



EXPLORING THE HIDDEN RISKS TO INDIA'S INTELLIGENT SYSTEMS AND DEVICES

A Roadmap to Digital Sovereignty Knowledge Paper

November 2025

The Guild Co – Enabling India's Device Sovereignty

Prepared By
THE GUILD CO.

CONTENTS

EXECUTIVE SUMMARY 2

1. THE QUIET REVOLUTION: INDIA’S RELIANCE ON INTELLIGENT SYSTEMS AND DEVICES . 3

2. THE HIDDEN LAYER: REGISTRIES, OTA, TELEMETRY, AND BEYOND 4

3. WHY THIS MATTERS: THE STAKES FOR INDIA’S FUTURE 6

4. INDIA’S DIGITAL SOVEREIGNTY PUSH: KEY INITIATIVES AND GAPS 6

5. A CALL FOR DEVICE SOVEREIGNTY 7

6. THE GUILD CO: CATALYZING THE SHIFT TO SOVEREIGNTY 8

7. A PHASED ROADMAP: FROM DEPENDENCY TO DOMINION 8

8. CASE IN POINT: POS AND PAYMENT DEVICES – RISKS AND REMEDIES..... 9

8. COLLECTIVE ACTION IS REQUIRED..... 11

REFERENCES 12

DISCLAIMER 14

EXECUTIVE SUMMARY

India's digital and industrial transformation is nothing short of extraordinary. From the streets of Tier-3 towns to the factories of industrial corridors, **intelligent systems and devices** are the unseen force driving progress. In 2024 alone, **Unified Payments Interface (UPI)** processed over **₹200 lakh crore (~USD 2.4 trillion)** in transactions, drones mapped millions of rural properties under **Swamitva Yojana (SVAMITVA)**, and **over 12 million Closed-Circuit Television (CCTV)** cameras watched over smart cities. Yet, as we celebrate these milestones, a quiet vulnerability lingers: the control of these devices.

These are not just gadgets—they are **networked computers**, pulsing with firmware, telemetry, and updates orchestrated from servers far beyond our borders. Walk into a kirana store for a quick UPI scan, board a metro with **Automated Fare Collection (AFC)**, or glance at a surveillance feed in a bustling market. Each interaction hinges on devices governed by foreign platforms. And that begs a profound question: ***How sovereign is India's intelligent edge?***



This paper uncovers these hidden risks across **Point of Sale (POS)** terminals, drones, biometrics, CCTV, robotics, AFC systems, and video conferencing. It reviews India's key digital sovereignty initiatives, highlights gaps in Device Management Platform (DMP) coverage, and charts a phased path to sovereignty—beginning with localized **Device Management Platform (DMP)**—and spotlights POS/payment infrastructure as a proving ground, with tailored recommendations to secure it first.

The Guild Co is among those catalysing this shift for neutral / India-hosted platforms to reclaim control. But this is a national call: for policymakers, industry, and innovators to act before dependencies turn into disruptions.

1. THE QUIET REVOLUTION: INDIA’S RELIANCE ON INTELLIGENT SYSTEMS AND DEVICES

India’s story of the last decade is one of bold digital leaps. UPI has woven payments into the fabric of daily life, processing ₹246 lakh crore (~USD 2.9 trillion) in 2024 alone—equivalent to fuelling a nation’s economy in real time. Drones under **SVAMITVA** and **Drone Shakti** have surveyed over **2.93 lakh (293,000)** villages, empowering rural land rights. **Over 12 million CCTV cameras** now guard **Safe City** projects, from Bengaluru’s **7,500-unit** network to Delhi’s **3 lakh (300,000)** installations. **Aadhaar Enabled Payment System (AEPS)** biometric devices, numbering in the **millions**, enable cash withdrawals for the unbanked. Industrial robotics—**over 50,000 units strong**—hum in factories, while **1 million+ video conferencing endpoints** bridge boardrooms and remote teams.



But with this scale comes a hidden challenge. While we champion homegrown apps and data localization, the devices themselves—the last mile of intelligence—remain tethered to foreign control planes. They are computers, yes, but ones whose registries live in overseas clouds, whose firmware updates arrive via distant pipelines, and whose telemetry whispers economic secrets abroad.

