Security Concerns with DJI Products

Andrew V. Shelley [*]

Aviation Safety Management Systems Ltd

Revised 12 January 2020

1 Introduction

This paper summarises key security concerns that have arisen and continue to arise with drones manufactured by Chinese company Da Jiang Innovations [DJI]. Section 2 provides a very brief overview of a typical DJI drone system. Section 3 provides a summary of some key events relating to security vulnerabilities in DJI products. It starts with the concerns of the US, Australia, and New Zealand military; and the measures adopted by those organisations in response. Section 3 then presents selected vulnerabilities identified by security researchers, and DJI's efforts to address the identified vulnerabilities. Section 4 summarises general UAS security warnings issued by the US Department of Homeland Security. Some of these warnings are directed to drones in general, while one warning is specifically directed at Chinese-made drones. Section 5 addresses the "Government Edition" firmware which DJI claims "meets the stringent requirements of the government sector for data management, risk mitigation, and enterprise-level data sharing control" (DJI, 2019a). Tellingly, the US Department of the Interior recommends the adoption of additional controls. Section 6 which provides DJI's responses to the some of the identified vulnerabilities, in particular the implementation of a Local Data Mode and recommended data security practices. Section 7 provides conclusions.

2 Overview of DJI Drone Systems

The typical DJI implementation of a DJI drone system consists of:

- the drone;
- a remote controller; and
- a tablet or other smart device running the DJI GO app.

The drone is has an onboard computer that controls the motors in response to control and sensor inputs. The drone's computer runs a particular version of firmware on an operating system. The Mavic (prior to the Mavic 2) utilised the Android operating system.

The drone communicates with the remote controller via a radio link. The drone is 'bound' to a particular remote controller so that it will ordinarily only accept commands from a single controller. The remote controller converts commands from the pilot (via the control sticks) or the DJI GO app into control signals to broadcast to the drone. The remote controller also receives telemetry and a video signal from the drone. The radio bands used are the Industrial Scientific and Medical (ISM) bands, particularly 2.4GHz and 5.8GHz.

The remote controller then communicates via WiFi with the smart device running the DJI GO app. If internet connection is enabled, the DJI GO app may communicate with the internet, including to obtain map updates, synchronise data, etc.

[*] Email address:andrew@asms.co.nz.

3 Key Events

3.1 Military use of DJI Products

In a memorandum dated 24 May 2017, the US Navy warned of operational risks regarding the DJI family of products (Department of the Navy, 2017). The memo notes potential cyber vulnerabilities and recommends training in areas that are not operationally sensitive, avoiding connecting the ground control station (GCS) to military networks, and only connecting to the internet if “all images, video, and flight records are deleted from the GCS cache and micro-SD cards prior to connection to the web.”

The US Army followed suit in a memorandum apparently issued on or before 2 August 2017, with a directive to “cease all use, uninstall all DJI applications, remove all batteries/storage media from devices, and secure equipment for follow on direction” (Department of the Army, 2017). The directive refers to a classified Army Research Laboratory report titled “DJI UAS Technology Threat and User Vulnerabilities,” dated 25 May 2017, and the 24 May 2017 Navy memorandum.

On becoming aware of the US Army memorandum, the Australian Defence Force suspended use of DJI products on 9 August 2017 (Australian Defence Force [ADF], 2019). After completing a “cyber vulnerability assessment” and implementing new procedures, the suspension was lifted on 21 August 2017. In August 2018, the ADF was reported as taking delivery of further DJI drones, but with the caveat that “there was a review done working in conjunction with the US” and the drones “will only be used in unclassified training scenarios” (Levick, 2018). In November 2018 the Australian Army completed the roll-out of 350 DJI Phantom 4 drones to every unit (ADF, 2019).

On 9 August 2017, the Department of Homeland Security Special Agent in Charge Intelligence Programme Los Angeles released an intelligence bulletin warning that DJI was likely providing law enforcement and infrastructure data to China (Department of Homeland Security [DHS], 2017). This analysis was based in part on the US Army’s memo, reports from DJI that it could provide data to the Chinese government, and a number of classified interviews. Three months later, on becoming aware of the intelligence bulletin, DJI issued a press release rejecting the bulletin as “profoundly wrong” (DJI, 2017c).

