



India Buys Indian

Personal Economic Responsibility

Circulated with The Economic Times, Mumbai, Delhi, Bengaluru, Pune, Chandigarh, Ahmedabad, Lucknow, Jaipur, Kochi, Kolkata, Patna, Ranchi, Bhubaneswar, Chennai, Hyderabad, Goa, Nagpur and Indore

Tuesday, 30 June, 2026

An Advertorial, Lifestyle Promotional Feature
An Optimal Media Solutions Initiative, A division of Times Internet Limited

'Be Indian, Buy Indian' and build the digital trust that holds it all together

Defending Digital Economy Indigenously: 63SATS Cybertech's 'Cyberdome' and 'CyberSecurity Force' shield national infrastructure with purpose-built AI defence and robust DPDP Act compliance

"Be Indian, Buy Indian" has powered a remarkable national project. We have learned to make our own goods, build our own digital rails, and increasingly write our own software and train our own AI. The campaign has always been about more than economics; it is about self-reliance, confidence, and the conviction that a nation should own the systems on which its future rests.

But there is a dimension of self-reliance that rarely makes the headlines, and it is the one that decides whether everything else holds. A country can manufacture its own products, host its own data, and deploy its own AI and still be undone if the trust beneath all of it is borrowed, brittle, or controlled from elsewhere. In a digital economy, trust is not a sentiment. It is infrastructure. And like any infrastructure, it can be indigenous or imported, sovereign or dependent.

This is the conviction on which 63SATS Cybertech is building its products and offerings. While many fine Indian companies are building the nation's digital and AI economy, the mandate of 63SATS Cybertech is to safeguard it and to be the strategic trust layer on which national resilience rests. "We are an operator, not an advisor." 63SATS Cybertech builds and runs sovereign, India-first defence systems for enterprises, governments, and citizens. If "Buy Indian" is to mean anything in the digital age, it must extend to the security that protects the very things we are so proud to have built at home.

TRUST IS THE NEW "MADE IN INDIA"

For decades, "Made in India" was a statement about products you could hold like a car, a phone, a vaccine. The next chapter is about something you cannot hold but cannot live without: The assurance that your data is safe, your identity is yours, your transactions are real, and the AI making decisions on your behalf are not tampered with. That assurance is digital trust, and it is fast becoming the most valuable thing a nation can produce for itself.

Here lies a quiet strategic risk. A great deal of the security stake that Indian organisations rely on is designed, owned, and operated from outside the country. Threat intelligence, detection logic, and even the keys to critical systems can sit on foreign soil and under foreign jurisdiction. In ordinary times this is merely a dependency. In a crisis, be it geopolitical, regulatory, or adversarial, it becomes a vulnerability.

It is a foreign vendor can be subpoenaed by its own government, cut off by a sanctions regime, or simply deprioritise a market far from its headquarters. The data that defines an Indian citizen, the model that runs an Indian bank, the alert that should have stopped an attack on Indian infrastructure — none of these can be hostage to decisions made elsewhere. Sovereign digital trust means the ability to defend ourselves with capability we control, on our own terms, aligned to our own laws such as the Digital Personal Data Protection (DPDP) Act and the directions of CERT-In, SEBI and RBI.

SAFEGUARDING THE AI ECONOMY INDIA IS RACING TO BUILD

India is adopting AI faster than almost any major economy, and with it comes an entirely new class of asset to protect. When an organisation deploys an AI model, it is not adding another application; it is introducing something that thinks, learns and responds, with attack surfaces no firewall or antivirus was built to defend. There is no signature for a poisoned dataset, no patch for a prompt injection. If AI is becoming critical to our digital infrastructure, it deserves an

India defence capability built specifically for it.

That is the purpose of 63SATS CYBX DNA – AI CyberOps Division, a dedicated

research and operations capability focused on protecting AI systems themselves. Its mandate spans model assurance, adversarial validation, AI supply-chain integrity, and sovereign defence-grade research, organised across six pillars covering offensive AI security, AI asset management, secure AI development, autonomous defence, threat intelligence, and AI governance. It is, quite deliberately, Indian capability for an Indian AI economy so that the intelligence we build at home is also defended at home.

