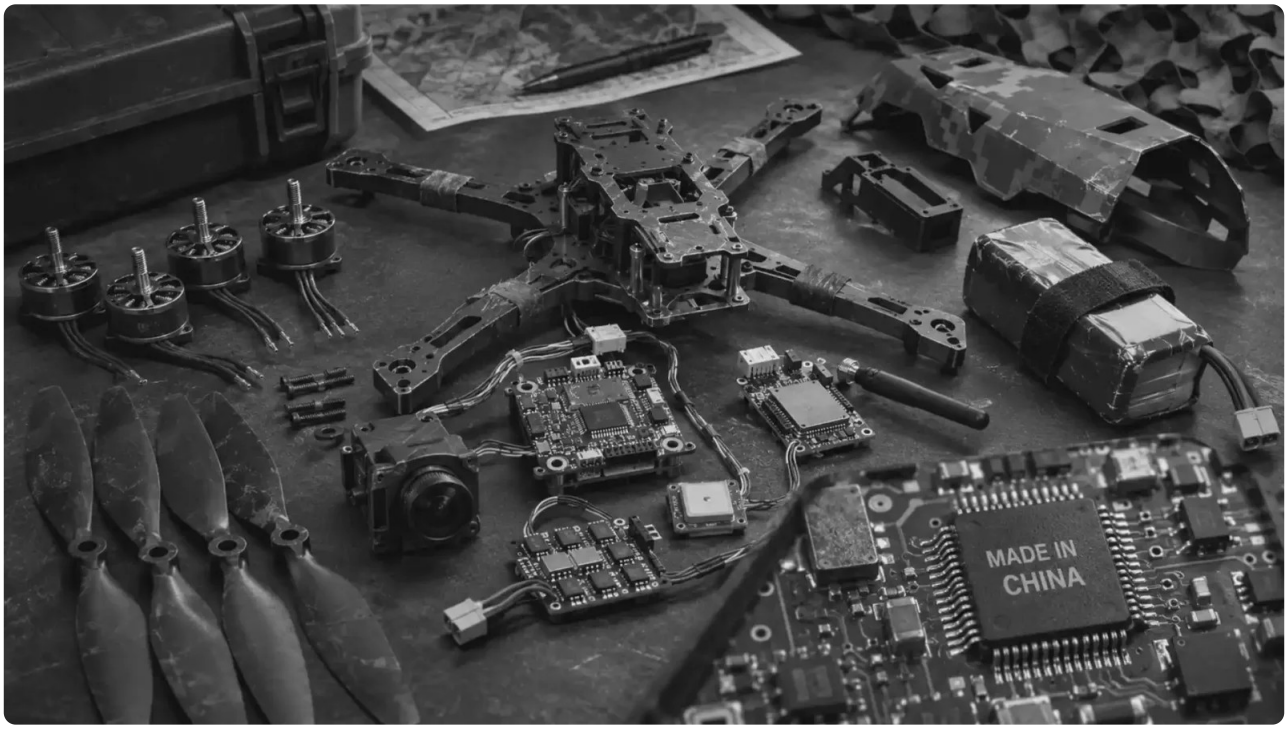
SITUATIONAL REPORTS

Chinese Components in 689 Indian Military Drone Tenders: A Supply-Chain Security Crisis?

Author: CNAWS Research Team • **Published:** November 23, 2026 • **Source:** Centre for New Age Warfare Studies