In early March 2018 the NZDF confirmed that it would continue to utilise DJI products, but that as a security mitigation the drones were “never connected to the Internet or NZDF networks, and are not for deployment” (Bayer, 2018). Verbal confirmation was obtained in August 2019 that this policy remains in place (H. Robinson, personal communication, 5 August 2019).

Notwithstanding these concerns, a Voice of America investigation identified that US Special Forces units continued to purchase DJI drones in 2018 and 2019 (Babb & Xie, 2019). One document seen by Voice of America claimed that software had been developed ”and implemented to eliminate the cyber security concerns that are inherent to the DJI Mavic Pro.”

On 20 December 2019, the National Defense Authorization Act for Fiscal Year 2020 became law, prohibiting the US military from operating or purchasing any drones (a) manufactured in the Peoples’ Republic of China, (b) using components manufactured in China, (c) using a ground control system or software developed in China, or (d) “uses network connectivity or data storage located in or administered by an entity domiciled in [China]” (s 848). The only exemptions are for counter-UAS testing and training or “intelligence, electronic warfare, and information warfare operations, testing, analysis, and training.”

In December 2019 the Japanese Coast Guard was reported as planning to “stop using and procuring Chinese-made drones in fiscal 2020 ”(Nikkei staff, 2019).

3.2 Security Researchers

Amid growing concerns of bugs and vulnerabilities in DJI’s software, on 28 August 2017 DJI announced a “bug bounty” programme whereby it would pay security researchers a reward for identifying threats (DJI, 2017d). Security researcher Kevin Finisterre reports on how, as part of researching vulnerabilities, he was able to access unencrypted flight logs and personally identifiable information such as drivers licences and passports (Finisterre, 2017).

In response to the above revelations, additional revelations as to the key for DJI's SSL Certificate being publicly available on GitHub, other data being publicly available on a server, and the DHS memo of 9 August 2017, in November 2017 DJI released a statement that it had addressed all substantive concerns identified (DJI, 2017e).

In March 2018, Check Point Research discovered a vulnerability that would enable an attacker to gain access to a user's DJI account, and consequently access to (Vanunu, Barda & Zaikin, 2018):

- "Flight logs, photos and videos generated during drone flights, if a DJI user had synced them with DJI's cloud servers.
- A live camera view and map view during drone flights, if a DJI user were using DJI's FlightHub flight management software.
- Information associated with a DJI user's account, including user profile information."

A detailed description of the vulnerability and how it could be exploited is provided in (Vanunu et al., 2018), published two months after the vulnerability had been patched (Townsend, 2018).

In an effort to reassure users of DJI products, DJI hired San Franciso-based Kivu Consulting Inc to assess its data and security practices. In April 2018 DJI publicly released a summary of findings (Brush, 2018; DJI, 2018), while the full technical report was made available to some technology reporters on the condition that they did not reproduce key parts of the report (Cameron, 2018). Kivu conducted its analysis using independently purchased DJI drones, and independently purchased android and iOS devices with apps downloaded from the respective app store. It appears that Kivu did not attempt to reverse-engineer or decompile the code in the drones they purchased, but DJI did provide them with access to the relevant code repositories for the GO 4 app (Brush, 2018).

Kivu did find that when the DJI GO 4 application is launched " a file is sent from the user's phone to an Alibaba server, ... containing details about the operating system of the operator's mobile device and the SSID (or name) of the connected Wi-Fi network" (Cameron, 2018). For the US products tested, the Alibaba server was US-based, although that is no guarantee that the server won't be accessed by Alibaba in China.

Kivu also found that (Cameron, 2018):

> DJI's GO 4 app did communicate with servers in China through Bugly, an app used to report crashes. Files within a database named "Bugly_db_" include a table that "contained the last IP address the mobile device was connected to, along with the International Mobile Equipment Identity ('IMEI') of the mobile device".

In contrast to the above findings, Kivu also makes the point that no information is uploaded to the internet without the user choosing to upload (Brush, 2018):

> DJI drones record flight logs and store them on the drones themselves and within the GO 4 application. These files are stored in a proprietary format designed by DJI. Flight logs consist of GPS location, gimbal information, photo and video capture time,thumbnails of images or video taken during flight,detailed aircraft data, flight time, and battery information. Neither DJI drones nor the GO 4 application automatically upload or transmit flight logs to any remote server. Users must affirmatively choose to upload, or "sync," flight logs within the GO 4 application.

The same assurances are given by Kivu in respect of images and videos recorded by the drone.

