Addressing Security Concerns with Chinese Drones and DJI Products

Andrew V. Shelley [*]

Aviation Safety Management Systems Ltd

Revised 29 July 2020[†]

1 Introduction

This paper summarises key security concerns that have arisen and continue to arise with drones manufactured by Chinese company DJI. Section 2 starts with a brief overview of a typical drone system. It then 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 3 provides a summary of some key events relating to security vulnerabilities in DJI products. Section 3.2 starts with the concerns of the US, Australia, and New Zealand military; and the measures adopted by those organisations in response. Section 3.3 then presents selected vulnerabilities identified by security researchers. Section 3.4 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" [3]. The US Department of the Interior recommends the adoption of additional controls even with the Government Edition firmware, and has subsequently grounded all Chinese-manufactured drones.

Section 4 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 5 details particular concerns that may arise in deploying drones within a secure (government) organisational environment in New Zealand. Section 6 provides conclusions.

2 Technical Overview and General Warnings

2.1 Generic Drone Systems and Vulnerabilities

Figure 1 provides a schematic representation of a drone and the associated systems. The remote controller is shown at the left of the figure, and the drone is shown as the group of components inside the dashed line. The remote controller communicates with the drone 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 other control software) 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 drone itself is shown inside the dashed box. The 'heart' of the drone is the flight controller, which is a computer that controls the operation of the drone. The flight

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

[†] Updated to include Synacktiv analysis of DJI GO 4 [1].

controller takes signals from the radio receiver and GPS receiver and provides control signals to the power distribution board. The power distribution board then distributes the control signals and power to the motors via electronic speed controllers (ESCs). The onboard computer also sends data back to the remote controller via the transmitter on the drone.

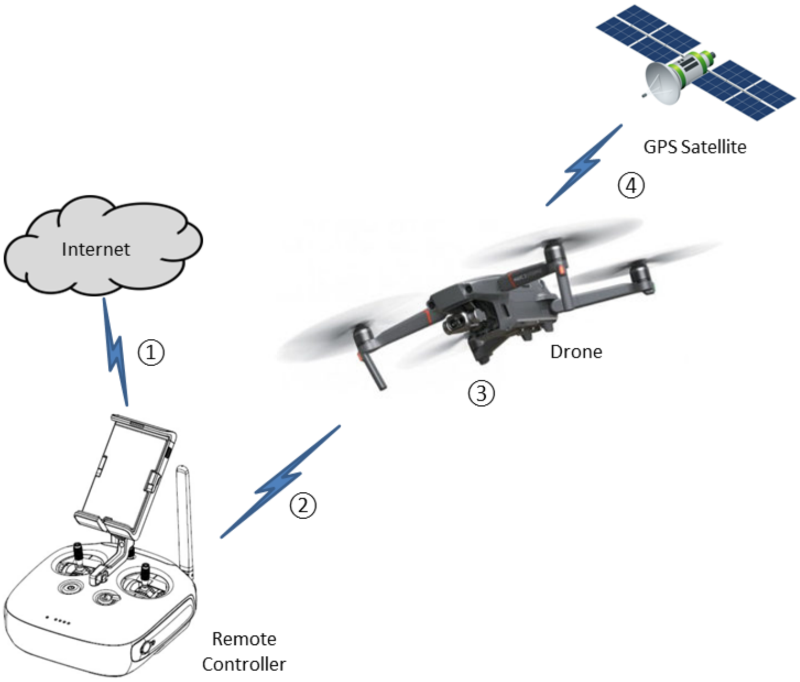

Figure 1. Schematic diagram of drone and associated systems. Numbers in circles denote key areas of vulnerability: ① is potential link to internet; ② is command and control and data link to drone; ③ is the onboard flight controller, which is vulnerable to firmware updates, malware introduced via SD-cards, etc; ④ is the GPS link.

The remote controller *may* connect to the internet. If so, this provides the first major set of vulnerabilities: the signal between the device and the physical network may be intercepted, and once on the internet the data stream might be intercepted by an unauthorised third party. Furthermore, the remote controller may connect to a smartphone or tablet either by WiFi or by cable: a WiFi connection is inherently unsecure unless suitable encryption is utilised with an appropriately strong password.

The second potential vulnerability is the transmissions between the remote controller and the drone: the signal in either directed could be hacked, either providing access to the data stream from the drone, or providing the opportunity for a third party to take control of the drone.

The third potential vulnerability is the flight controller itself. The flight controller runs firmware on top of an underlying computer operating system. Both the firmware and the operating system could potentially contain bugs, malware, or vulnerabilities. Bugs and malware could both be introduced via firmware updates, or via an 'infected' SD card used to transfer data from the drone.

