U.S. Immigration and Customs Enforcement | Homeland Security Investigations
SAC Intelligence Program Los Angeles

INTELLIGENCE BULLETIN

ICE-IL-17-0019

(U) Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government

9 August 2017

(U//FOUO) Special Agent in Charge Intelligence Program (SIP) Los Angeles is generating this product in response to several requests for information received from the intelligence and law enforcement communities. It is based on information derived from open source reporting and a reliable source within the unmanned aerial systems (UAS) industry with first and secondhand access. The date of information is 9 August 2017.

(U//LES) SIP Los Angeles assesses with moderate confidence that Chinese-based company DJI Science and Technology is providing U.S. critical infrastructure and law enforcement data to the Chinese government. SIP Los Angeles further assesses with high confidence the company is selectively targeting government and privately owned entities within these sectors to expand its ability to collect and exploit sensitive U.S. data.

(U) Since 2015, DJI has targeted a number of U.S. companies in the critical infrastructure and law enforcement sectors to market its UAS. As of July 2017, at least ten large companies and organizations operating in the railroad, utility, media, farming, education, and federal law enforcement sectors have already purchased and begun using DJI UAS. The most frequent uses include mapping land, inspecting infrastructure, conducting surveillance, and monitoring hazardous materials.[1]

(U//LES) DJI sells group one category (under five pounds) UAS intended for consumer and professional use. The UAS operate on two Android smartphone applications called DJI GO and Sky Pixels that automatically tag GPS imagery and locations, register facial recognition data even when the system is off, and access users' phone data. Additionally, the applications capture user identification, e-mail addresses, full names, phone numbers, images, videos, and computer credentials. Much of the information collected includes proprietary and sensitive critical infrastructure data, such as detailed imagery of power control panels, security measures for critical infrastructure sites, or materials used in bridge construction. According to the source of information (SOI), DJI automatically uploads this information into cloud storage systems located in Taiwan, China, and Hong Kong, to which the Chinese government most likely has access.[2] SIP Los Angeles assesses with high confidence a foreign government with access to this information could easily coordinate physical or cyber attacks against critical sites.

— (U//LES) After downloading DJI applications, users are prompted to acknowledge DJI's terms and conditions, which grant DJI permission to own and exploit user data. The agreement reads, "Please note that if you conduct your flight in certain countries, your flight data might be monitored and provided to the government authorities according to local regulatory laws."[3]

— (U) In April 2016, a DJI spokesperson announced in a briefing for Chinese and foreign journalists that the company complies with Chinese government requests to hand over data collected in China, according to the *New York Times*. The same article stated DJI could also give the government data from flights in Hong Kong. The spokesperson revealed for the moment DJI was uncertain what they would decide to do with the data and which government departments they would give it to because it was a continuing discussion.[4]

— (U//FOUO) In August 2017, the U.S. Army issued a memo to its units to immediately discontinue the use of DJI UAS due to an increased awareness of cyber vulnerabilities associated with DJI products. Although the vulnerabilities are not specified in the memo, it could refer to how DJI is using the data collected. The memo also references a May 2017 U.S. Navy memo addressing operational risks related to DJI products.[5]

— (U//LES) The Chinese government is using DJI UAS as an inexpensive, hard-to-trace method to collect on U.S. critical assets, according to the SOI. The Chinese government directorates most likely receiving the data from DJI's cloud are the offices responsible for defense, critical infrastructure, traffic controlling, and cyber offense, according to the same source.[6]

(U) DJI's Target Customers

(U//LES) DJI targets key federal, state, and local law enforcement entities through exhibits at trade shows across the United States. These shows are an attractive outlet for DJI to market its UAS since a large number of resellers and product representatives are present at each show. Since 2015, DJI has specifically targeted Sheriff's Departments and Search and Rescue teams that attended the shows.[7]

— (U) In January 2017, the Los Angeles Sheriff's Department announced they would begin deploying UAS under limited circumstances, including search and rescue missions, explosive ordnance detection missions, disaster response, barricaded suspects, hostage situations and other high-risk tactical operations, hazardous materials incidents, and fire related incidents.[8] The Department is using a DJI Inspire UAS.[9]

— (U//LES) The Department of Homeland Security is currently building a National Bio and Agro-Defense Facility in Manhattan, Kansas to study diseases that threaten America's animal agricultural industry and public health.[10] The contractor building the facility is using DJI UAS to assist with construction layout and provide security during construction.[11]