4 General UAS Security Warnings

On 22 May 2018, the DHS's Office of Cyber and Infrastructure Analysis warned that (DHS, 2018):

> [UAS] are vulnerable to exploitation. Many commercial UAS variations, for example, currently communicate with ground stations and operators using unencrypted feeds. This can allow a malicious actor to intercept and review data sent to and from the UAS.
>
> Malicious actors can target UASs belonging to critical infrastructure operators, using vulnerabilities within UAS software or firmware in order to compromise the systems and access sensitive networks and information. Malware can also be pre-installed in a UAS application or in UAS software or firmware by a malicious actor with access to the UAS' supply chain. Likewise, embedded malware could compromise the computer, phone, or tablet where the application resides. A malicious actor cancompromise any one of these systems to extract sensitive data, further infiltrate any networks the UAS interacts with, and take control of the victim's UAS.

On 23 May 2018, the US Deputy Secretary of Defense issued the following direction to all US Department of Defense units (Kesteloo, 2018):

> "Effective immediately you must suspend purchases of [commercial-off-the-shelf (COTS)] UAS for operational use until the DoD develops a strategy to adequately assess and mitigate the risks associated with their use. In addition you must suspend the use of COTS UASs until the DoD identifies and fields a solution to mitigate known cybersecurity risks."

In May 2019, DHS's Cybersecurity and Infrastructure Security Agency again issued an alert warning of concerns that Chinese-made drones are a "potential risk to an organization's information," and "contain components that can compromise your data and share your information on a server accessed beyond the company itself" (Shortell, 2019).

5 DJI Government Edition Firmware & US DOI Recommendations

In 2015 the US Department of the Interior (DOI) Office of Aviation Services (OAS) determined that DJI did not meet the DOI's data management security standard

> to decline and lock out any device information sharing including telemetry through aircraft, software or applications preventing any automated uploads or downloads (Bathrick & Koeckeritz, 2019).

In 2017, OAS was approached by DJI with an offer to collaborate on the development of a solution that would meet the DOI's UAS data management and risk mitigation requirements. DJI consequently developed the "Government Edition" (GE) software, firmware and hardware for the DJI Matrice 600 Pro and DJI Mavic Pro drones.

Testing of the GE software was conducted by a third party consultancy Drone Amplified. The company does not have a background in security testing, but has developed drone control software. The test procedure involved setting a laptop as the WiFi hotspot to which the flight controller connected, running the programme Wireshark on that laptop, and monitoring all requests for internet access. As a result of the testing Drone Amplified identified three instances where GE software 'pinged' DJI servers. It was also identified that a public version of the DJI GO app could connect to the DOI's Mavic Pro "and get video feed, position, and status. This has the potential to leak flight data to DJI Servers, as these apps are not secured" (Detweiler & Beachly, 2018). At

Drone Amplified's request, the Mavic Pro firmware was updated so that this no longer occurred.

Specific recommendations from the OAS following the evaluation are (Bathrick & Koeckeritz, 2019, p.2):

> It is recommended GE (Pilot App version 1.3 19743, Assistant 2 GE Version 9-5) equipped Matrice 600 Pro and Mavic Pro aircraft be authorized for Interior fleet and contract use in accordance with additional risk mitigation practices ...
>
> *While the tested GE version met Interior requirements, 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.*
>
> Continued collaboration with federal and industry partners to identify additional solutions that meet DOI data management assurance requirements and are easier and less costly to sustain and scale is also recommended. [emphasis added]

In October 2019 the Idaho National Laboratory (INL) released the results of a preliminary and limited scope evaluation of the cybersecurity risks associated with four drones including the DJI Mavic Pro and the DJI Matrice 600 Pro (Idaho National Laboratory, 2019). INL was unable to detect any data leakage during the limited scope analysis, but also noted that the GE solution is only an interim measure. As longer-term actions, INL recommended reverse-engineering software, hardware, and an operational system to assess data security.

Notwithstanding these findings and recommendations, on Wednesday 30 October 2019 the DOI grounded all "drones manufactured in China or made from Chinese components," except for "emergency purposes, such as fighting wildfires, search and rescue, and dealing with natural disasters that may threaten life or property" (Newcomer, 2019). It is unclear whether this action is a result of new security threats or whether it is a result of pressure from US politicians.

