- Reuses infrastructure, identities and accounts
- Learns continuously
- Moves quickly

INSTITUTIONAL RESPONSE

- Multiple institutions
- Disconnected systems
- Institutional boundaries
- Jurisdictional boundaries
- Manual coordination
- Sequential workflows
- Different data and protocols
- Limited shared memory

THE MISMATCH IS THE PROBLEM.

Criminals operate across boundaries. Our response must coordinate across them.

What is missing

Capable institutions do not automatically add up to a coordinated system.

Instead, what we need:

- Connected intelligence across incidents and institutions
- Trusted information exchange
- Coordinated action across institutional boundaries
- Shared context across cases and jurisdictions
- Standardised information and evidence pathways
- Continuous learning across the ecosystem

The next leap is from capable institutions to a coordinated national response.

The Proposed Solution

NATIONAL CYBER TRUST INFRASTRUCTURE (NCTI)

Proposed as a Federated DPI to Connect Existing Institutions

CONNECTS THROUGH

- Common protocols
- Trusted information exchange
- Automation
- Shared intelligence

WHILE PRESERVING

- Institutional mandates
- State authorities
- Privacy
- Accountability

THE IDEA IS SIMPLE:

“Don't replace what exists. Make it work together.”

NCTI is not another portal

WHAT NCTI IS NOT

- ✗ Another reporting portal or agency
- ✗ Another command or control centre
- ✗ A replacement for I4C or state police systems
- ✗ A central repository of all cybercrime data
- ✗ Unrestricted data sharing

WHAT NCTI IS

A COMMON DIGITAL FABRIC TO:

- Store data effectively, emerge and create intelligence
- Exchange trusted signals
- Connect related intelligence
- Coordinate actions
- Move evidence through standardised pathways
- Retain institutional control
- Learn collectively

It does not replace institutions. It enables them to work together.

The DPI way

India has solved large coordination problems through common infrastructure.

AADHAAR

Common foundation for
trusted identity

Did not replace institutions.

UPI

Common rails for payments

Did not replace banks.

ACCOUNT AGGREGATOR

Consent-based data-sharing
protocols

Did not centralise data.

