

Chinese sUAS Technology in the U.S. Public Safety Sector

ANALYSTS: Christopher Todd, CEM and Chief Charles Werner, (ret.) **ASSOCIATE ANALYST:** Chantell Mazo

KEY FINDINGS

- 1) DJI is the leading brand of sUAS aircraft operated by public safety users. 73% of public safety UAS operators are flying the DJI Mavic series, with 47% operating the DJI Matrice series, and 46% using the DJI Phantom series.
- 2) DJI is also the leading brand of sUAS flight control software used by public safety remote pilots. 77% of operators are flying via the DJI GO4 app, with 67% using DJI Pilot.
- 3) DJI's public safety marketplace dominance should continue for at least another year. 55% of public safety operators say their department or agency intends to purchase a DJIbrand drone within the next year, with 29% of operators indicating that they are unsure. Only 21% of public safety operators claim the intent to purchase a non-DJI branded drone within the coming year.
- 4) Confusion exists within the public safety sector about alleged security vulnerabilities surrounding Chinese drone technology. While 44% of public safety remote pilots indicate that they are not concerned about potential security vulnerabilities such as Chinese "spyware," 33% of operators are somewhat concerned, and 23% are extremely concerned.
- 5) Brand loyalty to DJI is precarious. Of the 10 most important attributes regarding UAS technology for public safety operators, brand ranked the lowest among all choices. Additionally, an overwhelming 88% of public safety operators stated a preference to purchase a drone from a U.S.-headquartered company if all other factors such as quality, capabilities, and price were nearly identical.

EXECUTIVE SUMMARY

As the debate surrounding alleged security vulnerabilities with Chinese drone technology escalates, public safety UAS operators are uncertain about whether drone data is truly safe from foreign eyes. Nevertheless, Chinese drone manufacturer DJI continues to dominate the small UAS landscape within the public safety sector; a trend that will continue for the immediate future.

DJI has demonstrated a savvy prowess at garnering global market share, and the company deserves substantial credit for enabling U.S. public safety agencies to effectively use sUAS for a wide variety of missions. But while public safety UAS operators have embraced DJI as a

low-cost, reliable gateway drone, their loyalty to the DJI brand is tenuous. Time will tell if DJI has the staying power to remain the leader in an industry that could soon rapidly evolve.

The September 18 introduction of the *American Security Drone Act of 2019* – proposed legislation spearheaded by a bipartisan group of U.S. lawmakers seeking to ban drone purchases by federal agencies from China (and other countries identified with national security concerns) – represents a new salvo echoing across the beltway and beyond. If enacted, this legislation would also prohibit U.S. public safety agencies from using federal grant money to procure banned sUAS technology, further jeopardizing China's grasp on the public safety marketplace, while also potentially sending many U.S. public safety drone programs into a tailspin.

INTRODUCTION

Chinese company Da-Jang Innovations (DJI) – the world's leading sUAS manufacturer in terms of market share – can trace its origins back to 2006 and the college dorm room of founder Frank Wang at the Hong Kong University of Science and Technology. After graduating, Wang relocated his start-up to Shenzhen (China's renowned manufacturing mecca) and began selling do-it-yourself drone kits and controllers.¹

In 2013, DJI released their first ready-to-fly drone platform, the DJI Phantom 1 (P1). The P1 included an internal GPS system which was a revolutionary breakthrough representing the first time a consumer drone user had on-board technical assistance for maintaining and stabilizing the aircraft's position in the air.

Each new version of the DJI Phantom series showed technological improvements, with each offering greater capabilities for the operator. DJI quickly became a gateway drone, capturing the imagination of photographers and videographers. DJI Phantoms, as well as the DJI Inspire series of aircraft, were soon embraced across commercial sectors for various operations including agriculture, mining, construction, critical infrastructure inspection, public safety operations, and more.

As interest and enthusiasm surrounding commercial drone use proliferated, DJI saw a new opportunity to migrate beyond the consumer-grade Phantom and mid-grade Inspire series. The company began to develop and release more advanced, "prosumer" and professional-grade sUAS as they introduced both their Matrice and Mavic series. The Mavic series touted a highly portable, compact size, while the Matrice series offered a larger, more robust, customizable platform for commercial operations.

