



LOW-ALTITUDE ALERT

Liam Hutcheson warns that though the UK built its drone doctrine for the last aerial threat, the next one is already overhead

China's recent decision to impose sweeping restrictions on civilian drone use has reignited a debate among Western governments on how far states should go in controlling drones. Complete ban, as Beijing has done, or regulation? That question sits at the heart of this article.

The debate around drone security has long focused on payloads – on what a drone may carry, such as weapons and contraband. That focus is not without justification, but it has drawn attention away from a parallel and arguably durable risk. The drone that carries nothing at all, yet hovers for six minutes over a data centre, an energy substation or a defence logistics hub, transmitting everything it sees to someone who never came near the perimeter – and for what purpose?

This article examines that problem through a UK lens. It considers what China's crackdown reveals about the governance of low-altitude airspace, whether Britain could or should move toward similar restrictions and if another targeted approach would be more suitable. It addresses the growing question of trust around drones and components manufactured overseas – particularly where those systems may collect, transmit or expose sensitive

data. And it examines drone security across prisons, ports, airports, energy sites and data centres – and whether their operators are prepared. From May 2026, Beijing moved decisively to restrict civilian drone activity within the capital. The measures go further than simple operational limits. They introduce a comprehensive ban on the sale, production, assembly, rental and import of drones and 17 key components within the city. All existing devices must be registered, with a maximum of three drones permitted under a single address. Operation without explicit government approval is prohibited outright.

The political rationale was stated plainly. Xiong Junghua, Deputy Head of the Legal Committee of the Beijing Standing Committee of the Municipal People's Congress, explained that as the capital, Beijing faces greater challenges in low-altitude security, making stronger regulation of unmanned aerial vehicles an urgent necessity. As a country that controls an estimated 70 percent of the global drone manufacturing market China has, within its own borders, determined that civilian access to that technology requires comprehensive state oversight.

China is not the only jurisdiction moving in this direction. In December 2025, the United States Federal

Britain has demonstrated it can respond to drone incidents. It has not yet demonstrated it can anticipate them

Communications Commission announced it would ban new foreign-manufactured drones from the American market; a decision that effectively blocks Chinese manufacturers who have become dominant players across farming, mapping, law enforcement and filmmaking. The FCC's review concluded that all drones and critical components produced in foreign countries posed unacceptable risks to national security, with exemptions available only where the Pentagon or Department of Homeland Security determined otherwise. The move followed Congressional legislation raising national security concerns about Chinese-manufactured drone technology and its growing footprint across critical American industries.

Western security circles have been quick to ask whether comparable frameworks could be introduced domestically. It is a logical reflection, but not the right starting point. Regulation alone does not solve this. The more substantive question is what this debate exposes – about data provenance, supply chain trust, who is ultimately responsible for governing low-altitude airspace and, critically, what equipment and legal authorities are needed to enforce any framework that emerges.

Whatever Beijing's underlying motivations – and they are worth neither idealising nor dismissing – the regulatory architecture it has built raises questions that apply just as much in London. Who currently controls what happens in British low-altitude airspace? Who can see what those platforms are collecting? And when an unauthorised platform is detected, who has the authority and the equipment to act? Governance without enforcement capability is a policy document, not a security posture.

No single authority in the UK has full visibility of low-altitude airspace, understands what drone platforms are collecting, or holds clear legal authority to act when they should not be there. That is the gap at the centre of this debate and it remains unresolved.

Britain's approach to drone regulation has developed largely in reactive bursts, each triggered by an incident rather than a strategic assessment of where the threat was heading.

The 33 hours of runway closure at Gatwick in December 2018, when over a hundred credible sightings of unauthorised drone activity halted around 800 flights and stranded more than 140,000 passengers, demonstrated that UK airports were operating in critical airspace without meaningful detection or response capability. The legislative response extended exclusion zones and mandated registration. It was necessary, but also backward-looking, designed to prevent the recurrence of a specific incident rather than to address the evolving capability of the threat.

Within the prison space, the problem followed a similar arc. Drone captures and sightings within prison grounds in England and Wales more than doubled between 2019 and 2021, reaching 500 incidents. In one operation in the North-West of England, a criminal gang conducted 20 flights attempting to deliver drugs, mobile phones and SIM cards with a combined street value exceeding £1.7-million. The legislative answer was a 400m no-fly zone. A border response to a border breach.

