SITUATIONAL REPORTS

Military Drone Supply-Chain Risks: How Chinese Components Expose Western Autonomous Weapons

Author: CNAWS Research Team • **Published:** August 10, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

The next vulnerability in autonomous warfare may not come from enemy jamming, missiles, or cyberattacks. It may already be built into the weapon itself. Britain's discovery that cameras aboard Royal Navy K3 Scout uncrewed vessels were communicating with an IP address in China has highlighted a deeper issue facing modern militaries: autonomous systems are increasingly assembled from globally sourced sensors, processors, batteries, communications modules, and software whose origins and behaviour are not always fully understood. From Europe and the United States to India, defence establishments are now grappling with an uncomfortable reality. A drone may be assembled domestically, operated by national forces, and even marketed as indigenous, yet still rely on foreign components that can introduce hidden technical and data-security risks. In the rush to deploy autonomous systems quickly and at scale, supply-chain security is becoming just as critical as the weapons themselves.

What Britain's K3 Scout Incident Reveals About the Security of the Drone Age

The rapid proliferation of unmanned systems is changing the economics of military power. Armed forces that once depended almost exclusively on expensive aircraft, warships and armoured platforms are increasingly fielding comparatively inexpensive drones, autonomous boats, robotic vehicles and loitering munitions. The attraction is

obvious. They can be purchased in greater numbers, deployed without risking personnel and upgraded much faster than traditional military platforms.

But this model carries a vulnerability that is receiving far less attention than missiles, electronic warfare or counter-drone systems: the integrity of the components inside the unmanned platform itself. The recent discovery of unexplained communications between cameras aboard British Royal Navy K3 Scout uncrewed surface vessels and an IP address in China illustrates the problem particularly well. It does not establish that China penetrated Royal Navy systems or obtained classified intelligence. What it does demonstrate is arguably more important from a procurement perspective: a military platform can be designed and assembled by a trusted domestic defence company while still containing third-party components whose behaviour, software architecture and external communications are not fully understood by the final operator.

The K3 Scout Case

Britain awarded Kraken Works a £12.3 million contract in March 2026 for a fleet of 20 uncrewed surface vessels under Project Beehive. The vessels are intended to support Royal Navy training, experimentation and operations as Britain moves towards a hybrid fleet combining crewed and uncrewed systems. The K3 Scout itself is an 8.4-metre vessel capable of speeds of up to 55 knots, carrying a 600 kg payload and operating in configurations that include maritime surveillance, C4ISR, electronic warfare, force protection and precision-strike support. It can operate through supervised autonomy or remote control.

That makes the description of the K3 as simply a “drone boat” somewhat misleading. It is effectively a modular maritime sensor and effects node capable of being integrated into a wider military network. A routine British Ministry of Defence cyber-vulnerability assessment subsequently discovered that cameras fitted to the vessels were transmitting what were described as “heartbeat communications” to an IP address in China. Such signals ordinarily indicate that a connected device is functioning and online. The MoD removed internet connectivity from the affected cameras and investigated the system. Crucially, it said it found no evidence that MoD information or systems had been accessed, compromised or transmitted externally, and there is no public evidence that imagery, audio, location information or operational plans were sent to China.

Kraken said the cameras came from a third-party supplier and contained a small number of components originating outside Britain. Following an audit with the Royal Navy, the company said vulnerabilities had been addressed and that it was confident sensitive information had not been transmitted through unintended channels.

This distinction is important. The K3 episode should not yet be described as a confirmed Chinese espionage operation. Yet the absence of confirmed espionage does not make the incident trivial. In a military sensor system, the fact that a subsystem can initiate an unexpected external connection is itself significant. It establishes the existence of a data pathway that the end user apparently did not intend to be there. The question therefore moves from *“Was China spying on the Royal Navy?”* to the much more consequential question: “How did an externally communicating component enter a sensitive military platform without that behaviour being identified before deployment?”

Europe Had Already Seen the Warning Signs

Britain had been confronting essentially the same problem with Chinese surveillance technology years before the K3 incident. In November 2022, the British government instructed departments to stop deploying surveillance equipment produced by companies subject to China's National Intelligence Law at sensitive government sites. By June 2023, London had committed to establishing a timetable for removing such equipment from sensitive central-government facilities. The concern was not that every Chinese-made camera contained an intelligence backdoor, but that highly

connected surveillance equipment represented a potentially unacceptable combination of technical vulnerability, remote connectivity and supplier risk.

A government survey published in 2023 exposed the scale of the dependency. Of 31 responding British policing organisations operating cameras aboard drones or UAVs, 23 acknowledged security or ethical concerns involving the manufacturer of their drones, DJI. The same survey found extensive use of surveillance equipment associated with manufacturers such as Hikvision and Dahua across the British policing estate.

The issue has increasingly become European rather than exclusively British. A 2025 European Parliament exchange specifically referred to restrictions imposed by Lithuania and the Netherlands on Chinese-manufactured drones in defence or public-security applications and raised concerns about data exfiltration, telemetry and foreign supplier leverage. The European Commission, while emphasising national responsibility for security decisions, acknowledged that UAS could create cybersecurity and digital-reconnaissance risks and pointed towards broader EU mechanisms for evaluating supply-chain security.