Intelligent System	Scale in India (2024)	Who Controls the Core?
POS / SmartPOS	1.5 crore+ (15 million+)	Verifone Central, Ingenico Estate Manager, PAX Technology (PAX) MAXSTORE, Sunmi Device Management Platform (Sunmi DMP)
Drones	10 lakh+ (1 million+) deployed	DJI (Da-Jiang Innovations) flight controls, Autel geofencing

Intelligent System	Scale in India (2024)	Who Controls the Core?
Biometrics (AEPS)	Millions in use	Mantra, Idemia (formerly Morpho), Thales backends
CCTV / Surveillance	1.2 crore+ (12 million+)	Hikvision, Dahua AI analytics
AFC Systems	50+ cities	Thales, Cubic ticketing logic
Industrial Robotics	50,000+ units	FANUC, ABB, Yaskawa, KUKA remote diagnostics
Video Conferencing	10 lakh+ (1 million+)	Zoom, Cisco Webex, Poly (formerly Polycom) firmware

In normal times, this dependency hums along efficiently. But in a world of geopolitical tensions or supply chain shocks—who decides if your drone lifts off, your POS authenticates, or your CCTV feed goes dark? The risk is structural, not speculative.

2. THE HIDDEN LAYER: REGISTRIES, OTA, TELEMETRY, AND BEYOND

Every intelligent device has a digital heartbeat: a registry that holds its identity, **Over-The-Air (OTA)** pipelines that breathe life into its software, telemetry that maps its every move, and keys that guard its secrets. These are the control planes—and they are rarely ours.



The Registry Problem: Who Owns the Digital Identity?

Picture a fleet of **15 million+ POS terminals** or **1 million+ drones**. Each is registered somewhere—a digital passport with serial numbers, encryption keys, firmware hashes, and bindings to users or merchants. Without it, verification fails; the device becomes a ghost.

The catch? Platforms like Verifone Central or **DJI's** cloud host these overseas, often in the US or China. AEPS biometrics fare better under **Unique Identification Authority of India (UIDAI)'s Registered Devices (RD) 2.x** framework, mandating India-based keys. But for most CCTV from **Hikvision** or robotics from **FANUC**? No such shield. In a crisis—say, strained ties with a hardware giant—who authenticates **12 million+ cameras** or bricks **50,000+ robots**?

OTA Updates: The Invisible Kill Switch



Updates keep devices alive: patching vulnerabilities, refreshing apps, rotating keys. They flow OTA from vendor hubs—Ingenico’s **Telium Manager**, **PAX’s** MAXSTORE, **Zoom’s** firmware servers. Signed abroad, hosted abroad, these pipelines decide what runs, when, and where.

Here’s the shadow: A rogue update could flood **15 million POS units** with malware, as in the 2023 **Mage2POS** campaign that hit 5,000+ Android terminals in APAC. Or disable them outright—a kill switch in foreign hands. For drones or AFC gates, that means grounded flights or stalled metros. Can India assure continuity when **1 million+ video endpoints** depend on **Cisco’s** overseas OTA?

Telemetry: The Data That Slips Away

Reserve Bank of India (RBI) locks down payment data, **Digital Personal Data Protection (DPDP) Act** protects personal info—but telemetry? Device health logs, error patterns, merchant spikes, geofence breaches—the “data around the data”—often streams unchecked to vendor clouds. Not classified as sensitive, it evades rules.

This isn’t trivial. From POS, it reveals **kirana transaction heatmaps**; from CCTV, urban flow insights; from robotics, factory efficiencies. Foreign hosts gain a live feed on India’s economy—**UPI spikes on pension days**, drone routes over farms, robotic output in auto plants. Even UIDAI-controlled AEPS leaks analytics unless restricted. Without mandates, it’s a quiet exfiltration of national intelligence.

Supply Chain and Firmware Shadows

The vulnerability starts upstream. **90%+ of POS and drones** hail from China or Taiwan; robotics from Japan or Germany. Firmware—flashed pre-shipment—carries potential backdoors. Customs scans boxes, not code. A tampered chipset in a **Thales** AFC gate or **Hikvision** camera could lurk for years, processing billions in fares or watching silently.

Known echoes: 2022 **Sunmi** POS shipped with malware; **81.5 crore (815 million) Aadhaar-linked records** exposed in 2024 **Indian Council of Medical Research (ICMR)** leaks, eroding biometric trust. Legacy flaws persist too—UPI overlay attacks, AEPS fingerprint spoofs, **Zoom Zero-Day** intercepts.

The Quantum Shadow on the Horizon

Looming larger: cryptography’s endgame. **Rivest-Shamir-Adleman (RSA)** and **Elliptic Curve Cryptography (ECC)**, the backbone of device keys and OTA signing, crumble to quantum by 2029. India’s quantum readiness? A mere **2.4 out of 5**, per surveys—leaving **15 million POS**, **12 million CCTV**, and beyond exposed to retroactive decryption. Unless **Post-Quantum Cryptography (PQC)** migration starts now, we court a security cliff.

