RAMAIAH UNIVERSITY OF APPLIED SCIENCES
CENTRE FOR NATIONAL SECURITY STUDIES

Securing India: Balancing self-reliance and collaboration

Suryesh Kumar Namdeo, Senior Researcher and Pavithran Rajan, Advisor to CNSS Council in Voices, India, TOI

Union minister Ashwini Vaishnav's recent decision to adopt Zoho, an Indian platform to manage official documents, has sparked wider conversations about technological self-reliance in India. While the choice of productivity software might seem mundane to the uninformed. It represents a larger strategic decision India put off addressing in 2013, when Edward Snowden revealed the global surveillance empire the US and its Five Eyes allies had created in partnership with Big Tech. India has an uphill task in guarding the privacy of its citizens and protecting sensitive research and intellectual property from foreign surveillance in an increasingly complex geopolitical landscape.

The global surveillance architecture

The interconnected nature of today's digital ecosystem has created unprecedented vulnerabilities. American technology platforms dominate Indian markets for email services, cloud storage, and digital productivity tools. This allows the US government to surveil India's most personal and corporate data. The United States CLOUD Act of 2018 empowers law enforcement agencies to compel American companies to produce data under their control, regardless of where that information originates or resides physically. Section 702 of the Foreign Intelligence Surveillance Act goes further, allowing the government to require electronic service providers to hand over data belonging to non-US persons.

Meanwhile, China's National Intelligence Law of 2017 casts an even wider net, mandating cooperation from all Chinese companies, academic institutions, and individual citizens in intelligence gathering activities. A significant section of commercial and consumer ICT products sold in India is Chinese. This provides access of substantial Indian data to Chinese corporates and state agencies. Ironically, China has faced accusations of cyber espionage against the African Union Parliament, a building that Beijing constructed and equipped with digital infrastructure. These examples illustrate how digital dependency can become a liability when geopolitical interests diverge.

The risks of technological dependence

Reliance on foreign digital infrastructure poses multifaceted threats to a nation aspiring to technological leadership. Cyber espionage and intellectual property theft are significant concerns today. These are especially significant in research related to advanced biotechnology, quantum materials, artificial intelligence, and various other strategic domains. Sensitive data in collaborative projects may be quietly exfiltrated through foreign ICT providers or compromised joint facilities, undermining years of research investment.

Beyond espionage, there are risks of sabotage and foreign interference in critical systems. The geopolitical dimension became apparent during the Ukraine conflict when Western technology companies blocked access to Russian platforms. This demonstrated how digital dependencies can be weaponised during international disputes, crippling research institutions and strategic projects overnight. Economic considerations compound these security concerns. Foreign technology giants often leverage oligopolistic market positions, employ predatory pricing and strategic acquisitions to stifle domestic competitors. Additionally, foreign firms tend to circumvent or ignore national privacy and security regulations. They treat compliance as optional when it conflicts with corporate interests or home-country demands.

A strategic imperative for India

India’s research ecosystem spans government laboratories, academic institutions, and private facilities. While national laboratories under DRDO, ISRO, and the Department of Atomic Energy employ air gaps and other measures for sensitive work, many academic and private research facilities employ minimal measures for guarding sensitive information. These institutions are increasingly engaged in cutting-edge research, yet often remain unaware of, or unconcerned about, the risks inherent in using foreign digital platforms. This dependency has developed over decades, rooted in legacy systems, established trust relationships, and a lax security culture. However, the geopolitical and technological landscape has shifted dramatically. India now possesses the capability and incentive to develop robust domestic alternatives.

A risk-based framework

The solution requires nuance and a structured transition plan. An awareness campaign and risk-based approach should guide policy, with laboratories involved in highly sensitive research on strategic technologies mandated to use domestic platforms. This strategy should gradually be expanded to school and university ecosystems, typical low-risk avenues, in a phased manner, with awareness of privacy and cybersecurity mandated. Clear definitions are essential. Policymakers must identify which laboratories and technology areas warrant enhanced security measures. Vague or overly broad classifications would create bureaucratic obstacles that impede innovation without meaningfully improving security. The goal is protection, not paralysis.

India must promote only high-quality domestic technology platforms selected through competitive, merit-based processes. This requires substantial investment incentives for Indian companies to develop world-class solutions that can compete on functionality, reliability, and user experience, not just on national origin. This will require a government supported Venture Capital ecosystem that identifies and promotes national champions that foreign companies cannot acquire. The recently approved Research, Development and Innovation (RDI) scheme with Rs. One lakh Crore corpus could play a significant role here.

Essential safeguards and awareness

Implementation must be accompanied by awareness-raising and capacity-building initiatives. Many researchers lack adequate training in information security, privacy and research security protocols. Educational programs should help institutions understand threat landscapes, implement enhanced security protocols, and adopt appropriate cybersecurity standards.

Risk assessment must be continuous and dynamic. Technology platforms pose varying threat levels depending on their architecture, ownership structure, data handling practices, and the geopolitical context. Regular analysis can identify the highest-risk platforms in different settings, allowing institutions to prioritise their security investments effectively.

Maintaining international trust

Maintaining India’s reputation as an open, collaborative research destination is the most delicate challenge. If the international scientific community perceives that the Indian government conducts surveillance through mandated domestic platforms, it could severely damage critical international partnerships. Research depends on cross-border collaboration, and any hint of government intrusion into academic work could prompt foreign institutions and researchers to disengage.

Similarly, perceptions of diminished academic freedom would undermine India’s broader ambitions to become a global research hub. The country must therefore ensure that enhanced security measures for sensitive research don’t create a chilling effect on legitimate scientific inquiry or international cooperation.

The path forward

India needs a comprehensive national strategy and roadmap addressing these challenges. This requires sustained policy research to develop solutions that protect sensitive research without compromising scientific openness where it matters most. The plan should include regular reviews to adapt to evolving threats and technologies. The goal is not technological isolation but strategic autonomy in critical domains to ensure technology sovereignty and research security. India should continue engaging with the global research community while ensuring that its most sensitive work, which underpins future technological capabilities and national security, remains protected from foreign surveillance and interference. Finding this balance is complex but achievable. With thoughtful policy, competitive domestic alternatives, and targeted application of security measures, India can protect its vital research assets. The stakes, technological leadership, economic growth, and national security, demand nothing less.