The lesson from Europe is that the vulnerability is progressively moving from fixed infrastructure into mobile and autonomous platforms. A compromised CCTV camera observes one location. A compromised unmanned platform can carry its sensors through naval bases, military exercises, ports, border areas and operational environments. That fundamentally increases the intelligence value of whatever information it collects.

The United States Identified the Problem Earlier

The United States has dealt with similar concerns for almost a decade. The U.S. Army stopped using DJI products in 2017 following cybersecurity concerns. The Pentagon subsequently prohibited the purchase and use of commercial off-the-shelf drones in 2018, and Congress went further by restricting Pentagon procurement of Chinese-produced drones and components. In a 2021 statement, the Department of Defense explicitly maintained that DJI systems represented potential national-security threats. The technical concern was subsequently articulated more clearly.

A 2019 Department of Homeland Security alert warned that Chinese-manufactured UAS could expose organisations through automatic data transmission, insecure communications, vendor access and network intrusion. The alert advised operators to consider disabling internet connectivity and carefully controlling storage and firmware.

In 2024, CISA and the FBI went further. Their joint cybersecurity guidance described drones as information and communications technology devices rather than simply aircraft. They identified potential vulnerabilities involving data transfer, cloud storage, firmware updates, docking stations and other connected peripherals. Most significantly, they recommended supply-chain risk management and both Software Bills of Materials and Hardware Bills of Materials, providing operators with visibility into what actually exists inside a supposedly trusted platform.

The problem extends considerably beyond drones.

A 2025 Government Accountability Office investigation found that the Pentagon's procurement systems provide remarkably limited visibility into lower-tier suppliers. Chinese-origin magnets had appeared in F-35 aircraft, while a deeper Pentagon analysis detected Chinese integration in lower sub-tiers of the MQ-9 Reaper drone supply chain even though its principal suppliers were predominantly American and European. For the F-35, the Pentagon had country-of-origin information for less than 10 percent of all suppliers providing components and raw materials to the programme.

That finding gets to the heart of the K3 problem.

A platform may be British. Its prime contractor may be British. Its principal electronics integrator may be allied. Yet four or five layers down, the sensor processor, communications module, memory device, firmware library, battery cell, magnet or microcontroller may originate elsewhere. National origin at the platform level is therefore no longer a reliable measure of technological sovereignty.

India Faces an Even More Difficult Dependency

India recognised this vulnerability particularly clearly in 2023, when military procurement authorities began preventing domestic manufacturers from using Chinese-origin components in defence drones. Documents and officials cited by Reuters showed that Indian security planners were specifically concerned about Chinese components used in cameras, communication systems, radio transmission equipment and operating software. Tender discussions instructed manufacturers that equipment or subcomponents originating in countries sharing land borders with India would not be acceptable on security grounds. One Indian drone-industry executive estimated at the time that roughly 70 percent of relevant goods within the wider drone supply chain were manufactured in China.

The dilemma subsequently became more pronounced. Following the India-Pakistan drone exchanges of May 2025, Reuters reported that Indian manufacturers still faced dependencies on Chinese-origin magnets and lithium used in UAV batteries. Industry representatives warned that diversification could not be accomplished quickly because Chinese manufacturing had become deeply embedded within the international drone-component ecosystem.

New Delhi has consequently begun moving beyond simply banning complete Chinese drones.

In July 2025, the Ministry of Defence convened an industry workshop specifically focused on indigenising critical UAV and counter-UAS components currently imported from foreign manufacturers.

The policy hardened further in 2026. The Ministry of Defence published a *Framework for Testing Security Vulnerabilities in Drones*, explicitly arguing that foreign components create potential avenues of compromise and that the armed forces should procure systems that are “secure-by-design.” The framework addresses component-level vulnerabilities, secure supply chains, communications, indigenous navigation, secure boot processes and digitally signed firmware.

Defence Minister Rajnath Singh separately argued in March 2026 that genuine drone self-reliance requires indigenous capability extending from software and engines to batteries and other components, acknowledging that critical drone components remain heavily dependent on Chinese production internationally.

India is therefore confronting exactly the challenge highlighted by the K3 episode: a drone assembled domestically is not necessarily an indigenous or secure drone.

Autonomy Makes Supply-Chain Security More Important, Not Less

The transition towards autonomous warfare magnifies this problem. Traditional military equipment certainly contains foreign components, but an autonomous system is unusually dependent upon sensors, software, processors, navigation systems and communications simultaneously. Its camera determines what it sees. Its flight controller determines where it goes. Its navigation module determines where it believes it is. Its datalink determines whom it communicates with. Its firmware determines how all those components behave.