Other companies, including U.S. startup firm 3D Robotics (3DR) and even powerhouse technology company Intel attempted to compete against DJI, but could not find success in a market where DJI could flood the shelves with low-cost, good-quality drones that were relatively reliable and easy to use right out of the box.

U.S. aerospace and defense stalwarts such as AeroVironment, Boeing, Lockheed Martin, and others could have targeted the professional and public safety drone markets, but this would have likely meant increasing their cost of sales while simultaneously lowering their prices (and thus their margins) from their existing lucrative defense contracts in an attempt to pursue and accommodate the modest budgets of most public safety agencies. That clearly wasn't going to happen.

French firm Parrot continues to pursue DJI, albeit with very limited success. Even other

¹ Ali Crane, Dronelife, From Startup to Empire: The Evolution of DJI Drones, May 2018

Chinese companies -- most notably Yuneec - have failed to find secure footing in the battle against DJI for dominance of the skies.

DJI was perfectly positioned in the marketplace and like most smart technology companies, was listening to feedback from their customers. DJI learned what capabilities were needed, and improvements were introduced with each new drone release. This was especially true for public safety users, for whom DJI had created a direct point of contact.

All of this was happening as DJI's global drone market share continued to expand.

In early 2017, DJI introduced the Matrice 200 series - their new enterprise-level workhorse drone for commercial users. This aircraft touted a more robust, industrial platform with swappable batteries, interchangeable payloads, and a software development kit (SDK) for developers to customize certain features of the drone.

But on August 4, 2017, a controversy began to bubble when SUAS News published a copy of a memo from the U.S. Army Aviation Directorate via the Army's Deputy Chief of Staff directing all personnel to cease all DJI use, uninstall all DJI applications, and await follow-on direction.²

A 2017 internal report from the Los Angeles intelligence division of the Immigration and Customs Enforcement (ICE) agency stated that DJI was "selectively targeting government and privately-owned entities ... to expand its ability to collect and exploit sensitive U.S. data."3

Shortly thereafter, DJI unveiled the Mavic 2 Pro series, and quickly followed a few months later with the Mavic 2 Enterprise series. The DJI Mavic 2 series represented what both hobbyist and commercial drone users were seeking in a sUAS; portability, reliability, longer flight time, and assorted payloads (depending on the model).

By 2018, DJI had ascended to a seemingly untouchable position in the emerging drone marketplace. The company reported \$2.7 billion in revenue for 2017⁴, and owned 74% of the global drone brand market share, according to Skylogic Research.

The reign of DJI closely resembled that of America Online (AOL) -- the leading online access firm that dominated the connectivity gateway more than two-decades earlier during the dawn of home Internet use.

But by spring 2019, storm clouds were again forming on the horizon of DJI. In a notice titled Chinese Manufactured Unmanned Aircraft Systems⁵, the U.S. Department of Homeland Security warned U.S. companies about "strong concerns" that Chinese-made drones are stealing data. The DHS notice was issued on the heels of the issuance of an executive order signed by President Donald Trump effectively banning U.S. companies from using telecommunications equipment made by Chinese company Huawei.

Sensing that it would have a fight on its hands, DJI bolstered its U.S. legal team in May 2019, just prior to the FAA UAS Symposium in Baltimore, MD.⁶

Echoing the DRONERESPONDERS 2019 Mid-Year Public Safety UAS Report published August 5, 2019, less than 1% of U.S. public safety agencies have historically had direct access to aviation resources.⁷ The high costs surrounding manned aviation were simply too expensive for small police and fire departments to absorb. Small unmanned aircraft systems (sUAS) are

² Gary Mortimer, sUAS News, US Army Calls for Units to Discontinue Use of DJI Equipment, August 4, 2017

³ David Shortel, CNN, DHS warns of 'strong concerns' that Chinese-made drones are stealing data, May 20, 2019 4 Shortel, CNN

⁵ David Shepardson, Reuters, DHS warns of data threat from Chinese-made drones, May 20, 2019

⁶ DJI, Newsroom, DJI Welcomes Mark Aitken To Its Washington Advocacy Team, May 30, 2019 ⁷ Lynn Langdon, National Institute of Justice, The Functions and Costs of Law Enforcement Aviation Units, 2007

rapidly changing that landscape as public safety agencies of all sizes seek to launch drone programs to help perform a variety of life safety missions more successfully.