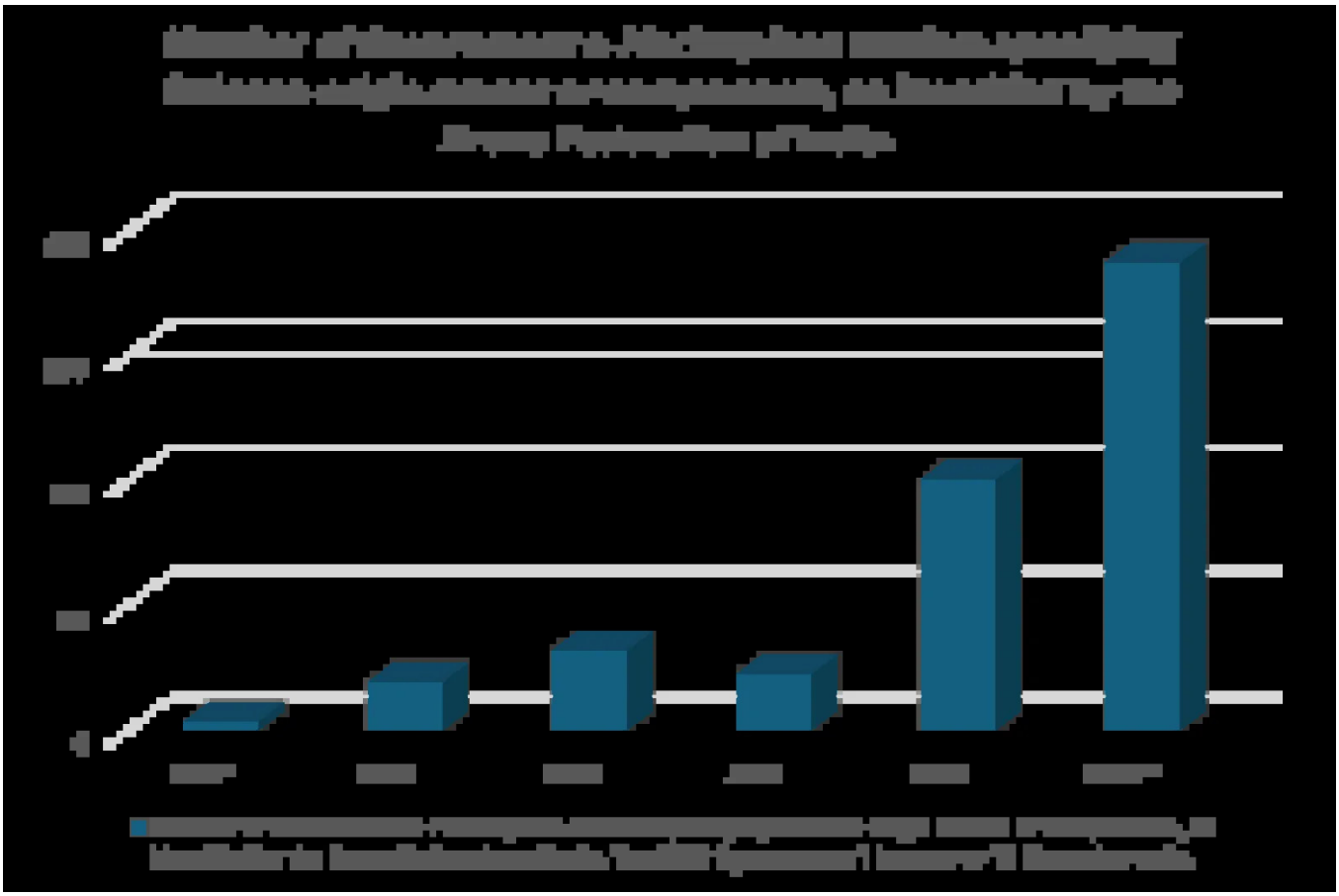
EXECUTIVE BRIEF & KEY FINDINGS

The Drone Federation of India (DFI) has identified 689 government procurement tenders specifying Chinese-origin drones or components between March 2021 and November 2026, including 580 issued by Indian Army units. More concerning is the acceleration in such tenders during 2026, despite existing military procurement restrictions on Chinese components and the establishment of dedicated hardware-security testing facilities. The findings expose a potential disconnect between India's defence indigenisation objectives, decentralised military procurement practices and the security requirements of modern unmanned warfare. The strategic implications extend beyond possible cyber vulnerabilities. Dependence on Chinese-origin flight controllers, navigation modules, communication systems and propulsion components could expose India's drone ecosystem to supply-chain disruption, maintenance constraints and operational uncertainty during a military confrontation with China. However, the reported tenders do not independently establish that the components were purchased, deployed or compromised. This SITREP examines the evidence, technological vulnerabilities and implications for India's military preparedness.