6 DJI Responses

6.1 DJI Local Data Mode

In response to the moves by the US and Australian military, on 14 August 2017 DJI announced that it was"developing" a "local data mode that stops internet traffic to and from its flight control apps, in order to provide enhanced data privacy assurances for sensitive government and enterprise customers" (DJI, 2017a). This mode subsequently went "live" on 2 October 2010 (DJI, 2017b). The DJI press release states:

> Since Local Data Mode blocks all internet data, the DJI Pilot app will not be able to detect the location of the user, show the map and geofencing information such as No Fly Zones and temporary flight restrictions. In addition, it will not notify drone operators of firmware updates. Telemetry data on flight logs such as altitude, distance or speed will remain stored on the aircraft even if the user deactivates Local Data Mode.
>
> Whether Local Data Mode is activated or not, photos and videos captured by the user are always stored on the drone's SD card and are only shared if the user chooses to upload them online to the SkyPixel community, social media or other websites.
>
> When using Local Data Mode, drone operators are reminded that they are solely responsible for the safety of their flight operation and that they understand that features that may enhance and support the safety of their operations, but that rely on internet connectivity, are no longer available.
>
> Drone operators can enable Local Data Mode by opening the DJI Pilot app, clicking on "Activate LDM Mode" and entering a password which will

> be required to deactivate Local Data Mode when they decide to go online again.
>
> New drones will still have to be activated first by logging into the user's DJI account with an email and a password. To ensure the drone has the latest firmware, users can download and update it while they have internet connectivity before re-activating Local Data Mode.

The description of Local Data Mode is consistent with the procedures understood to have been adopted by NZDF.

6.2 DJI Data Security Recommendations

On 23 May 2019, DJI responded to the DHS industry alerts with the statement that "your data is not our business" (DJI, 2019b). As part of this statement, DJI also released five data security recommendations:

1. Deactivate Internet Connection from Devices Used to Operate the UAS
2. Take Precautionary Steps Before Installing Updated Software or Firmware
3. Remove the Secure Digital Card from the Main Flight Controller/Drone
4. If an SD Card is Required to Fly the Drone, Remove All Data from the Card After Every Flight
5. Encrypt and Password Protect Your Data

The details of DJI's recommendations are provided in Appendix A. The recommendation to deactivate the internet connection specifically references the Local Data Mode.

7 Conclusion

DJI UAS have a demonstrated history of cyber vulnerabilities. While these vulnerabilities have ultimately been addressed by DJI by way of firmware updates, future firmware updates are equally capable of introducing new vulnerabilities.

A specific "Government Edition" has been developed for some DJI craft, but the need to test and validate every update means that this is not a viable long term solution.

Policies and procedures for the use of DJI drones should be premised on the assumption that the craft are not secure if connected to the internet. In particular, the drones should be operated in Local Data Mode. It would be appropriate for the password that is used to activate and deactivate Local Data Mode to be held centrally and not available to individual drone users.

If the drones utilise the DJI GO app rather than DJI Pilot then Local Data Mode will not be available. In this case, the smart device should be set to airplane mode, and preferably contain no SIM card to prevent connection to the mobile network.

Even with Local Data Mode there is some risk that a future firmware update could re-enable data sharing. The DJI Data Security Recommendations, including centralised approval of updates before installation, and the US Navy recommendations from 2017 both provide an important controls.

Appendix A DJI Drone Industry Data Security Recommendations

A.1 Recommendation #1: Deactivate Internet Connection from Devices Used to Operate the UAS

Our drones do not directly connect to the internet, but instead, use your mobile device or a hotspot-enabled controller with a built-in screen. These devices then connect to the internet for updating apps and firmware, as well as handling other essential functions like updates to our geofencing safety system. We built Local Data mode into our DJI Pilot flight control app, which allows users additional security assurances by stopping any connectivity between DJI's mobile app and the internet. For customers using our DJI GO family of apps, the same level of security can be obtained by activating Airplane mode on your mobile device when flying.

A.2 Recommendation #2: Take Precautionary Steps Before Installing Updated Software or Firmware

All firmware updates for our drones and their accessories go through our company's rigorous software quality assurance process, and our flight control mobile apps are additionally reviewed by Google Play and the App stores to ensure they are secure prior to release. For organizations with large-scale drone deployments, the DJI FlightHub Enterprise fleet management software provides your organization's IT team with full control over the installation of all software and firmware updates to your drone fleet. This means that no mobile app or firmware updates are pushed out unless approved by your IT administrator.