Neither response engaged with the deeper structural question: the perimeter model of site security is fundamentally broken. A line drawn on a map does

not stop a drone. It creates a criminal offence after the fact. Those are not the same thing. Britain has demonstrated it can respond to drone incidents. It has not yet demonstrated it can anticipate them. The conversation about drone security in Britain has focused almost entirely on where drones fly. It has paid far less attention to what they collect, and who benefits from that. The risk is not confined to foreign state actors. A drone operated by a legitimate UK business can be used to surveil a competitor's facility. A contracted survey team flying over a logistics hub can capture operational patterns, staffing rhythms and infrastructure layouts that have significant commercial value to the wrong recipient. A disgruntled employee with a consumer drone and 15 minutes can extract more useful intelligence about a site than a month of open-source research. None of those scenarios require foreign involvement. All of them are happening.

THE POWER TO TAKE ACTION AGAINST AN UNCREWED AIRCRAFT IN FLIGHT IS RESTRICTED

Supply chain is a separate but related dimension. The components inside most commercial drones used across UK critical infrastructure – such as sensors, transmission modules and flight controllers – originate predominantly from a small number of overseas manufacturers. Drones are connected devices. They capture imagery, positional data, thermal signatures and access patterns. A drone conducting a legitimate survey of a data centre or energy substation is, simultaneously, a data-collection platform operating at close range over sensitive infrastructure. The question of where that data goes after capture, and under what legal framework it can be accessed or compelled by a third party, has not been answered with any consistency in British security planning.

The US approach offers something worth examining, not as a model to replicate wholesale, but as an illustration of what a government looks like when it has decided to take supply chain trust seriously. The FCC's decision was not primarily about where drones fly. It was about who built them, what the data architecture looks like and whether operational use of those platforms inside sensitive environments creates an acceptable or unacceptable exposure. Britain has not had that conversation at policy level. It needs to. But it also needs to have an equally serious conversation about the domestic operators already flying over sites that matter, with no malicious foreign connection required.

Assume for a moment that both problems are addressed. Trusted platforms verified operators. The next problem is detection and it is substantial. Persistent, reliable detection of small uncrewed aircraft in low-altitude airspace requires a layered approach. Radar alone does not cover it. Small drones have low radar cross-sections and fly beneath the altitude thresholds where most traditional air surveillance systems operate. Effective detection combines radio frequency analysis, identifying the communication signals between a drone and its operator, with acoustic sensors, optical systems and, increasingly, AI-assisted

classification that can distinguish a delivery drone from a surveillance platform mid-flight.

The technology exists. It has been deployed effectively at military installations and at a small number of high-security civilian sites in the UK and across NATO partner countries. The gap is not technological. It is structural. Most of Britain's critical infrastructure: its ports, its energy grid substations, its water treatment facilities and its data centres operate without any of it.

THE 33 HOURS OF RUNWAY CLOSURE AT GATWICK IN DECEMBER 2018 HALTED AROUND 800 FLIGHTS

Site operators are not unaware of the problem. Many are acutely aware of it. What they lack is clarity on three things: what they are legally permitted to deploy, who bears responsibility for responding when a threat is identified and what the response options are. On all three, the current framework leaves them exposed.

Detecting a drone and doing something about it are different legal acts in the UK and the distance between them is where the current framework falls apart. Under existing legislation, the power to take action against an uncrewed aircraft in flight is tightly restricted. It sits with the police and with specific agencies operating under defined authority. A site security team that detects an unauthorised drone conducting a sustained overflight of a nuclear facility does not have the legal standing to intervene. They can report it. They can document it. The drone continues to fly.

What is needed is a defined and workable authority structure. That means identifying which sites qualify for enhanced protection status, granting their operators – or contracted security providers working on their behalf – clear legal authority to deploy detection systems and establishing an unambiguous chain of escalation when a threat is confirmed. It also means funding the capability to act on what detection reveals, which requires investment in both equipment and trained personnel.

Britain does not need to follow Beijing. A comprehensive civilian ban would be disproportionate, economically damaging and difficult to enforce in a market where drones are already part of everyday commercial activity. What it does need is a shift from reaction to control. That starts with recognising that the obvious critical national infrastructure sites are only part of the problem. Nuclear facilities, major ports and energy assets matter, but they are not the full picture. Logistics hubs, industrial estates, commercial warehouses and data-linked businesses are increasingly exposed, often without realising it. Many of the organisations that need detection capability today do not yet recognise themselves as targets.

It also means looking beyond where drones are flown to what they are doing, what they are collecting and where that data ends up. A legitimate platform and operator can still create a security problem if the data it captures is sensitive.

Finally, detection has to be matched with authority. Identifying a drone without the ability to act does little to change the outcome. Site operators and security services need clear, workable powers alongside the technology to use them.

The next significant drone incident in the UK is unlikely to be dramatic. It will be brief, precise, and easy to miss. The impact will come later. The question is whether Britain builds the capability to deal with that now, or waits until it has to •

Liam Hutcheson is UK
Director at MyDefence.

When an unauthorised platform is detected, who has the necessary authority and the equipment to act?



Picture credit: Getty Images