1. The Development

On 20 November 2026, the Drone Federation of India submitted a formal representation to Defence Secretary Rajesh Kumar Singh and Chief of Defence Staff General N. S. Raja Subramani, raising concerns over the continued specification of Chinese-origin drones and components in Indian government procurement tenders. The organisation examined publicly available bid documents on the Government e-Marketplace (GeM) covering the period from 10 March 2021 to 19 November 2026. Its findings identified 689 tenders specifying Chinese drones or drone components, of which 580, approximately 84 per cent, originated from Indian Army units.[1]

The procurement specifications reportedly included products associated with Chinese manufacturers and brands such as DJI, EMAX, RunCam, SpeedyBee, RadioMaster, T-Motor, GEPRC and HGLRC. The components ranged from brushless motors and electronic speed controllers (ESCs) to flight controllers, communication receivers, cameras and video-transmission equipment. These are integral to the functioning of an unmanned aerial system. The flight controller processes sensor inputs and flight commands, the ESC regulates motor operation, while communication and navigation subsystems determine how an aircraft exchanges information and maintains its intended trajectory.



*2021 begins 10 March. *2026 ends 19 November. Figures are from DFI's review of GeM tender documents, as reported by ThePrint. They do not represent awarded contracts or delivered equipment.*

The trend is noteworthy. The number of identified tenders increased from 42 in 2024 to 190 in 2025, before reaching 355 during the first eleven months of 2026. Of the tenders identified in 2026, 328 originated from Army units. Moneycontrol independently located at least ten Army tenders naming Chinese-linked drone brands, providing limited corroboration of the wider industry body's findings.[2]

Nevertheless, three distinctions are necessary. First, a procurement tender demonstrates the requirements expressed by a buyer, not necessarily that an order was awarded or that the equipment entered operational service. Second, the figures do not establish what percentage of all military drone procurement uses Chinese-origin components. Third, the increase may partly reflect the rapid expansion of military drone procurement after Operation Sindoor, rather than a proportional deterioration in supply-chain security. These distinctions do not invalidate the concerns but establish the limits of what the evidence currently demonstrates.

DFI President Smit Shah subsequently stated that many of the smaller tenders were intended for training, assembly and familiarisation.[3] Consequently, the immediate findings should be treated as evidence of procurement exposure and potential inconsistencies in implementation, rather than proof of a systemic operational compromise.

2. A Recurring Problem Despite Existing Restrictions

The controversy is not entirely new. In August 2023, Reuters reported that Indian military authorities had instructed prospective drone manufacturers to avoid equipment and subcomponents sourced from countries sharing land borders with India. The restrictions followed concerns that Chinese-origin cameras, communication equipment, radio-transmission systems and operating software could introduce vulnerabilities into sensitive military platforms. The report also highlighted the challenge faced by Indian manufacturers, many of whom depended on Chinese electronics and faced significantly higher costs when seeking alternative suppliers.?

The effectiveness of these restrictions came under scrutiny in February 2025, when the Army reportedly cancelled contracts worth approximately ?230 crore involving at least 400 logistics drones intended for deployment along the Line of Actual Control. The cancellation followed allegations concerning Chinese-origin components, although a supplier disputed the allegations.?

A distinction must also be made between India's general import policy and military-specific procurement restrictions. In a parliamentary response dated 2 February 2026, the Ministry of Civil Aviation clarified that while the import of completely built, semi-knocked-down and completely-knocked-down drones was generally prohibited under the February 2022 import policy, the import of drone components remained free. Military restrictions on Chinese components therefore operate through defence procurement requirements and security conditions rather than a blanket prohibition on all civilian component imports.?

The Ministry of Defence attempted to institutionalise stronger safeguards in March 2026 through a draft *Framework for Testing Security Vulnerabilities in Drones*, prepared with the Army Design Bureau. The framework emphasised secure-by-design systems, hardware validation, vulnerability testing and the protection of sensitive information against interception, manipulation and unauthorised transmission.?

The Army subsequently inaugurated its first AASHVAST facility in Delhi on 14 August 2026. AASHVAST, or Assessment and Analysis of Electronic Systems Hardware for Vulnerabilities and Security Threats, was developed to identify problematic electronic components, analyse firmware and detect hidden access mechanisms. By September, plans had been reported for five additional facilities.?

Yet DFI identified 104 Army tenders specifying Chinese-linked components after the inauguration of the first facility. This does not demonstrate that the laboratory failed, since the facility's testing mandate and individual units' purchasing processes are separate stages. It does, however, raise an important question about whether centralised security standards are being consistently applied to decentralised procurement.

The larger concern is therefore institutional. India appears to be developing increasingly sophisticated mechanisms to identify untrusted components after procurement while some purchasing specifications continue to introduce the same categories of exposure at the beginning of the acquisition process.