A.3 Recommendation #3: Remove the Secure Digital Card from the Main Flight Controller/Drone

In most cases, our drones and remote controllers feature slots for removable secure digital (SD) memory cards, whose containing data is only accessible to the user. DJI drones do not directly connect to the internet, and no DJI drone or controller is built with a cellular modem installed. Without this data connection, the photos and videos you capture are inherently secure and stay on the SD card. Users should always remove them when the drone is not in use so that if a drone or RC become lost, there is no risk of data leakage.

A.4 Recommendation #4: If an SD Card is Required to Fly the Drone, Remove All Data from the Card After Every Flight

None of DJI's drone products require an SD card to be installed to operate the drone. Regardless, it is considered good practice to remove the card after each flight, retrieve its data, and erase the SD card before the next flight.

DJI's Mavic 2 series drones do feature non-removable in-built memory for storing image data. In this situation, download all footage captured from the internal storage drive, then delete the data stored and format the drive after each flight.

A.5 Recommendation #5: Encrypt and Password Protect Your Data

To provide additional data security assurance, we suggest a fifth addition regarding data encryption and password protection. DJI's newest enterprise drones connect to their controller using our OcuSync 2.0 protocol and are encrypted using the leading AES-256 standard, ensuring critical information exchanged between the drone and its remote is protected.

Our Mavic 2 Enterprise and Mavic 2 Enterprise Dual drones feature password protection. To enhance the security of the drone and this data, users are required to enter a password each time they activate the drone, link a remote controller with the drone, or access the drone's onboard storage. This provides secure access to the drone and its onboard data while protecting that data, even if the drone is lost or physically compromised.

References

Australian Defence Force. (2019, January 29). *Australian Defence Force us of DJI drones and Hikvision and Dahua Surveillance Cameras*. Retrieved from http://www.defence.gov.au/FOI/Docs/Disclosures/304_1819_Documents.pdf

Babb, C. & Xie, H. (2019, September 17). US Military Still Buying Chinese-Made Drones Despite Spying Concerns. *Voice Of America*. Retrieved from https://www.voanews.com/usa/us-military-still-buying-chinese-made-drones-despite-spying-concerns

Bathrick, M. L. & Koeckeritz, B. (2019, July 2). *DJI Unmanned Aircraft System (UAS) Mission Functionality and Data Management Assurance Assessment*. U.S. Department of the Interior, Office of Aviation Services. Retrieved from https://www.doi.gov/sites/doi.gov/files/uploads/oas_flight_test_and_technical_evaluation_report_-_dji_uas_data_managment_assurance_evaluation_-_7-2-19_v2.0.pdf

Bayer, K. (2018, March 2). NZDF has no plans to ground drones banned by US military allies over cyber-safety fears. *NZ Herald*. Retrieved from https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12005158

Brush, D. A. (2018, February 14). Uav data transmission & storage. letter to DJI Research LLC. Retrieved from https://www.dropbox.com/s/u221xdd3w0tkde6/Kivu%20summary%20of%20DJI%20report.pdf

Cameron, D. (2018, April 24). DJI releases security findings it hopes will quash 'chinese spying' fears. *Gizmodo*. Retrieved from https://www.gizmodo.com.au/2018/04/dji-releases-security-findings-it-hopes-will-quash-chinese-spying-fears/

Da Jiang Innovations. (2017a, August 14). DJI Develops Option For Pilots To Fly Without Internet Data Transfer. press release. Retrieved from https://www.dji.com/newsroom/news/dji-develops-option-for-pilots-to-fly-without-internet-data-transfer

Da Jiang Innovations. (2017b, October 2). DJI Launches Privacy Mode For Drone Operators To Fly Without Internet Data Transfer. press release. Retrieved from https://www.dji.com/newsroom/news/dji-launches-privacy-mode-for-drone-operators-to-fly-without-internet-data-transfer

Da Jiang Innovations. (2017c, November 18). DJI Statement On ICE Bulletin. press release. Retrieved from https://www.dji.com/newsroom/news/dji-statement-on-ice-bulletin

Da Jiang Innovations. (2017d, August 28). DJI To Offer 'Bug Bounty' Rewards For Reporting Software Issues. press release. Retrieved from https://www.dji.com/newsroom/news/dji-to-offer-bug-bounty-rewards-for-reporting-software-issues