DJI brand drones are currently the most widely used sUAS by U.S. public safety agencies. According to DRONERESPONDERS *2019 Fall Public Safety UAS Survey* data, 73% of public safety agencies or organizations claim to be operating a DJI Mavic series drone. DJI also commands the number 2-4 slots with 47% of respondents reporting use of the DJI Matrice series, 46% the DJI Phantom series, and 37% the DJI Inspire series.

Even the lowest reported DJI sUAS in use by public safety organizations, the DJI Inspire at 37%, more than double digits that of Yuneec at 12% -- the next closest named sUAS brand in the DRONERESPONDERS survey.

In summary, the top 5 sUAS used by public safety organizations are all made by Chinese companies. The same trend holds true for the flight control software used to operate the majority of the drones used by public safety organizations.

Almost 77% of public safety organizations claim to have used the *DJI GO4* flight control application within the past 90-days, according to DRONERESPONDERS *2019 Fall Public Safety UAS Survey* data. The next most used app is *DJI Pilot* at roughly 67%.

When asked "does your department of agency intend to purchase a DJI-brand drone within the next calendar year," 55% of the 224 respondents replied "yes," with another 29% stating they were unsure, according to DRONERESPONDERS *2019 Fall Public Safety UAS Survey* data.



FIGURE 1: DOES YOUR DEPARTMENT OR AGENCY INTEND TO PURCHASE A DJI-BRAND DRONE WITHIN THE NEXT YEAR?

SOURCE: DRONERESPONDERS Fall 2019 Public Safety UAS Survey, September 2019

Contrarily, when asked "does your department of agency intend to purchase a non-DJI branded drone within the next year," 34% of those same respondents replied "no," with 46% claiming they were unsure, according to DRONERESPONDERS.

While these trends are not projected to change substantially in the immediate future, there may be cause to believe that DJI's dominance within the public safety marketplace could be in jeopardy as time progresses.

PROBLEM

The origin of the DJI name is said to come from the Chinese phrase "大志无疆," which essentially translates to "great innovation has no boundaries."⁸ It is this self-proclaimed lack of boundaries that has many U.S. lawmakers and security officials worried.

Two pieces of Chinese legislation can be linked to the heart of U.S. concern. According to a March 4 report from MSNBC, both the 2017 National Intelligence Law and the 2014 Counter-Espionage Law grant the Chinese government broad powers in forcing Chinese organizations and individuals to "support, assist, and cooperate with state intelligence work" without the ability to refuse.

In essence, if you are a Chinese company and the Chinese government says they have a legal justification for seizing your data, then you must cooperate or potentially face dire consequences. This is precisely why the United States and other countries have prohibited Chinese telecommunication equipment manufacturer Huawei from providing hardware to the next generation of 5G mobile networks.⁹

And this is the same argument that is now being directed toward DJI.

DJI vehemently refutes innuendo that the Chinese government has access to DJI customer drone data. Additionally, the company retorts that drone operators using DJI technology have the choice of if, and when, they send flight data to the DJI cloud.

In a June 24, 2019 letter to the U.S. Senate Committee on Commerce, Science, and Transportation, Subcommittee on Security, DJI wrote "... DJI drones do not share flight logs, photos, or videos unless the drone pilot deliberate chooses to do so. They do not automatically send flight data to China or anywhere else ..."

DJI then unveiled the "DJI Government Edition" (GE) drone system which claims to offer additional data privacy safeguards including blocked Internet access for the device, along with locally stored data files. DJI also announced plans to start assembling drones in California – in what would be its first assembly line located outside of Shenzhen.¹⁰

Bolstering DJI's position was a July 2019 report by the U.S. Department of the Interior (DOI) which ultimately authorized DJI Matrice 600 Pro and Mavic Pro aircraft equipped and tested with GE to be authorized for DOI use – but only for "non-sensitive missions that collect publicly releasable data." DJI touted the results of this study, highlighting their collaboration with DOI and NASA to validate the GE drone system.¹¹

But the second to the last sentence of the DOI report's summary section contains cautioning language stating; "... the necessity to test and validate future GE updates to ensure continued security makes this solution time-consuming and costly to maintain and scale; not a suitable long-term solution."