3. The Technical Vulnerabilities

A modern military drone is not merely an aircraft fitted with a camera. It is a network of interconnected electronic subsystems integrating navigation, communication, propulsion, processing and data storage. Its security depends on the integrity of the entire system, including the ground-control equipment and supporting software.

In January 2024, the US Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) jointly warned about cybersecurity risks associated with Chinese-manufactured unmanned aerial systems. Their guidance identified potential pathways for data collection, unauthorised firmware changes, network compromise and exposure of sensitive operational information.? These are relevant threat categories for Indian military planners, although the presence of a Chinese-manufactured component alone does not establish malicious behaviour.

Flight Controllers and Firmware Integrity

The flight controller is among the most consequential components because it processes navigation inputs, stabilises the aircraft and executes flight-control instructions. Its embedded software can influence how the aircraft responds to external commands and changing environmental conditions.

The principal concern is whether an unverified controller contains undocumented functions, insecure update mechanisms, hidden credentials or exploitable software vulnerabilities. These weaknesses could potentially interfere with the aircraft's navigation or response to operator commands. In more serious circumstances, maliciously altered firmware could affect operations only under particular conditions, complicating detection during routine testing.

The AASHVAST programme is specifically intended to identify several categories of such vulnerabilities, including hidden code, time-dependent failures and location-dependent behaviour.? However, a hypothetical firmware compromise must not be confused with evidence that a particular Chinese manufacturer has deliberately installed a military backdoor. Establishing that would require forensic examination of the affected hardware and software.

Communication Links and Intelligence Exposure

Communication equipment presents a different set of risks. A drone's command-and-control system exchanges instructions, telemetry and sometimes real-time imagery with its operator. If security controls are inadequate, these links may expose sensitive data or become vulnerable to interception, manipulation and unauthorised access.

The military significance extends beyond the possible loss of an individual drone. Persistent exposure of surveillance imagery, geographic coordinates, operating frequencies or mission patterns could reveal valuable information about military activity. When aggregated over time, such information may contribute to an adversary's understanding of deployment patterns and operational routines.

The degree of exposure depends on the actual architecture. An isolated, encrypted drone without internet connectivity presents a different threat profile from a system that uses externally hosted services, network-enabled applications or vendor-controlled firmware updates. The presence of a foreign-made motor or basic electronic component does not automatically create an independent pathway for data transmission.

Navigation and Electronic Warfare

Global navigation satellite system (GNSS) receivers, inertial navigation components and associated firmware determine how drones estimate their positions and navigate. These systems can be vulnerable to interference, spoofing and sensor manipulation, depending on their design and protective measures.

Such vulnerabilities are particularly relevant to operations in the mountainous areas of Ladakh and Arunachal Pradesh, where difficult terrain, environmental conditions and contested electromagnetic environments already complicate drone operations.

Importantly, GNSS jamming and spoofing can affect domestically manufactured systems as well. Chinese origin is therefore not the cause of every navigation vulnerability. The pertinent question is whether specific components have been independently tested against foreseeable electronic warfare threats and whether the operator possesses sufficient control over their configuration, updates and recovery mechanisms.

The risk becomes more consequential when unreliable components are integrated into systems conducting reconnaissance, targeting support or precision-strike missions, where navigation or communications failures could reduce mission effectiveness or disrupt wider operations.

4. China's Export Controls and the Risk of Supply Disruption

Cybersecurity is only one dimension of the problem. The second, and potentially more immediate, vulnerability concerns India's dependence on external suppliers for critical electronic components.

DFI estimates reported in November 2026 suggest that approximately 80–90 per cent of flight controllers, 90–95 per cent of GNSS modules and 70–80 per cent of brushless motors used in Indian drones are imported, with China accounting for much of this sourcing.[3] These are industry estimates of import dependence, not independently established Chinese market shares. The distinction is important because an imported component may originate from countries other than China.

The timing of DFI's representation is especially significant. On 19 October 2026, China's Ministry of Commerce announced adjustments to export controls covering specified drones, related components and technologies. The measures entered into force on 18 November 2026. They include licensing requirements for certain propulsion, flight-control, navigation and communication technologies. Beijing described the measures as intended to protect national security and meet non-proliferation obligations, while maintaining that compliant licence applications would be reviewed and approved.[1]?