The fourth potential vulnerability is the GPS signal received by the drone. It is possible to overpower this signal and fool the drone into 'believing' that it is in a different location than its true position. This could be used by an adversary to cause the drone to fly away from a pre-programmed surveillance location or to fly sideways into an obstacle. This is a potential issue with all drones relying on GPS, and is not considered further in this paper.

2.2 General UAS Security Warnings

The generic vulnerabilities identified above are reflected in security warnings about UAS generally. For example, on 22 May 2018, the DHS's Office of Cyber and Infrastructure Analysis warned that [4]:

> [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 [5]:

> "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" [6].

3 Concerns with DJI Products

To aid understanding, section 3.1 commences with a brief note on the two apps that can be used in conjunction with DJI drones. Section 3.2 provides a chronology of the use of DJI drones by the US and allied military forces (including Australia and New Zealand). Section 3.3 describes vulnerabilities identified by security researchers, as well as a study commissioned by DJI in the United States to demonstrate the security of its products. Section 3.4 discusses the "Government Edition" firmware released by DJI to address the concerns of the US Department of the Interior (DOI). Section 3.5 then summarises the DOI's subsequent grounding of all drones made in China or made from Chinese components.

3.1 Technical Note

Before delving into the detail of this section, it is important to first note that the DJI remote controller *may* be connected to a smart device (phone or tablet). The smart device will be running either the DJI GO app or the DJI Pilot app. Most DJI drones will only operate with one of the two apps. If internet connection is enabled, the app may communicate with the internet, including to obtain map updates, synchronise data, etc.

The DJI GO app is associated with the consumer and professional grade drones; the DJI Pilot app is associated with the enterprise grade drones. As such, the DJI Pilot app has enhanced security features relative to the DJI GO app.

3.2 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 [7]. 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” [8]. 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 [9]. 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” [10]. In November 2018 the Australian Army completed the roll-out of 350 DJI Phantom 4 drones to every unit [9].

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 [11]. 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” [2].

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” [12]. 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 [13]. 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 ”[15].

3.3 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 [16]. 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 [17].

In response to the above revelations, additional revelations as to the key for DJI's SSL Certificate being publicly available on the public software repository 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 [18]. However, Subsequent analysis by Israeli firm Check Point Research [19] and French firm Synacktiv [1] indicates that significant vulnerabilities remain.

3.3.1 Check Point Research

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 [19]:

- "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 [19], published two months after the vulnerability had been patched [20].

3.3.2 Kivu Report

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 [21, 22], 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 [23]. 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 [22].

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" [23]. 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 [23]:

> 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 [22]:

> 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.

3.3.3 Synacktiv Analysis

In direct contrast to Kivu, in July 2020 the French IT security firm Synacktiv published analysis of three versions of the DJI GO 4 app: the first released December 2017, the second released October 2019, and the third released May 2020.

The most significant "feature" identified by Synacktiv is an auto-update mechanism providing DJI with the ability to force the installation of new software on the user's phone [1]. Synacktiv comments:

> This mechanism is very similar to command and control servers encountered with malwares. Given the wide permissions required by DJI GO 4 ..., the DJI or Weibo Chinese servers have almost full control over the user's phone.
>
> [Given this update mechanism], any security assessment made on this application, such as [that made by] Kivu, is strongly limited because potential malicious code can be pushed by DJI afterwards through this auto-update mechanism.

Synacktiv also found that[1]:

> [R]ecent versions of DJI Android GO 4 application collects personal data such as IMSI, IMEI, the serial number of the SIM card, etc. This data is not relevant or necessary for drone flights .... For example, IMSI is used by cellular network operators. These sensitive, unique, persistent data identifiers can be used by intelligence agencies or malicious people to later track individuals or eavesdrop communications.

Finally:

> The DJI GO 4 application on the Android platform does not close when the user closes the app with a swipe right. The app continues to run in the background and makes network requests.

The analysis by Synacktiv appears to confirm the concerns espoused by the US Government.

3.4 DJI Government Edition Firmware

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 [24].

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" [25]. 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 [24, 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 [26]. 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.

The vulnerability of both firmware and operating systems to new bugs as updates are introduced is illustrated by recent patches to fix bugs in the Android operating system used on many mobile phones. As an aside, the DJI Mavic (prior to the DJI Mavic 2) utilised the Android operating system. In early February 2020, Google patched a serious "remote code execution bug" in later versions of the Android operating system, which Google describes as enabling "a remote attacker using a specially crafted transmission to execute arbitrary code" [27, 28]. Thus, even if the GE software was secure, that security only lasts as long as the software is not updated, hence INL's comment that the GE could only be an interim measure.