(U//LES) SIP Los Angeles assesses with high confidence that outside of DJI's goal to attain law enforcement customers, DJI's criteria for selecting accounts to target appears to focus on the account holder's ability to disrupt critical infrastructure. As a result, DJI has amassed customers such as American Water[USPER], Union Pacific[USPER], and American Electric Power[USPER], some of the biggest utility and transportation companies in the United States.[12]

— (U//LES) DJI is particularly interested in exploiting data from two critical infrastructure sectors: U.S. railroads and utilities. In early 2017, the company invited senior level management from critical infrastructure sectors to a three-day conference at its new innovation center in Silicon Valley, California. The 12,000 square foot facility is the largest UAS training center on the West Coast and is designed for research, development, and training. DJI is inviting key customers to attend training sessions and conferences to further encourage U.S. companies to purchase and use DJI systems.[13]

— (U//LES) Specifically, DJI is focused on targeting utility companies responsible for providing drinking water in New Jersey, New York, Los Angeles, and Chicago, as well as railway companies in Omaha, Nebraska; Los Angeles, California; and Dallas-Fort Worth, Texas.[14]

— (U//LES) DJI is also interested in targeting Fort Riley, Kansas and the Tennessee-based Milan Army Ammunition Plant where munitions and weapons materiel are stored.[15]

(U//LES) Furthermore, the Chinese government is likely using information acquired from DJI systems as a way to target assets they are planning to purchase. For instance, a large family-owned wine producer in California purchased DJI UAS to survey its vineyards and monitor grape production. Soon afterwards, Chinese companies began purchasing vineyards in the same area. According to the SOI, it appeared the companies were able to use DJI data to their own benefit and profit.[16]

— (U//LES) In 2017, DJI began offering clients a normalized difference vegetation index (NDVI) infrared scanner to use with UAS. The NDVI picked up reflective images of leaves to calculate the nitrogen levels of plants. The device provided the user with details such as how much nitrogen to add to the soil to optimize plant growth. It also collected information on the location and lifecycle stages of food.[17]

— (U//LES) As of May 2017, the only customers using the NDVI scanner were wine producers along the coast of California; however the scanner would work with cash crops. SIP Los Angeles assesses with low confidence if the cash crops industry began using the scanner, it could allow China the opportunity to influence the cash crop market and futures.[18] SIP Los Angeles further assesses with low confidence it could provide China insider information on the ability to disrupt and degrade the United States' food supply.

(U) Dumping Techniques

(U) In 2015, DJI aggressively dropped its prices by as much as 70 percent in less than one year, effectively forcing its main competitors out of the market. Since that time, DJI's biggest competitors, Parrot in France, 3D Robotics[USPER] in the U.S., and Yuneec in China, all stopped production due to their inability to match DJI's prices.[19] Using dumping techniques, DJI was able to sell category one UAS in the United States for approximately $900 USD. Comparatively, other group one category UAS with the same level of technology sold for $3,500 USD.[20]

(U) What is "Dumping"?

(U) The illegal practice of exporting a product at a price lower than the cost to manufacture the product or lower than the price the manufacturer would charge in its own home market.

— (U) Since DJI creates, manufactures, and tests its UAS in its own facilities in Shenzhen, it is able to keep costs much lower than its foreign competitors, who have higher operating costs and often have to travel across the world to build their products.[21]

— (U) Lower manufacturing costs, combined with illegal dumping tactics, have effectively given DJI a monopoly in the category one UAS market in the United States. As a result, U.S. companies have fewer options and are more likely to purchase DJI UAS.

— (U//LES) From August 2016 to August 2017, DJI imported 10,321 shipments into the United States, 1,741 of which entered through the Ports of Los Angeles and Long Beach. Comparatively, from August 2015 to August 2016, DJI imported 2,873 shipments into the United States.[22] In a one year period, DJI was able to drastically increase shipments of UAS to the United States market, likely due to its low prices and lack of competition.