These controls do not amount to a comprehensive embargo on drone components exported to India. Nevertheless, they provide Beijing with a regulatory mechanism capable of influencing the availability of selected technologies.

The military implications become apparent when considering sustained operations rather than initial procurement. Small drones have relatively short operational lives in high-intensity environments because of combat losses, accidents, environmental damage and wear. Maintaining operational capability requires a continuous supply of replacement aircraft, motors, batteries, electronics and other consumable components.

A force might therefore begin a conflict with adequate drone stocks but encounter increasing difficulties replacing damaged platforms if access to a major supplier becomes restricted. Even where alternative components are available, compatibility issues, qualification requirements and delivery delays could complicate substitution.

The strategic danger is not necessarily that China would halt all exports once a conflict begins. It is that India's ability to sustain a sufficiently large and reliable unmanned fleet could remain partly dependent on commercial and regulatory decisions taken outside India. Such dependence introduces uncertainty into mobilisation planning, procurement forecasts and wartime replenishment.

5. Implications for a Future India–China Conflict

A future military confrontation with China would likely occur in an environment involving substantial electronic warfare activity, persistent surveillance and increased use of unmanned platforms. Drones would be useful for observing difficult terrain, monitoring troop movements, supporting artillery engagements, conducting local reconnaissance and maintaining situational awareness across dispersed military positions.

Under these circumstances, the reliability of unmanned platforms becomes inseparable from the credibility of the intelligence they generate. A reconnaissance drone that experiences unexpected navigation failures, loses its command link or produces unreliable location data can disrupt decision-making even if no adversary has directly compromised the system.

There are three broader strategic implications.

The first concerns operational assurance. Military commanders must be confident that the systems they employ will function as expected under electronic interference, harsh weather and sustained operational stress. A platform assembled domestically but containing unverified foreign control electronics may offer less assurance than its indigenous branding suggests. Security concerns become more serious when platforms are employed for sensitive missions or integrated into larger intelligence and targeting networks.

The second concerns information security. Small drones can collect highly valuable information without carrying sophisticated sensors. Repeated flights over military installations or deployment areas may generate imagery and location records that reveal local infrastructure, logistics patterns and unit activities. A compromised ground-control application or connected data-storage system could therefore be more consequential than the loss of the aircraft itself.

The third concerns industrial resilience. India's drone strategy increasingly depends on the ability to manufacture, repair and replace large numbers of relatively inexpensive systems. If domestic manufacturers remain reliant on foreign flight controllers, propulsion electronics and navigation modules, the expansion of assembly capacity may not translate into equivalent strategic autonomy.

However, the likelihood of China exploiting these dependencies in a future conflict cannot be established from the DFI findings alone. Doing so would require evidence concerning actual military deployments, component vulnerabilities, supplier relationships and China's ability to influence the affected systems.

The credible strategic assessment is that these dependencies represent avoidable risks in a conflict scenario where China would already possess significant advantages in domestic electronics production and supply-chain control.

6. Lessons from Operation Sindoor and the Pakistan Front

Operation Sindoor demonstrated the growing importance of unmanned systems and counter-drone capabilities in India's immediate security environment. In July 2025, then Chief of Defence Staff General Anil Chauhan emphasised that the operation had established the operational importance of indigenous unmanned aerial vehicles and counter-UAS systems. He also warned that dependence on imported niche technologies weakened readiness, scalability and the

ability to sustain operations.[11]

The relevance of the current controversy therefore extends beyond a possible confrontation with China. In another India–Pakistan conflict, drones could be employed at scale for surveillance, reconnaissance, force protection and strike missions. Their reliability would influence tactical intelligence collection, artillery effectiveness, local situational awareness and the ability of units to respond quickly to emerging threats.

The critical issue is not whether Pakistan could automatically exploit Chinese-manufactured equipment inside Indian drones. Such a capability has not been demonstrated by the present reporting. Rather, India's exposure involves the broader possibility that vulnerabilities in poorly verified electronics could become exploitable by a capable adversary, whether through cyber operations, electronic warfare or the exploitation of maintenance and software-update weaknesses.

The distinction matters because threat assessment must separate vulnerability, capability and intent. A vulnerable component creates a potential attack surface. Exploitation requires technical capability and access. Deliberate interference requires evidence of intent or hostile action. Conflating these elements produces dramatic conclusions without the evidentiary foundation necessary for serious military analysis.