The result of this complicated quagmire has been to cause uncertainty among many public safety operators who operate DJI aircraft. And it unfortunately comes at a time when most public safety UAS programs are just starting to get off the ground.

According to DRONERESPONDERS Fall 2019 Public Safety Survey data, 23% of total public

⁸ Crane, Dronelife

^o Arjun Kharpal. MSNBC, Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice, March 4, 2019

¹⁰ Cyrus Lee, ZDNet, DJI unveils plans to start assembling drones in US amid security concerns, June 26, 2019

safety survey respondents say they are "extremely concerned" about recent allegation that Chinese-made drones and associated technology may contain "spyware" or other hidden capabilities to transmit sensitive data from UAS operations back to China. An additional 33% said they were "somewhat concerned," with 35% reporting to be "not very concerned," and 9% as "unconcerned."

FIGURE 2: HOW CONCERNED ARE YOU ABOUT RECENT ALLEGATIONS THAT CHINESE-MADE DRONES AND ASSOCIATED TECHNOLOGY MAY CONTAIN "SPYWARE" OR OTHER HIDDEN CAPABILTIES TO TRANSMIT SENSITIVE DATA FROM YOUR UAS OPERATIONS BACK TO CHINA?





SOURCE: DRONERESPONDERS Fall 2019 Public Safety UAS Survey, September 2019

When drilling down into the DRONERESPONDERS data and analyzing only law enforcement user responses, 25% of survey respondents report they are "extremely concerned," with 25% "somewhat concerned," 39% "not very concerned," and 10% "unconcerned."

Contrast this with fire rescue user responses, and the DRONERESPONDERS data shows that 14% of respondents are "extremely concerned," with 41% of firefighters "somewhat concerned," 36% "not very concerned," and 9% "unconcerned."

This wide spectrum of public safety perceptions toward Chinese-drone technology is not healthy in a profession where confidence and trust in equipment can mean the difference between life and death during a response.

Public safety professionals rely on their training along with clear guidance from leadership to make correct decisions when lives are on the line. This guidance, combined with established standards and procedures, helps to define the rules of engagement and best course of action. These public safety drone operators want and need a reliable, durable, and accurate drone that is ready to fly when needed. It is here where the dilemma exists.

Public safety drone program managers and remote pilots have spent considerable time and effort diligently analyzing and evaluating available UAS technology in the marketplace. In the absence of an abundance of clear guidance from Washington D.C., these public safety

professionals are now forced to rethink their decision-making process in an environment where accusations are prevalent, but empirical evidence is limited.

As the DOI report noted, the notion of having to continually test and evaluate new software updates for security purposes is simply not cost feasible – especially for smaller agencies operating on shoestring budgets. Sacrificing Internet connectivity for data security is also not a tradeoff that most drone operators are eagerly willing to accept.

The September 18 introduction of the *American Security Drone Act of 2019* by a bipartisan group of lawmakers seeks to ban federal departments and agencies from purchasing any drone or sUAS manufactured or assembled in China, or other countries identified as posing national security concerns for the U.S. The proposed legislation would also prohibit law enforcement agencies – including local police forces – from using federal money to purchase the banned technology.¹²

According to DRONERESPONDERS *Fall 2019 Public Safety UAS* Survey data, the mean UAS program budget for local police departments is \$18,000 USD per year. Police departments historically rely on Federal grants as well as seizure funding to help purchase needed equipment and technology. The inability to use federal grant money to purchase DJI drones and other Chinese UAS technology threatens to substantially impact the way U.S. law enforcement agencies structure their UAS operations.

The overarching result of the continued sparring sessions between the U.S. government and the leading manufacturer of UAS technology is an exacerbation of uncertainty. This potentially threatens to hamper the near-term growth and adoption of sUAS by public safety agencies as an important tool to help save lives and protect property.

SOLUTION

As previously stated, public safety drone operators need clear guidance for their planning purposes. Continual allegations surrounding Chinese sUAS technology is only serving to confuse public safety drone users. If U.S. lawmakers are intent upon banning Chinese drones, they should take swift action to provide the needed clarity and guidance for the public safety sector before those agencies invest deeper into Chinese sUAS technology.