3. WHY THIS MATTERS: THE STAKES FOR INDIA'S FUTURE

It's easy to dismiss these as tech footnotes for **Chief Information Officers (CIOs)** or regulators. But intelligent devices are the **last mile of trust** in our digital nervous system. Offshore registries mean lost fleet sovereignty. Foreign OTA inherits kill switches. Telemetry outflows gift economic blueprints. Supply chains embed ghosts. Quantum looms unaddressed.

The fallout ripples wide:

- **Economic Stability:** A bricked POS fleet freezes **USD 2.4 trillion** in commerce; stalled drones halt farm deliveries. Losses? **Thousands of crores in hours.**
- **National Security:** Surveillance or AFC under foreign thumb becomes leverage in conflicts.
- **Compliance and Credibility:** Offshore telemetry undercuts UPI's global push; weak governance erodes Aadhaar's promise.
- **Public Trust:** When biometrics spoof or video feeds leak, inclusion falters—citizens retreat from the digital fold just as momentum builds.



India's intelligent edge isn't just infrastructure; it's resilience. Without sovereignty, it's fragility.

4. INDIA'S DIGITAL SOVEREIGNTY PUSH: KEY INITIATIVES AND GAPS

India has made remarkable strides toward digital sovereignty, recognizing that self-reliance is essential for a USD 5 trillion economy. Key initiatives underscore this commitment:

- **Digital Personal Data Protection (DPDP) Act, 2023:** Enforced with draft rules in January 2025, it mandates data localization for sensitive information, empowering individuals with rights to access, correct, and erase data. This builds trust in systems like Aadhaar and UPI.
- **India Semiconductor Mission (ISM):** Launched in 2021 and scaling in 2025, it invests INR 76,000 crore (~USD 9 billion) to foster domestic chip design and fabrication, reducing reliance on foreign hardware for devices like POS and drones.
- **National AI Stack:** A 2025 initiative by the Ministry of Electronics and Information Technology (MeitY), it leverages India's datasets for ethical AI development, ensuring sovereign control over algorithms in surveillance and robotics.

- Indigenous Web Browser and iGOT Karmayogi Platform: MeitY's 2025 secure browser promotes data privacy, while the Integrated Government Online Training (iGOT) platform modernizes governance with tools like e-Office and Government e-Marketplace (GeM).
- Production Linked Incentive (PLI) Scheme 2.0: Expanded in 2025, it incentivizes local manufacturing of electronics, including secure components for intelligent devices.
- SAP Sovereign Cloud: Rolled out in September 2025 with Amazon Web Services (AWS), it offers compliant, India-hosted cloud for enterprises, aligning with DPDP.



These efforts have boosted Digital Public Infrastructure (DPI) like UPI and Open Network for Digital Commerce (ONDC), positioning India as a global leader in inclusive tech.

Yet, gaps persist—particularly in Device Management Platforms (DMPs). While data laws like DPDP enforce residency for personal info, device telemetry and OTA pipelines remain unregulated for non-AEPS systems. No national mandate exists for India-hosted DMPs, leaving 15 million+ POS terminals and 12 million+ CCTV cameras vulnerable to foreign registries. Quantum readiness lags, with no unified PQC framework for devices. Supply chains, despite PLI, import 90%+ hardware without mandatory firmware attestation. The result? Operational risks in crises, where foreign kill switches could disrupt USD 2.9 trillion in UPI flows. Bridging these with localized DMPs is the urgent next frontier.

5. A CALL FOR DEVICE SOVEREIGNTY

As India's intelligent systems & device ecosystem scales, securing apps, APIs, and networks is no longer enough. The devices themselves must be brought under a framework of device sovereignty. That shall lead to, for example:

