Understanding DJI's AeroScope Solution

Last month DJI introduced AeroScope, its ready-to-use system to identify, track and monitor airborne drones while protecting the privacy of drone operators and imposing no costs upon them. Law enforcement, national security and aviation safety officials have been pleased to see AeroScope address their legitimate concerns about drone safety and security.

However, some "counter-drone" companies that see AeroScope as a competitive threat to their expensive products have deliberately distorted how AeroScope works and raised spurious objections to how AeroScope supports legitimate drone operations.

Consider the source

One recent attack came from Department 13, a company that sells a $340,000 drone detection system with a $44,000 annual maintenance fee. Department 13 saw its stock price fall 20% to a 21-month low after DJI announced AeroScope. (DJI has not set a price for AeroScope, but it is expected to be less than $5,000.)

DJI AeroScope uses the existing communications radio equipment onboard drones to provide a reliable way for authorities to identify and monitor airborne drones, especially near sensitive locations or places that may raise safety concerns such as airports. The solution acts like an "electronic license plate for drones" and helps to ensure drones remain a safe, secure and a beneficial addition to our airspace.

Department 13 released a paper questioning the security of the AeroScope protocols and the entire concept of a local broadcast solution that identifies drones while protecting operator privacy. DJI wishes to correct the inaccurate or misleading claims being spread by this company and to further explain how AeroScope is a solution that can be broadly used by all unmanned aircraft systems (UAS) companies to provide common standards for safety, security and drone pilot privacy, at very low cost.

Privacy rights of drone pilots

Governments around the world have made clear they intend to soon require all drones to transmit some form of identification and telemetry information. DJI believes an important public policy debate is necessary to balance authorities' legitimate concerns against the privacy interests of drone operators, as well as the burdens and costs that will be placed upon them.

DJI has been the most vocal industry advocate for addressing the privacy, cost and operational concerns of drone pilots in these regulatory discussions, as reflected in our March 2017 white paper on the topic. DJI remains the only major company in the UAS industry that we know of that has expressly asserted the privacy rights of drone operators in their business and personal drone use, and advocated for those rights in policy forums and rulemaking committees. A number of other major companies in the UAS industry take precisely the opposite view on drone operator privacy.

The discussion about Automated License Plate Readers (ALPR) and government or private databases is also valid. However, the white paper by Department 13 envisions a possible long-term outcome no worse than various alternative remote ID solutions in which a "total awareness" system is not just a

possible outcome, but the *starting point* by design. Department 13, whose own product would be susceptible to the same ALPR concerns, presents no alternative proposal for UAS remote ID.

Concerns about spoofing

First, there is a misunderstanding about the public policy assumptions behind drone remote ID. Remote identification policy, similar to UAS registration policy, presumes that most people want or will comply voluntarily with legal requirements and a means of compliance is presented to them that involves a fairly low burden.

Registration and ID solutions do not seek to stop the "bad actors" who will find ways to operate outside the system, just as a license plate system does not do anything to prevent people from removing, forging, covering, or stealing and swapping license plates. We have also heard from safety and security agencies that the goal for remote ID is to have a high percentage of drones identified, with an *expectation* that some drones will never be identified.

Second, to "jailbreak" a drone via software hacking is both a violation of DJI terms of use (because it compromises safety features) and also beyond the capabilities or interest of the vast majority of drone users. Those who would spoof their identification information in the face of a legal requirement would likely buy a non-ID-compliant brand or self-built drone anyway. Moreover, other remote ID solutions that allow drone users to provide ID information into a system will also be susceptible to some risk of spoofing, perhaps on a system-wide basis.

Third, once Remote ID is a legal mandate, there will be a back-end method, be it for aviation authorities or law enforcement agencies, to verify that the ID being transmitted is valid and corresponds to the drone pilot. This would be analogous to law enforcement officers verifying license plate and registration information on the road. Since there is no legal requirement for remote ID yet, it is premature for DJI and aviation authorities to implement a method to secure the remote ID mechanism. When remote ID regulatory requirements come into effect, DJI is confident that AeroScope will have the ability to adapt and meet the required security needs.

The ability to display drone ID without using an AeroScope receiver

DJI intended from the start for its solution to allow other companies to design and build receivers so that remote identification information transmitted by the drone's command-and-control radio could be the simplest and least costly method of accomplishing the policy need for remote identification. We are pleased that other companies are already learning how to build receivers on their own.

Ability to turn off parts of the remote ID information

The Department 13 white paper also points out that certain information in the remote ID transmission currently can be turned on and off by the user. This is by design, to allow DJI customers to make certain decisions about which data to broadcast in advance of a regulatory mandate. As with most technology, the pre-release, pre-regulation version will often differ from a final implementation version. Once a remote identification requirement is implemented by government, some of these user options will be removed so that the information required to be transmitted is in fact always transmitted.

An open and flexible solution

Department 13's white paper does not discuss other remote identification solutions nor provide insightful recommendations. DJI understands and expects that being first to market with a comprehensive and effective remote identification technology will subject AeroScope to scrutiny. A useful evaluation of remote identification technologies would also examine alternative methods, which from our perspective are more invasive, more burdensome, more costly, and potentially less secure than AeroScope.

DJI intends for other companies to build receivers that can detect and identify DJI drones as well as drones from other manufacturers, so that the solution to drone ID policy challenges can be accessible and affordable to the authorities who require it. Our goal is very clear: We are seeking to solve a problem and enable drones to become more accepted by society to enable amazing applications, not to make a huge profit from the concerns raised by a small number of unauthorized drones in sensitive locations.

For more information on DJI's AeroScope Solution, please visit https://www.dji.com/newsroom/news/dji-demonstrates-drone-license-plate-technology-and-knowledge-quiz

For more information about DJI's commitment to data security, please visit: https://security.dji.com/post?id=dji-src-announcement-1&lang=en_US

# # #