3.5 US DOI Grounds DJI Drones

Notwithstanding the findings and recommendations above, 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" [29]. This action was formalised in an order dated 29 January 2020, with the scope expanded to include "UAS manufactured by designated foreign-owned companies or UAS with designated foreign-manufactured components" [30].[1]

At the time of these actions no detailed technical analysis had been released by the US Government to justify the grounding. As such it was unclear whether the grounding was the result of new security threats or whether it was a result of pressure from US politicians with the growing tension between the US and China. However, the subsequent analysis Synacktiv analysis, summarised in section 3.3.3 above, suggests that the grounding could be a result of valid concerns.

[1] Note that the use of the term "designated" in the Order differs from the use of the term "covered" in the National Defense Authorization Act for Fiscal Year 2020, which is expressly defined to refer to China.

4 DJI Responses

4.1 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” [31]. This mode subsequently went “live” on 2 October 2017 [32]. 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.

4.2 DJI Data Security Recommendations

On 23 May 2019, DJI responded to the DHS industry alerts[2] with the statement that “your data is not our business” [33]. 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 available on the DJI Pilot app.

[2] Refer section 2.2.

5 Deployment of DJI Drones in a Secure Organisational Environment in New Zealand

Drones are a computing device that form part of a broader network. The drone will be used to collect information, and in some way will interact with the organisation's computer networks. The first step before purchasing drones should be a risk assessment. Key questions to be considered in the risk assessment are what information is collected, and what harm would occur to the organisation if that information were to be intercepted by an unauthorised third party. Public sector organisations should carefully consider the likely security classification of information to be collected, both on its own and in aggregate.

This may also be a good time to conduct a Privacy Impact Assessment (PIA) [34], which considers the sensitivity of information in relation to information about an identifiable individual. The PIA and the risk assessment should then inform the purchase decision(s)and the controls placed around drone use.

5.1 Transmission from the Drone to the Remote Controller

An essential requirement for a drone is that it transmits information back to the remote controller. Without that transmission the pilot will not know what the drone can "see" and any situational awareness or surveillance that the drone might have provided is lost. From an information security perspective, however, a drone that is transmitting information is effectively the same as a mobile device. Referring back to figure 1 this raises concerns with potential vulnerabilities ① and ②.

DJI claims that all data transmitted via OcuSync 2.0 from the drone to the remote controller is encrypted with using AES-256 encryption, which in practice means that all of the DJI Enterprise drones have the data at ② potentially encrypted. AES-256 is an approved encryption algorithm in the NZISM [35, pp. 17.2.10, 17.2.12]. However, the GCSB warns that the use of an Electronic Code Book (ECB) implementation of the AES standard can introduce significant vulnerabilities and warns that for all security classifications "agencies using AES... should not use Electronic Code Book [m]ode" [35, p. 17.2.26.C.01].

Synacktiv [1] report that DJI log files are encrypted with AES 256 CBC rather than ECB, but they were readily able to derive the password and decrypt the files. Given the evidence provided by Synacktiv [1] it should be assumed that other DJI implementations of AES are similarly insecure until proven otherwise. Thus, even though DJI claims AES-256, weaknesses in password generation mean that it is likely that there are vulnerabilities at ②.

The NZISM requires that where information has a higher level security classification (i.e. is Confidential, Secret, or Top Secret), Government departments and agencies [35, p. 11.4.10.C.01]

> MUST ensure that:
>
> - the network has been certified and accredited for the purpose;
> - all classified traffic that passes over mobile devices is appropriately encrypted; and
> - users are aware of the area, surroundings, potential for overhearing and potential for oversight when using the device.

Absent further detailed investigation, it is not possible to conclude that the traffic is appropriately encrypted, which in turn means that an off-the-shelf DJI product is not appropriate for a higher level security environment. Furthermore, there is no reason to assume that DJI products are less secure than other Chinese made drones. This reinforces the need for public sector organisations to assess the likely security classification of information to be collected by a drone prior to making a purchase.

5.2 Transfer from Remote Controller to Cloud Server

Once it has been received by the remote controller, the information collected by the drone might then be transferred back to a cloud server. The cloud server may be a DJI server, an Amazon Web Server (AWS), or a private cloud server depending on the specifics of the implementation:

- Standard professional / consumer drones do not utilise the DJI Pilot app and may store data on a DJI server;
- Enterprise series drones may utilise the DJI Pilot app or DJI Pilot PE (Private Edition) and as a consequence may be able to turn off all data sharing (Local Data Mode);
- Enterprise series drones utilising the DJI Pilot app in conjunction with the DJI FlightHub Enterprise software (refer Section 5.4 below) may store data on AWS;
- Enterprise series drones utilising DJI Pilot PE (Private Edition) in conjunction with the DJI FlightHub Enterprise software may store data on a private server.