For India, the operational lesson is that the expansion of drone numbers must be accompanied by comparable investment in cybersecurity, electromagnetic resilience, secure communications and the assurance of replacement supplies.

7. Defence Indigenisation and the Procurement Contradiction

India's approach to defence indigenisation has encouraged domestic companies to manufacture and supply military drones. Yet the distinction between assembling a platform within India and developing control over its critical technologies remains substantial.

An Indian manufacturer may design the airframe, integrate the payload, develop ground-control interfaces and conduct the final assembly while purchasing its propulsion systems, electronic controllers, navigation modules or specialist sensors from overseas suppliers. Such a product can create domestic industrial value without necessarily eliminating strategically important foreign dependencies.

The current controversy illustrates why component-level indigenisation is more difficult than platform-level indigenisation. Indian firms seeking to develop alternative components must compete against established foreign manufacturers that already benefit from large production volumes, mature supplier networks and comparatively low prices. Without consistent domestic demand, investment in local substitutes becomes commercially uncertain.

DFI has argued that procurement practices should provide greater preference to indigenous components and require mandatory country-of-origin declarations and component-level traceability. Its Bharat Drone Stack initiative, launched in August 2025, seeks to connect drone integrators with Indian component manufacturers.[1]

These proposals address a genuine structural challenge. Nevertheless, replacing foreign components solely on the basis of origin would not guarantee superior security or operational performance. Indian substitutes must also satisfy military requirements concerning reliability, electromagnetic compatibility, environmental endurance and software integrity.

A credible indigenisation strategy should therefore prioritise both technological sovereignty and operational qualification. Components should be assessed according to their importance to flight safety, command-and-control, mission data and

supply continuity. Defence procurement must then create sufficient demand for trusted domestic alternatives while ensuring that critical capabilities are not delayed by unrealistic localisation requirements.

The ultimate objective should be to establish an industrial ecosystem in which India's armed forces can verify the origin, integrity, performance and continuing availability of the components on which their unmanned systems depend.

8. What India Should Do Next

The immediate requirement is to establish the full extent of the problem through an evidence-based procurement audit. DFI's findings provide a starting point, but a comprehensive assessment should examine whether the identified tenders resulted in purchase orders, which components were delivered, their intended operational roles and whether the resulting systems underwent security testing.

The Ministry of Defence should distinguish between equipment used exclusively for training and platforms intended for sensitive missions. This would make it possible to concentrate the most stringent controls on systems involved in intelligence collection, targeting, operational surveillance and other mission-critical functions without unnecessarily disrupting lower-risk activities.

Every military drone acquisition should require a documented component inventory, verified manufacturer and country-of-origin information, a record of firmware versions and a defined process for managing software updates. Testing should cover not only the completed aircraft but also the ground-control equipment, communications architecture and supporting applications.

The expansion of AASHVAST facilities offers an opportunity to standardise security testing across Army formations. However, these facilities would be more effective if procurement teams could identify prohibited or higher-risk components before publishing tenders. Embedding clear technical restrictions into GeM procurement templates would reduce the likelihood of unsuitable components entering the acquisition process in the first place.

At the industrial level, India should identify those technologies for which foreign dependence creates the greatest operational consequences and invest in domestic alternatives accordingly. Flight-control electronics, secure communications, navigation technologies, propulsion components and trusted firmware development would merit particular attention.

Finally, procurement planning must account for the possibility of import disruption during prolonged hostilities. This requires qualified alternative suppliers, adequate spare-part reserves and the ability to rapidly manufacture or substitute components without compromising flight safety or information security.

The effectiveness of these measures should be evaluated through measurable outcomes, including the proportion of mission-critical components with verified origins, the number of platforms that pass independent security testing and the extent to which essential spare parts can be sourced without relying on a single foreign supplier.

9. Strategic Assessment

The findings reported by the Drone Federation of India reveal a potential contradiction in India's military modernisation programme. The armed forces are expanding their use of unmanned systems while continuing to encounter the consequences of an electronics supply chain that remains heavily dependent on foreign manufacturers.

The reported 689 tenders do not prove that Chinese manufacturers have penetrated Indian military networks, installed malicious firmware or acquired sensitive operational data. They do, however, raise legitimate questions about the consistency of procurement controls, the traceability of critical components and the ability of security-testing arrangements to keep pace with rapidly expanding demand.

