# Information security audit of Chinese-manufactured drones

## Introduction

This document describes how Airpelago uses drones manufactured by Chinese companies during the inspection of critical infrastructure while maintaining the highest level of information security. The mitigation strategies are backed up by an external audit performed by Assured, an independent Swedish security firm.

## The concern

Operators inspecting critical infrastructure such as power lines, railways, pipelines, and industrial sites face a recurring objection that flying this hardware over sensitive assets means shipping imagery and telemetry to a jurisdiction outside their control. The objection is understandable, but with the correct precautions and methods, we can use these drones without compromising security.

## The actual risk

The drone itself is just an airframe and a radio link; it does not decide where your data goes. That decision is made by the software running on the drone and its remote controller. The remote controller software in particular determines which servers it authenticates against, which cloud it syncs flight records to, where captured media is uploaded, and what telemetry it reports.

In a default deployment, that software is the manufacturer's. Its endpoints, sync behaviour, and update mechanism are outside your control.

## Replacing the software layer

Airpelago's flight application replaces the manufacturer's flight app on the controller. Planning, flight execution, and data transfer are controlled by us. Captured imagery and LiDAR are only stored on the encrypted SD card in the drone, and later uploaded to Airpelago infrastructure hosted in the EU, in Stockholm. The manufacturer's cloud is not part of the data pipeline.

In independently captured traffic from live inspection flights using our proprietary software, manufacturer endpoints accounted for **0.12% of total data volume**. The other 99.88% went to infrastructure controlled by Airpelago.

## Different operating modes: two options

1. **Standard.** Full connectivity. The controller reaches Airpelago's EU-hosted backend for mission sync and data upload, plus mapping and time services. Residual manufacturer control-plane calls such as geofencing lookups and licence checks remain reachable.
2. **Offline.** No external connectivity during operation. Missions are loaded and data is extracted through a controlled process on the ground. There is no network path off the device in flight, so there is nothing to intercept, inspect, or trust.

We recommend standard connectivity for most operations, and the reason is safety rather than convenience. The manufacturer maintains a continuously updated database of geofences, no-fly zones, and temporary airspace restrictions, and an aircraft with access to it will refuse flights in these areas. In standard mode, we are also able to operate the drones using LTE connectivity, which improves both efficiency and flight safety.

For especially sensitive assets, offline mode removes external connectivity during flight entirely. Missions are loaded and data is extracted through a controlled ground process, so there is no in-flight network path at all.

## Independent verification

We commissioned Assured Security Consultants, a manufacturer-independent Swedish security firm, to capture and analyse all network traffic leaving a DJI RC Plus 2 controller across five real inspection flights in June 2026, using a DJI Matrice 4T and our proprietary software.

Their findings, in standard connected mode:

- **Manufacturer endpoints accounted for 0.12% of total observed data volume.** Across roughly 1.05 MB of traffic captured over five flights, all DJI-associated domains combined carried 1.28 MB. Even under the most conservative attribution, assigning DJI the entirety of a shared CDN[1] address it co-resolves with a mapping service, the figure stays below 0.7%.
- Excluding Airpelago's own LTE relay and counting only conventional HTTP host traffic, the manufacturer share is 2.9% of 43.4 MB. Both figures describe the same thing: control-plane scale, not payload scale.
- The remaining volume was concentrated almost entirely on Airpelago's EU-hosted infrastructure.
- **Only 245 KB was uploaded to manufacturer endpoints across all five flights**, roughly 49 KB per flight, or 0.023% of total traffic. The remaining 1.03 MB was inbound. Four fifths of the manufacturer relationship is the device *fetching* data, not sending it.
- No image- or video-sized transfers to third parties were observed. A single uncompressed 48 MP frame runs 140–150 MB; outbound traffic appeared in short bursts far below that threshold.
- No suspicious destinations were identified. The remainder was mapping, DNS, and time synchronisation.

**What that traffic most likely contains.**

The contents were encrypted, so the following is inference from hostnames, direction, and volume rather than observed fact. The download-dominant pattern is consistent with reference

[1] Content Delivery Network

data flowing to the aircraft: geofence and airspace restriction databases, terrain elevation tiles, SDK and CDN assets, and update manifests. Based on hostnames, the 245 KB of uplink can be assumed to consist of flight-safety lookups as well as account and licence endpoints. At that volume this is most plausibly TLS and HTTP overhead, device and licence identifiers, and the query parameters those lookups require.

We cannot rule out that the approximate location of the drone is sent to the manufacturer during flight; this is likely required for the geofencing service to function. The rough location of power line assets is, however, already easily accessible through other open sources such as public map providers (i.e., Google Maps or OpenStreetMap). We can definitely determine, based on the observed data patterns, that large amounts of sensitive data such as high-resolution imagery are not uploaded to the manufacturer.

## Summary

Capable drone hardware and controlled data handling are not mutually exclusive. The manufacturer builds the aircraft; who controls the software controls the data.

Replacing the manufacturer application reduces its share of observed traffic to 0.12% while retaining the airspace safety data that makes connected flight worthwhile. Where an asset does not tolerate even that, offline mode removes the network entirely. The exposure is a configuration decision, not a property of the airframe.

---

*Based on Assured Security Consultants' report AIR001 v2, 26 June 2026. Full report with per-endpoint traffic detail available on request.*