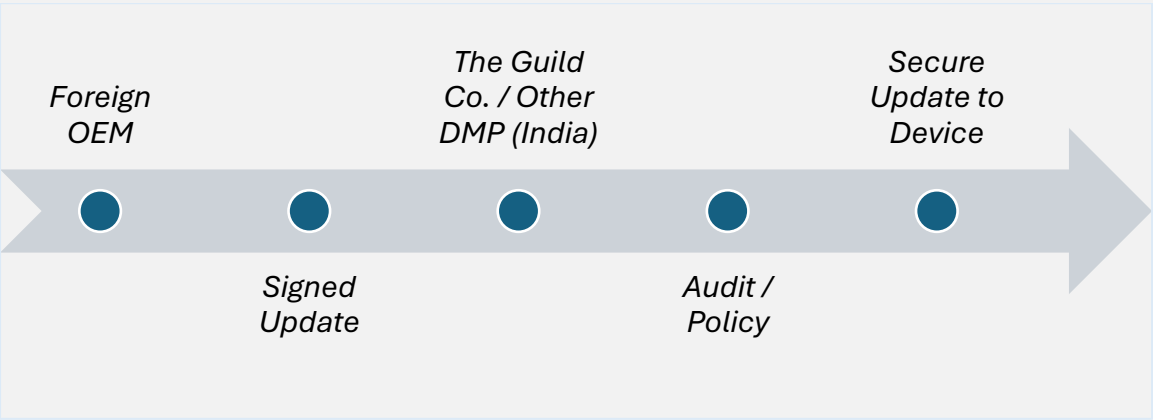
- Hosting registries and OTA control planes within India.
- Escrowing signing keys in India-resident HSMs under joint control.
- Classifying telemetry as critical data, mandating its storage and processing in India.
- Certifying devices under an India-centric Device Certification Authority, covering firmware integrity and rollback safeguards.
- Preparing today for quantum-safe cryptography across devices.

India’s digital journey has been one of the world’s great success stories. But to protect that success, we must ensure the devices that power it remain under our control, our jurisdiction, and our trust.

6. THE GUILD CO: CATALYZING THE SHIFT TO SOVEREIGNTY

Sovereignty isn’t isolation—it’s layered control. **The Guild Co** is working with the vision to be a neutrality enabler, not just a hardware provider. We’re forging a **multi-tenant, India-hosted DMP**—a compliant gateway that inserts India at the core without upending global supply. But we won’t be the only one and that is fine – the scale and scope of India’s digital ecosystem would support multiple players and we all need to come together to drive this.

Here’s how it flows:



Original Equipment Manufacturer (OEM)-agnostic, it supports Verifone to **Hikvision** via **Software Development Kits (SDKs)**. Registries localize, telemetry stays resident, keys escrow in Indian **Hardware Security Modules (HSMs)**. This **Stage 1** win scales across systems—**POS first, then drones to robotics**—building competencies in stages: management, then manufacturing, then indigenous **Research and Development (R&D)**.

Others join this ecosystem, but urgency demands collective action. The Guild Co’s pilots show it’s feasible—and cost-effective.

7. A PHASED ROADMAP: FROM DEPENDENCY TO DOMINION

Full sovereignty unfolds in stages, starting immediate:

Stage	Focus	Timeline	Win
1: Management Sovereignty	India DMP for registry/OTA/telemetry	12–24 months	Control the pulse
2: Ecosystem Build	Local Mobile Device Management (MDM) solutions, APIs, certifications	24–36 months	Interoperable trust

Stage	Focus	Timeline	Win
3: Hardware Depth	Secure flashing, assembly in India	36–48 months	Chain resilience
4: National Core	India Device Certification Authority (IDCA) , PQC standards, key escrow	48+ months	Global exporter

High-Level Imperative (All Systems): Mandate DMPs for critical fleets; classify telemetry as sovereign data; stand up an **IDCA**; **Production Linked Incentive (PLI)**-boost secure infra; quantum-migrate by 2028.

8. CASE IN POINT: POS AND PAYMENT DEVICES – RISKS AND REMEDIES

India’s payment revolution is a global marvel. Since UPI’s 2016 debut, **₹200 lakh crore (~USD 2.4 trillion)** flowed in 2024, touching every corner—from Tier-3 kiranas to metro cafés. **15 million+ terminals**—POS, **SmartPOS**, AEPS biometrics—make it seamless. But the devices? They’re the weak link.



A. The Registry Catch

Verifone, Ingenico, **PAX**, **Sunmi** registries sit overseas. AEPS wins with **UIDAI**’s India mandate—but standard POS? Exposed. A sourcing supplier could de-auth **15 million units**, freezing commerce.

B. OTA’s Shadow Switch

Updates from abroad signed abroad. 2023’s **Mage2POS** hit thousands; **Mirai** botnets turned **PAX** into **Distributed Denial of Service (DDoS)** zombies. Hypothetical: 40% fleet down in 30 minutes.

C. Telemetry’s Quiet Drain

RBI guards transactions; telemetry (usage patterns, merchant IDs) slips out, mapping **pension-day UPI surges** for foreign eyes.