Compromise does not necessarily require a dramatic “kill switch.” Intelligence can sometimes be derived from telemetry, operational patterns, system status or software-update mechanisms long before an adversary attempts to seize control of the platform. There is also a problem of scale. Militaries are deliberately pursuing thousands of relatively inexpensive unmanned platforms. A vulnerability incorporated into a component common across a fleet can therefore reproduce

itself hundreds or thousands of times. What appears to be a minor procurement shortcut can become a fleet-wide security weakness.

This is why simply banning products carrying a particular country's label will not be sufficient. The more sustainable approach is component-level assurance: verified hardware provenance, SBOMs and HBOMs, independent firmware examination, secure boot, signed updates, strict network segmentation, control of outbound communications and continuing security testing after equipment enters service. These measures are increasingly reflected in both American and Indian security guidance.

The K3 Scout controversy should therefore not primarily be understood as evidence of a successful Chinese espionage operation. Public evidence does not support that conclusion. Its strategic significance is more fundamental. Modern militaries are rapidly trying to acquire autonomous systems at commercial-technology speed and commercial-technology prices, but their procurement and security-assurance systems were largely developed for slower, vertically controlled defence programmes. The two models are colliding.

The greatest vulnerability in the emerging autonomous battlefield may consequently not be the drone that an adversary jams or shoots down. It may be the drone whose operator does not know precisely what is inside it, what its components are capable of communicating with, who controls its firmware, and where its data can ultimately travel.

In the age of autonomous warfare, sovereignty over the hull or airframe is no longer enough. Technological sovereignty increasingly means sovereignty over the entire data and component chain.

References

1. *The Times*. “Navy Drone Boats ‘Were Sending Data to China.’” August 9, 2026. *https://www.thetimes.com/uk/defence/article/navy-drone-boats-sending-data-china-k3-rcqd2jcfl*
2. Kraken Technology Group. “K3 Scout Unmanned Surface Vehicle.” Accessed August 10, 2026. *https://krakentechnology.com/platforms/k3-scout*
3. United Kingdom Ministry of Defence. “Project Beehive: USV and GCS Procurement.” *Find a Tender*, March 10, 2026. *https://www.find-tender.service.gov.uk/Notice/021405-2026/PDF*
4. United Kingdom Biometrics and Surveillance Camera Commissioner. “UK Policing ‘Shot Through’ with Chinese Surveillance Technology.” February 15, 2023. https://www.gov.uk/government/news/uk-policing-shot-through-with-chinese-surveillance-technology
5. United Kingdom Cabinet Office. “We Will Protect National Security through a Strengthened Procurement Regime.” June 7, 2023. *https://www.gov.uk/government/news/we-will-protect-national-security-through-a-strengthened-procurement-regime*
6. European Parliament. “Security Risks Posed by the Use of Chinese-Manufactured Drones by EU Security and Enforcement Bodies.” 2025. *https://www.europarl.europa.eu/RegData/questions/reponses_qe/2025/003323/P10_RE%282025%29003323_EN.pdf*
7. U.S. Department of Homeland Security. “Chinese Manufactured Unmanned Aircraft Systems: Industry Alert.” May 20, 2019. *https://content.govdelivery.com/attachments/USDHS/2020/06/03/file_attachments/1465486/Industry%20Alert%20-%20Chinese%20Manufactured%20UAS%20%2820%20May%202019%29.pdf*
8. U.S. Department of Defense. “Department Statement on DJI Systems.” July 23, 2021. *https://www.war.gov/News/Releases/Release/Article/2706082/department-statement-on-dji-systems*
9. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation. *Cybersecurity Guidance: Chinese-Manufactured UAS*. January 17, 2024. *https://www.ic3.gov/CSA/2024/240118.pdf*

10. U.S. Government Accountability Office. *Defense Industrial Base: Actions Needed to Address Risks Posed by Dependence on Foreign Suppliers*. GAO-25-107283. July 2025. *https://files.gao.gov/reports/GAO-25-107283/index.html*
11. Kaushik, Krishn. “India Bars Makers of Military Drones from Using Chinese Parts.” Reuters, August 8, 2023. *https://www.nasdaq.com/articles/exclusive-india-bars-makers-of-military-drones-from-using-chinese-parts*
12. Reuters. “India and Pakistan’s Drone Battles Mark New Arms Race in Asia.” May 27, 2025. *https://www.reuters.com/business/aerospace-defense/india-pakistans-drone-battles-mark-new-arms-race-asia-2025-05-27*
13. Government of India, Ministry of Defence. “MoD to Host Workshop on UAV & C-UAS Indigenisation.” July 15, 2025. *https://pib.gov.in/PressReleasePage.aspx?PRID=2144799*
14. Government of India, Ministry of Defence. *Framework for Testing Security Vulnerabilities in Drones*. March 2026. *https://mod.gov.in/sites/default/files/Final-Drone-Framework-24-Mar-25_0.pdf*
15. Government of India, Press Information Bureau. “India Must Become Global Hub of Drone Manufacturing in Next Few Years amid Current Geopolitical Instability: Raksha Mantri.” March 19, 2026. *https://pib.gov.in/PressReleasePage.aspx?PRID=2242398*