The problem becomes particularly significant in the context of India–China strategic competition. China possesses substantial capabilities in electronics manufacturing, drone components and the regulatory control of exports. India's reliance on these supply chains therefore creates an asymmetry that could become more pronounced during a prolonged military confrontation.

The establishment of AASHVAST facilities, the development of a drone security framework and the growing focus on indigenous manufacturing demonstrate that Indian defence institutions recognise these challenges. The remaining question is whether these initiatives can be translated into uniform procurement practices and sustained industrial capacity.

The central strategic concern is not simply that Chinese components may appear in Indian military drones. It is that India's ability to operate, secure and replenish parts of its unmanned fleet could remain dependent on technologies and supply chains over which it does not exercise sufficient control.

For a military increasingly reliant on drones for surveillance, targeting, battlefield awareness and precision engagement, such dependence represents a vulnerability that must be managed before it is tested in conflict.

Endnotes

1. Bhaswar Kumar, “Industry Body Raises Alarm: 689 Tenders for Chinese Drones and Parts Floated Since 2021, 84% by Army,” *ThePrint*, November 21, 2026. https://theprint.in/defence/industry-body-raises-alarm-689-tenders-for-chinese-drones-parts-floated-since-2021-84-by-army/3105003/

2. Aihik Sur, “Indian Army Units Sourcing Chinese Drone Components, Industry Tells Defence Ministry,” *Moneycontrol*, November 21, 2026. https://www.moneycontrol.com/news/business/indian-army-units-sourcing-chinese-drone-components-industry-tells-defence-ministry-cites-security-concerns-14086073.html

3. Mohammad Asif Khan, “Indian Army Buying Chinese-Made Drone Components, Says DFI President,” *Business Standard*, November 22, 2026. https://www.business-standard.com/external-affairs-defence-security/news/india-news-indian-army-buying-chinese-drone-components-dfi-chief-smit-shah-126112200276_1.html

4. Reuters, “India Bars Makers of Military Drones from Using Chinese Parts,” *The Indian Express*, August 8, 2023. https://indianexpress.com/article/india/india-bars-makers-military-drones-using-chinese-parts-8881963/

5. “Army Cancels Rs 230 Crore Drone Contracts over Alleged Use of Chinese Components,” *India Today*, February 7, 2025. https://www.indiatoday.in/india/story/army-cancels-rs-230-crore-drone-contracts-over-alleged-use-of-chinese-components-2676137-2025-02-07

6. Government of India, Ministry of Civil Aviation, “Underutilization of Fund for Drone and Reliance on Chinese Components,” Rajya Sabha Unstarred Question No. 180, February 2, 2026.

https://sansad.in/getFile/annex/270/AU180_laPMd4.pdf?source=pqars

7. Vijay Mohan, “India Drafts Framework to Tackle Drone Security Vulnerabilities amid Rising Threats,” *The Tribune*, March 26, 2026. https://www.tribuneindia.com/news/defence/india-drafts-framework-to-tackle-drone-security-vulnerabilities-amid-rising-threats/

8. Amrita Nayak Dutta, “New Army Labs to Weed Out Chinese Parts and Hidden Bugs in Drones,” *The Indian Express*, September 20, 2026. https://indianexpress.com/article/india/indian-army-establishing-six-aashvast-labs-drone-cctv-firmware-vulnerability-analysis-chinese-components-dg-eme-10886499/

9. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, “Cybersecurity Guidance: Chinese-Manufactured UAS,” January 17, 2024. https://www.cisa.gov/sites/default/files/2024-01/Cybersecurity%20Guidance%20Chinese-Manufactured%20UAS.pdf

10. Ministry of Commerce of the People's Republic of China, “MOFCOM Spokesperson's Remarks on Optimizing and Adjusting Export Control Measures for Drone-Related Items,” October 19, 2026. https://english.mofcom.gov.cn/News/SpokesmansRemarks/art/2026/art_3522f2c8fa074f34a6644192642228b9.html

11. Government of India, Ministry of Defence, “Operation Sindoor Demonstrated Operational Effectiveness and Strategic Value of Indigenous UAV and Counter-UAS Systems, Says Chief of Defence Staff,” *Press Information Bureau*, July 16, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2145420