D. Supply and Firmware Ghosts

Foreign origins, pre-flashed code. 2022 **Sunmi** malware; **81.5 crore (815 million) Aadhaar exposures** in 2024 **ICMR** leaks.

E. Quantum’s Approaching Storm

RSA/ECC vulnerable by 2029; India’s **2.4/5 readiness** leaves keys hanging.

F. Specific Remedies for POS/Payments

- **Mandate India DMP by 2027:** Route all OTA/registry/telemetry via **Tier-4 Data Centres (DCs)**; 36-month retrofit for legacy **15 million units**. Operator: **National Payments Corporation of India (NPCI)/RBI** entity.
- **Telemetry as Payment-Adjacent:** Amend **DPSS (Department of Payment and Settlement Systems)**—100% residency, anonymized access only.
- **POS Certification Mark:** Under **IDCA**—firmware attestation, rollback safeguards, PQC slots, emergency **Application Programming Interface (API)**. Label: “**POS-Secure India.**”
- **Import Re-Flash Protocol: Standardisation Testing and Quality Certification (STQC)** labs (Noida/Bengaluru/Chennai) verify and seal all inbound units.
- **Key Escrow & Audit:** Joint **HSM** custody; **blockchain**-anchored logs; Indian override for threats.
- **72-Hour Patch Guarantee:** Penalties for delays.
- **Quantum Roadmap:** 2026 pilot **Dilithium** OTA on **1 lakh (100,000)** units; 2027 PQC mandates; 2028 full high-value rollout.

Metric	Today	With India DMP
Registry	Overseas	India DC
OTA	Foreign-signed	Audited route
Patch Time	15–30 days	72 hours
Telemetry	Leaky	100% resident
Cost	USD 1.2–1.8/mo	Lower by up to 60%
Kill Switch	Inherited	Ours to wield

8. COLLECTIVE ACTION IS REQUIRED

Securing apps and networks was yesterday's battle. Today, it's the devices—the intelligent edge—that demands sovereignty. India's intelligent journey is a triumph. But to safeguard it, devices must answer to us—our control, our jurisdiction, our trust. This shall require collective action by manufacturers, customers, government, policy makers and many others.

LET US BUILD THIS, WE AT THE GUILD CO. ARE CERTAIN THAT WE WILL!

REFERENCES

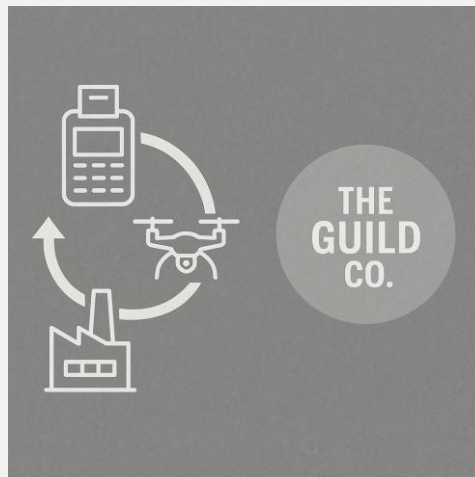
- RBI DPSS.CO.OD.NO. 2785/2021-22
- UIDAI Registered Devices 2.x
- National Critical Information Infrastructure Protection Centre (NCIIPC) Quantum Assessment (2024)
- Computer Emergency Response Team - India (CERT-In) Malware Advisories (2023–24)
- Additional: Statista UPI Data (2024); Resecurity Breach Report (2024)
- MeitY – DPDP Rules 2025, ISM, National AI Stack
- PIB – PLI 2.0, SAP Sovereign Cloud
- The Guild Co. Research and Analysis

[End of Document]

The Guild Co – Enabling India’s Device Sovereignty

DISCLAIMER

While every effort has been made to ensure the accuracy and reliability of the data and analysis presented in this document, the insights and recommendations are based on available information as of the delivery date and our own assessment. This document is intended for advisory purposes only, and The Guild Co. disclaims any liability for actions taken based on its contents. The recipient remains responsible for all business decisions made as a result of this deliverable.



Important Note for Partners: For partners in India, Japan, Taiwan and China – who are working on delivering this outcome for India – reach out to us (www.theguildco.com, Anshuman@theguildco.com – cofounder, Jay@theguildco.com – cofounder) to explore how can we deliver on this promise together.

Important Note for Media Enquiries: For Media Inquiries To explore how The Guild Co. is pioneering device sovereignty for India's intelligent future, contact us at (www.theguildco.com, Anshuman@theguildco.com – cofounder, Jay@theguildco.com – cofounder).