DEFENDING THE ENTERPRISES THAT POWER THE ECONOMY

The institutions at the heart of Indian growth, namely banks, capital markets, in-



surers, manufacturers, can no longer be defended with annual tests and perimeter tools while their attackers operate in AI time. They need continuous, expert-run defence, and they need it from partners who understand Indian regulation from the inside.

The enterprise practice, 63SATS CSF (CyberSecurity Force), is built for exactly this.

While many fine Indian companies are building the nation's digital and AI economy, our mandate is to safeguard it... As we celebrate the Indian brands building our digital and AI future, we must decide whether the trust that protects them will also be Indian or quietly outsourced

- Srinivas L, Joint MD & Joint CEO of 63SATS Cybertech

In a digital economy, trust is not a sentiment. It is infrastructure. And like any infrastructure, it can be indigenous or imported, sovereign or dependent... If "Buy Indian" is to mean anything in the digital age, it must extend to the security that protects the very things we are so proud to have built at home

- Neehar Pathare | MD, CEO & CIO of 63SATS Cybertech



Instead of point-in-time assessments, it runs continuous red-teaming and managed detection and response, now re-architected to ingest AI telemetry with model inputs, outputs and agent actions alongside conventional logs. Its advisory and vCISO (virtual Chief Information Security Officer) teams run DPDP-aligned AI usage audits that surface "shadow AI", the unsanctioned tools quietly handling sensitive data inside most organisations, and put governance around them. Because this capability is built and staffed in India, the institutions it defends are never waiting on a support desk in another time zone while an attack unfolds in real time. For boards answering to SEBI's CS-CRF (Cybersecurity and Cyber Resilience Framework) and RBI's IT directions, this is the difference between knowing your posture and assuming it.

SOVEREIGN DEFENCE FOR THE GOVERNMENT THAT GOVERNS IT

Nowhere is the case for indigenous trust stronger than in government. Ministries, state digital infrastructure and critical sectors cannot have their monitoring, data or defensive keys sitting under another country's control. Sovereignty here is not a preference; it is a precondition of national security.

This is the mandate of CyberDome, 63SATS Cybertech's government-facing practice, which invests in sovereign-grade monitoring for ministries, state systems and critical sector deployments where data residency, indigenous control and CERT-In alignment are non-negotiable. It is "Buy Indian" in its most consequential form: The systems that protect the nation's digital backbone, designed and run within the nation.

PROTECTING THE CITIZEN, WHO IS THE REAL ECONOMY

A digital economy is ultimately its people. India's largest attack surface is not its servers but its citizens who are being targeted by deepfake-driven fraud, AI-generated scam calls and identity theft that scale faster than

any regulation can. A campaign to buy Indian means little if the Indian buyer is being defrauded at the point of every transaction.

This is the gap 63SATS Cybertech's consumer business, CYBX, was built to close: An Indian cybersecurity super-app that has already crossed a million downloads, bringing scam detection, secure calling and embedded cyber insurance directly to citizens and small businesses. It is protection designed for Indian threats, Indian languages and Indian payment habits, not a foreign product retrofitted to our context. The company's upcoming CYBX Digital Identity is a blockchain-anchored, self-sovereign identity capability that will let Indians prove who they are without surrendering control of their data to any intermediary, domestic or foreign. It is self-reliance applied to the most personal asset of all, one's own identity, the truest expression of "Be Indian" in a digital age.

THE TRUST LAYER IS A NATIONAL CHOICE

India has a rare advantage in this moment. We are at once one of the world's largest consumers of AI and one of its largest producers of cybersecurity talent. Our regulators SEBI, RBI, CERT-In, MeitY are engaged earlier than most of their global peers. Our digital public infrastructure has already shown the world that sovereign, scaled, secure systems are not just possible but world-leading. The talent, the intent and the proof points are all here.

What remains is a choice. As we celebrate the Indian brands building our digital and AI future, we must decide whether the trust that protects them will also be Indian or quietly outsourced. For 63SATS Cybertech, the answer is settled. The company is building that trust layer across the enterprise, government and citizen, and running it as infrastructure: sovereign, accountable and continuously tested. "Be Indian, Buy Indian" should not stop at what we make. It should extend to who we trust to defend it. The digital economy will be safeguarded by what is deployed at home, not by what is debated abroad.