Accordingly, guidance that has been issued, such as *Cybersecurity Best Practices for Operating Commercial Unmanned Systems (UASs)* from the Cybersecurity and Infrastructure Security Agency (CISA) at DHS on June 11, 2019, should be formally indoctrinated into the standard operating procedures and workflows of public safety drone programs – especially for those agencies flying potentially security-sensitive missions with Chinese sUAS.

Lawmakers must recognize that a significant number of U.S. public safety agencies and local jurisdictions have already adopted Chinese technology for their aviation operations. DJI has become the de-facto industry standard in a public safety drone sector where formal standards have not yet been created. If Chinese-made sUAS are no longer be acceptable for use by U.S. public safety agencies, then what solutions are poised to fill the void left by DJI?

U.S. firms such as Altavian, FLIR, Impossible, Skydio, and others are working to develop viable solutions which could potentially be used in the public safety sector. However, the ability for any firm to achieve the level of consistency, reliability, accuracy, and at a price that public safety drone operators have become accustomed to from DJI remains highly questionable.

¹² Katy Stech Ferek, The Wall Street Journal, Lawmakers Seek Ban on Chinese Drone Purchases by Federal Agencies, September 18, 2019

Any potential Chinese drone ban must include provisions establishing either a buy-back and/or trade-in program for those agencies who have already invested heavily in Chinese UAS technology. A ban should also establish a sunset clause allowing those departments currently using Chinese-technology (including the DOI) to continue said use through the end of the aircraft's projected service life – at least for non-security sensitive operations.

DJI could potentially seek to preserve its market share by going "all-in" and establishing a U.S.headquartered UAS company with a proverbial Chinese wall severing all direct links between Shenzhen and North America. Whether DJI is willing to go to such lengths, and whether such action would be acceptable to U.S. lawmakers, remains uncertain.

In the end, brand loyalty is fickle. This is never truer than in the technology sector where a company is only as good as its latest product offerings. According to DRONERESPONDERS *Fall 2019 Public Safety UAS Survey* data, brand ranked lowest out of the 10 attributes survey respondents said they valued when selecting UAS technology for their public safety drone program.

Potentially even more foreboding for DJI is additional data uncovered by DRONERESPONDERS.

FIGURE 3: SCENARIO: THE YEAR IS 2022 AND FOUR DRONES HAVE NEARLY IDENTICAL QUALITY, CAPABILTIES, AND PRICE POINTS. ONE DRONE IS FROM A CHINESE-HQ COMPANY, ONE DRONE IS FROM A FRENCH HQ-COMPANY, ONE DRONE IS FROM A GERMAN HQ-COMPANY, AND ONE DRONE IS FROM A U.S.-HQ COMPANY. WHICH DRONE WOULD YOU BE MOST INCLINED TO PURCHASE IF ALL OTHER THINGS WERE EQUAL?



SOURCE: DRONERESPONDERS Fall 2019 Public Safety UAS Survey, September 2019

Fall 2019 Public Safety UAS Survey participants were presented with a scenario based in the year 2022. In this scenario, there were four drones possessing nearly identical quality, capabilities, and price points. One drone was from a Chinese-headquartered company, one drone was from a French-headquartered company, one drone was from a German-headquartered company, and one drone was from a U.S.-headquartered company.

Participants were asked which drone they would be most inclined to purchase if all other thing were equal?

9% of respondents said they were unsure which drone they would purchase, 3% claimed they would purchase the Chinese drone, and 88%, (196 of the 224 public safety respondents) said they would purchase the drone from the U.S.-headquartered company.

Regardless of what steps lawmakers take, these survey responses may point to an ominous future for Chinese drone companies in the U.S. public safety sector.