↓
SAME APPROACH
↓

NCTI APPLIES THIS TO CYBERCRIME

**COMMON
FRAMEWORK**

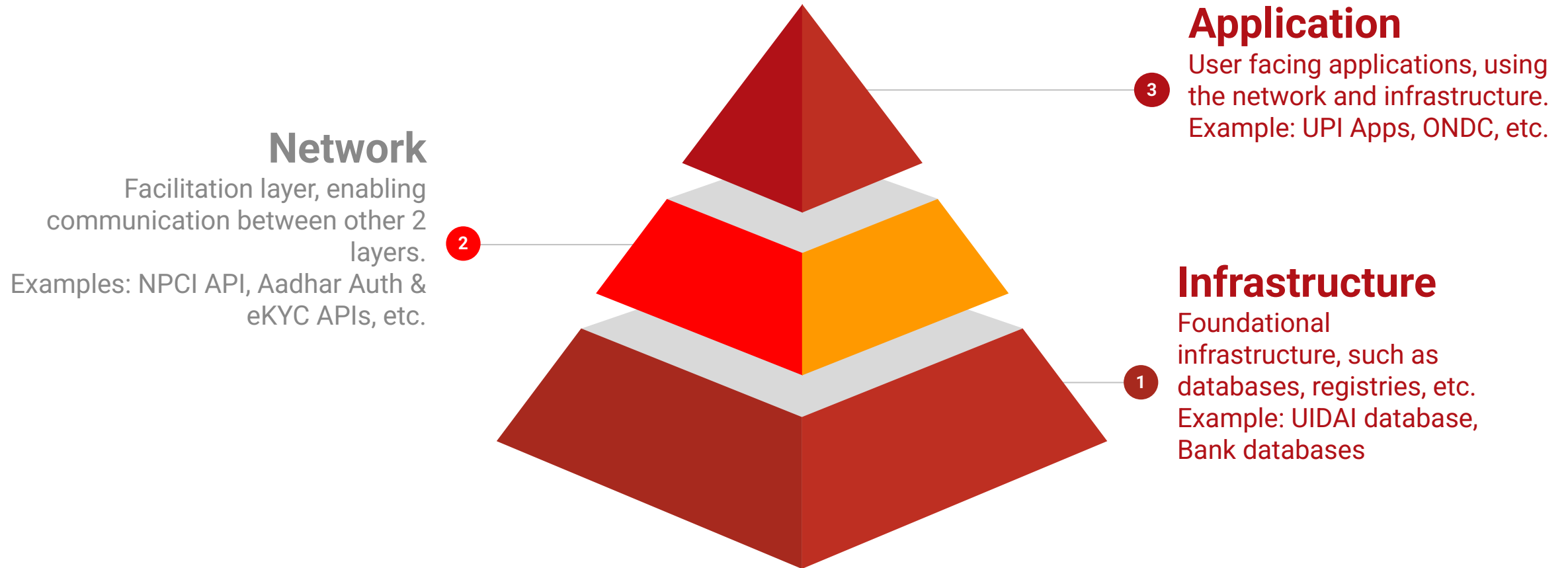
**INDEPENDENT
INSTITUTIONS**

**TRUSTED
PROTOCOLS**

**COORDINATED
OUTCOMES**

SHARED MEMORY

How DPIs work



How NCTI applies this DPI approach

POLICE

FINANCIAL INSTITUTIONS

TELECOM

PLATFORMS

CENTRAL ORGs

JUDICIAL ECOSYSTEM

NCTI – DPI LAYER

COMMON PROTOCOLS

Standardised interaction standards and APIs across entities

TRUSTED INFO EXCHANGE

Secure, privacy-preserving data sharing and signal transmission

AUTOMATION

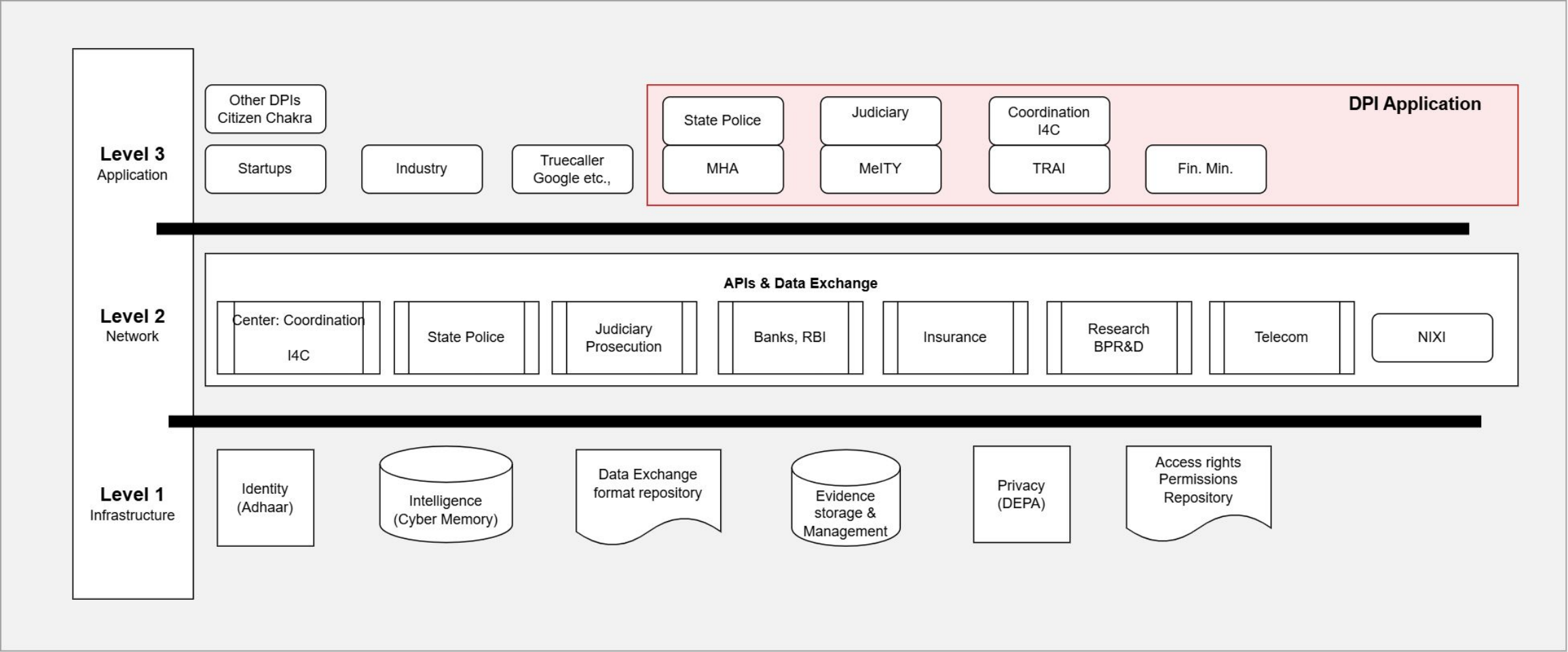
Automated workflows, evidence routing, and incident responses

SHARED INTELLIGENCE

Collective insight, pattern recognition, and cross-domain analytics

CONNECTED BY COMMON FRAMEWORK & PROTOCOLS. INDEPENDENT IN THEIR MANDATES.

Technical Overview



Trust, Privacy, and Institutional Control *by design*

PURPOSE-BOUND

Information is exchanged only for defined, lawful purposes.

CONTROLLED ACCESS

Each participant accesses only what it is authorised to access.

TRACEABLE

Access, disclosures and actions are logged and auditable.

INSTITUTIONAL ACCOUNTABILITY

Institutions retain their mandates, responsibilities and decision-making.

Shared framework. Trusted protocols.
Independent institutions. Accountable action.

Future with NCTI

TODAY

A complaint enters one system

Each institution sees its own slice of the network

Related accounts or incidents may go unnoticed

Information must be actively sought from other institutions

Requests move through separate workflows

Investigation, fund-freezing and evidence requests may proceed sequentially

Learning remains spread across cases

WITH NCTI

A complaint triggers a connected and coordinated response

Patterns across institutions become visible and are retained

Potential links across cases are surfaced

Relevant information can be fetched through trusted protocols

Relevant institutions receive actionable, authorised signals

Appropriate actions can proceed in parallel, subject to each institution's authority

Outcomes can improve future detection and response

Shared intelligence. Faster coordination. Stronger response.



Questions?

Thank you

Center for Digital Public Goods

Indian Institute of Management Bangalore

keshav.bhardwaj@iimb.ac.in | cdpg@iimb.ac.in

www.iimb.ac.in/cdpg