(U) Future Plans

(U//LES) In February 2017, DJI began developing an application that would digitize UAS pilot logs. The app would store the pilot's name, flight time, flight hours, flight route, and mission planning details. Once the app is fully developed, it will send pilot and flight information to the cloud based storage system where all the other information is stored.[23]

(U//LES) As of May 2017, DJI was attempting to add satellite communications to their UAS so operators were not reliant on cellular towers for the control stations. Satellite communications would allow real-time transmissions of information in rural areas or areas without adequate cellular towers.[24]

(U) Analytic Comment

(U//LES) SIP Los Angeles assesses with high confidence the critical infrastructure and law enforcement entities using DJI systems are collecting sensitive intelligence that the Chinese

government could use to conduct physical or cyber attacks against the United States and its population. Alternatively, China could provide DJI information to terrorist organizations, hostile non-state entities, or state-sponsored groups to coordinate attacks against U.S. critical infrastructure. The UAS capture close-up imagery and GPS information on water systems, rail systems, hazardous material storage systems, first responders' activity, and construction of highways, bridges, and rails.

(U) Tracked by: ICE-10000-17; ICE 15000-17

(U) Reporting Notice: This Intelligence Bulletin was prepared by Homeland Security Investigations, Los Angeles. Comments and queries may be directed to the Homeland Security Investigations Los Angeles Chief Intelligence Officer Mark Porter at INTEL.SACLA@ice.dhs.gov, or by phone at (562) 256-3411. The Joint Intelligence Operations Center (JIOC) is available 24/7 at 202-732-5156/57, NSTS: 263-2178.

(U) FEEDBACK: For general comments or questions related to the dissemination of this document, please e-mail the HSI Intel Production inbox at HSIIntelProduction@ice.dhs.gov.

1 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
2 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
3 (U) Internet Site; Author: Paul Mozur; Site: NY Times; Title: (U) China Drone Maker Says it May Share Data with State; Posting Date: 20 Apr 2016; Page/Paragraph Number: N/A; URL: https://www.nytimes.com/2016/04/21/world/asia/dji-drones-china.html; Date of Access: 25 Jul 2017.
4 (U) Internet Site; Author: Paul Mozur; Site: NY Times; Title: (U) China Drone Maker Says it May Share Data with State; Posting Date: 20 Apr 2016; Page/Paragraph Number: N/A; URL: https://www.nytimes.com/2016/04/21/world/asia/dji-drones-china.html; Date of Access: 25 Jul 2017.
5 (U) Originator: Department of the Army; Report Number: N/A; Tracking Number: N/A; Pub Date: 2 Aug 2017; DOI: 2 Aug 2017; Title: (U//FOUO) Discontinue Use of Dajiang Innovation (DJI) Corporation Unmanned Aircraft Systems; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//For Official Use Only.
6 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
7 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
8 (U) Originator: County of Los Angeles Sheriff's Department; Report Number: 761551 N25A- SH-AD (11/90); Tracking Number: N/A; Pub Date: 10 Jan 2017; DOI: 10 Jan 2017; Title: (U//FOUO) Utilization of Unmanned Aircraft System (UAS) Platform; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified.
9 (U) Originator: Los Angeles Sheriff's Department Criminal Intelligence Bureau Intelligence Analyst; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: 3 Aug 2017; Title: (U) E-Mail on LASD Drones; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
10 (U) Internet Site; Author: N/A; Site: DHS; Title: (U) National Bio and Agro-Defense Facility; Posting Date: N/A; Page/Paragraph Number: N/A; URL: https://www.dhs.gov/science-and-technology/national-bio-and-agro-defense-facility/; Date of Access: 3 Aug 2017.
11 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.

12 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
13 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
14 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
15 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
16 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
17 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
18 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
19 (U) Internet Site; Author: April Glaser; Site: Recode; Title: (U) DJI is Running Away with the Drone Market; Posting Date: 14 Apr 2017; Page/Paragraph Number: N/A; URL: https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast; Date of Access: 24 Jul 2017.
20 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
21 (U) Internet Site; Author: April Glaser; Site: Recode; Title: (U) DJI is Running Away with the Drone Market; Posting Date: 14 Apr 2017; Page/Paragraph Number: N/A; URL: https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast; Date of Access: 24 Jul 2017.
22 (U) Originator: U.S. Immigration and Customs Enforcement Data Analysis and Research for Trade Transparency System (DARTTS); Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: 9 Aug 2017; Title: N/A; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
23 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.
24 (U) Originator: Immigration and Customs Enforcement, HSI Los Angeles CPIC Source of Information; Report Number: N/A; Tracking Number: N/A; Publication Date: N/A; Date of Information: Dec 2016 - Jul 2017; Title: (U) Interview with CPIC Special Agent; Page/Paragraph Number: N/A; Overall Source Classification: Unclassified//Law Enforcement Sensitive.