CONCLUSIONS

- 1) U.S. public safety agencies need clarity from Washington D.C. surrounding which sUAS and technology they should be embracing as they continue to implement and build drone programs for their organizations.
- 2) U.S. public safety drone program managers and operators flying potentially securitysensitive missions with Chinese sUAS should heed the *Cybersecurity Best Practices for Operating Commercial Unmanned Systems (UASs)* DHS guidance from CISA, June 11, 2019, and incorporate the recommended safeguard measures into their operational workflow.
- 3) DJI's reign as king of the global sUAS market as well as the U.S. public safety sector will continue for the immediate term as organizations of all types and sizes continue to embrace DJI's capable, reliable, and reasonably priced product offerings.
- 4) Despite DJI's dominance of the UAS marketplace, public safety brand affinity toward DJI remains tenuous. The door is open for another UAS solution provider to seize market share if they can match DJI's product offering at a similar price point.
- 5) Bipartisan pressure from U.S. lawmakers in the form of the proposed *American Security Drone Act of 2019* currently represents the greatest threat to DJI's dominance of the public safety UAS sector.
- 6) U.S. lawmakers should be cognizant that a ban on the purchase and/or use of Chinese drone technology by public safety agencies may have severe unintended consequences which could outweigh intended security benefits in the near term.
- 7) The overwhelming majority of U.S. public safety professionals would prefer to be flying sUAS's made by a U.S. company rather than drones originating from a foreign firm.

SURVEY METHODOLOGY

The DRONERESPONDERS *Fall 2019 Public Safety UAS* represents a quantitative method, cross-sectional, self-selected, online questionnaire survey conducted by AIRT, Inc. and administered using SurveyMonkey technology between August 27 and September 15, 2019.

The survey was directly promoted to a highly-targeted, known, yet self-selecting, group of public safety UAS professionals representing a wide cross-section of the public safety UAS sector. Total responses per question range between 223 and 274 respondent answers. The margin of error for this survey is projected to be +/-5%.

SOURCES AND ADDITIONAL RESOURCES

- 1. The Functions and Costs of Law Enforcement Aviation Units, 2007, Lynn Langdon, Bureau of Justice Statistics
- 2. Considerations and Recommendations for Implementing an Unmanned Aircraft Systems (UAS) Program, December 2016, National Institute of Justice
- 3. US Army calls for units to discontinue use of DJI equipment, August 4, 2017, Gary Mortimer, sUAS News,
- 4. The Army Grounds Its DJI Drones Over Security Concerns, August 7, 2017, Lily Hay Newman, Wired
- 5. From Startup to Empire: The Evolution of DJI Drones, May 14, 2018, Ali Crane, Dronelife
- 6. 2018 Drone Market Sector Report, September 2018, Colin Snow, Skylogic Research
- 7. Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice, March 4, 2019, Arjun Kharpal, MSNBC
- 8. DHS warns of 'strong concerns' that Chinese-made drones are stealing data, May 20, 2019, David Shortell, CNN
- 9. DHS warns of data threat from Chinese-made drones, May 20,2019, David Shepardson, Reuters
- 10. DJI Welcomes Mark Aitken To Its Washington Advocacy Team, May 30, 2019, DJI Newsroom
- 11. *DJI Letter to U.S. Senate Subcommittee on Commerce, Science, and Transportation, June 24, 2019, Mario Rebello, Vice President and Regional Manager, North America, DJI Technology, Inc.*
- 12. DJI unveils plans to start assembling drones in US amid security concerns, June 26, 2019, Cyrus Lee, ZDNet
- 13. Flight Test and Technical Evaluation Report: DJI UAS Mission Functionality and Data Management Assurance Assessment, July 2, 2019, Mark L. Batherick and Brad Koeckeritz, U.S. Department of the Interior, Office of Aviation Services
- 14. U.S. Federal Agency Validates and Approved DJI's High-Security Solution for Government Drone Programs, July 7, 2019, DJI Newsroom
- 15. Why is DJI getting the Huawei treatment? August 26, 2019, Jackson Barnett, Cyberscoop
- 16. Fall 2019 Public Safety UAS Survey, September 16, 2019, DRONERESPONDERS
- 17. Lawmakers Seek Ban on Chinese Drone Purchases by Federal Agencies, September 18, 2019, Katy Stech Ferek, The Wall Street Journal

ABOUT

DRONERESPONDERS is the world's fastest growing non-profit program supporting public safety UAS. The DRONERESPONDERS mission is to facilitate preparedness, response and resilience using unmanned aircraft systems and related technologies operated by public safety, emergency management, and non-governmental volunteer organizations around the world. The DRONERESPONDERS Public Safety Alliance is a 501(c)3 non-profit operating program of <u>AIRT</u>, Inc. For more information on DRONERESPONDERS, please visit: <u>http://droneresponders.org</u>