Da Jiang Innovations. (2017e, November 25). Statement About DJI's Cyber Security and Privacy Practices. press release. Retrieved from https://www.dji.com/newsroom/news/statement-about-dji-cyber-security-and-privacy-practices

Da Jiang Innovations. (2018, April 23). Independent Study Validates DJI Data Security Practices. press release. Retrieved from https://www.dji.com/newsroom/news/independent-study-validates-dji-data-security-practices

Da Jiang Innovations. (2019a, June 24). DJI Creates High-Security Solution For Government Drone Programs. press release. Retrieved from https://www.dji.com/newsroom/news/dji-creates-high-security-solution-for-government-drone-programs

Da Jiang Innovations. (2019b, May 23). Your Data Is Not Our Business. Retrieved from https://content.dji.com/your-data-is-not-our-business/

Department of Homeland Security. (2017, August 9). *Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government*. Homeland Security Investigations,SAC Intelligence Program Los Angeles. Retrieved from https://info.publicintelligence.net/ICE-DJI-China.pdf

Department of Homeland Security. (2018, May 22). *Cybersecurity Risks Posed by Unmanned Aircraft Systems*. Office of Cyber, Infrastructure Analysis (OCIA), National Protection and Programs Directorate. Retrieved from https://info.publicintelligence.net/OCIA-UnmannedAircraftRisks.pdf

Department of the Army. (2017, August 2). Discontinue Use of Dajiang Innovations (DJI) Corporation Unmanned Aircraft Systems. For Official Use Only. Retrieved from https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment/

Department of the Navy. (2017, May 24). Operation risks with regards to DJI family of products. Ser PMA-263/17-183. Retrieved from http://www.documentcloud.org/documents/6579727-Navy-DJI-Assessment-2017.html

Detweiler, C. & Beachly, E. (2018, November 27). *Evaluation of DJI's specialized systems for the Department of the Interior*. Drone Amplified, INC. Appendix D to (Bathrick & Koeckeritz, 2019).

Finisterre, K. (2017, November 16). *Why I walked away from $30,000 of DJI bounty money*. Digital Munition. Retrieved from http://www.digitalmunition.com/WhyIWalkedFrom3k.pdf

Idaho National Laboratory. (2019). *Aviation cyber initiative unmanned aircraft system information security risks limited scope test & evaluation*. INL-LTD-19-55545 Revision 2. Prepared for the U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, Contract DE-AC07-05ID14517. Retrieved from https://www.documentcloud.org/documents/6579764-INL-Drone-Report-Oct-2019.html

Kesteloo, H. (2018, June 7). Department of Defense bans the purchase of commercial-over-the-shelf UAS, including DJI drones effective immediately. *Drone DJ*. Retrieved from https://dronedj.com/2018/06/07/department-of-defense-bans-the-purchase-of-commercial-over-the-shelf-uas-including-dji-drones/

Levick, E. (2018, August 23). Army targets drone literacy with phantom delivery. *Australian Defence Magazine*. Retrieved from https://www.australiandefence.com.au/land/army-targets-drone-literacy-with-phantom-delivery#HpMFXlYVBfPXYExx.99

National Defense Authorization Act for Fiscal Year 2020. (2019). S.1790 - 116th Congress. Retrieved from https://www.congress.gov/bill/116th-congress/senate-bill/1790/text

Newcomer, E. (2019, October 31). Interior Department will stop using non-essential Chinese drones. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2019-10-30/interior-department-will-stop-using-non-essential-chinese-drones

Nikkei staff. (2019, December 9). Japan coast guard to 'eliminate' chinese drones. *Nikkei Asian Review*. Retrieved from https://asia.nikkei.com/Politics/International-relations/Japan-Coast-Guard-to-eliminate-Chinese-drones

Shortell, D. (2019, May 20). DHS warns of 'strong concerns' that Chinese-made drones are stealing data. *CNN International Edition*. Retrieved from https://edition.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html

Townsend, K. (2018, November 8). DJI Drone Vulnerability Exposed Customer Data, Flight Logs, Photos and Videos. *Security Week*. Retrieved from https://www.securityweek.com/dji-drone-vulnerability-exposed-customer-data-flight-logs-photos-and-videos

Vanunu, O., Barda, D. & Zaikin, R. (2018, November 8). DJI Drone Vulnerability. Check Point Research. Retrieved from https://research.checkpoint.com/dji-drone-vulnerability/