The NZISM requires that organisations intending to adopt cloud technologies must conduct a comprehensive risk assessment [35, p. 2.3.20]. For government agencies, approval from the GCSB is required before cloud computing services or infrastructure are utilised for any information that has a higher level security classification, and a public cloud system must not be used for such data [35, p. 22.1.20].

Drones known to use the the DJI Pilot app (and therefore also able to use the DJI Pilot PE) are the Mavic 2 Enterprise and Matrice 200 Series V2. The 'standard' app used by other DJI drones is the DJI GO app, which was the app investigated by Synacktiv [1]. The Phantom 4 RTK is an Enterprise series drone, but uses the DJI GS RTK app. Similarly, the Phantom 4 Multispectral is an Enterprise series drone, but uses the DJI GS PRO app. It is not known whether the GS apps are built on the GO app, the Pilot app, or something entirely different. The Mavic Mini uses the DJI FLY app, which appears to have similar functionality to the GO app.

If a drone utilises the DJI Pilot app (or DJI Pilot PE) then Local Data Mode can be activated so that data is only stored on the drone (refer Section 4.1 above). None of the other DJI apps enable this Local Data Mode. However, the DJI Pilot app is not open source, and nor is it certified by an independent party, so it is possible that the software contains a bug or latent vulnerability that is not yet publicly known. Such vulnerabilities could provide the opportunity for a data leak in the same manner as has been demonstrated for DJI GO 4 [1].

5.3 The Necessity of Connecting to the Internet

As indicated above in DJI's press release on Local Data Mode, new drones must be activated by logging into a DJI account with an email and password. As part of good asset control and IT security practices, it is appropriate that this is performed centrally with a single email address, probably by the IT department.

A drone will also be loaded with the default DJI GEO zones, which may prevent flight in some locations such as airports [36]. The DJI GEO zones are not related to airspace restrictions imposed by the Civil Aviation Rules, but are instead a proprietary safety zone developed by DJI. Some GEO zones will prevent flight, and some may trigger a warning. In some zones flight may only be possible if the zone is 'unlocked' by users using a "DJI verified account," and such unlocking may required online access from the remote controller.

5.4 DJI FlightHub Enterprise

DJI has developed the FlightHub Enterprise software to enable the centralised management and deployment of drone operations within a private network [37]. FlightHub may be deployed on either a US-based Amazon Web Server (AWS) for a limited plan with no more than 10 drones, or within a private cloud server on an ‘Enterprise’ or ‘Government’ plan that allows more than 10 drones. Each of these drones must be controlled via the DJI Pilot app (AWS server) or DJI Pilot PE (Private Edition) app when deployed on a private cloud server.

DJI claims that FlightHub can be used with “Matrice 200 Series V2, Matrice 200 Series, Matrice 600 Series, Inspire 2, Mavic Pro, Mavic 2 Enterprise, Mavic 2 Enterprise Dual, Phantom 4, Phantom 4 Advanced (excluding Phantom 4 Advanced+), and Phantom 4 Pro (excluding Phantom 4 Pro+)” [37, p.2]. However, it is unclear whether all of these drones can actually be used with the DJI Pilot app. For example, the user guide for the Matrice 600 Pro refers to the DJI GO app and has no reference to the DJI Pilot app [38].

As was discussed above in relation to the DJI Pilot app, the FlightHub Enterprise software is not open source, and it is not certified by any independent party. This means that any of that software or firmware could have a bug or latent vulnerability, or even have intentionally malicious code.

6 Conclusion

DJI UAS have a demonstrated history of cyber vulnerabilities, which is unsurprising for any software-based products developed for the consumer market. Similar vulnerabilities are likely to exist in drones manufactured by other manufacturers, including those based in China.

While these vulnerabilities appeared to have been addressed by DJI by way of firmware updates, recent research into the DJI GO app indicates that significant vulnerabilities continue to exist. Even when a secure version of firmware is provided, 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, which in turn means that only Enterprise series drones should be used in conjunction with the DJI Pilot app. 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

1. Synacktiv. *DJI Android GO 4 Application Security Analysis* tech. rep. (23rd July 2020). `https://www.synacktiv.com/en/publications/dji-android-go-4-application-security-analysis.html`.
2. Da Jiang Innovations. *DJI Statement On ICE Bulletin* press release. 18th Nov. 2017. `https://www.dji.com/newsroom/news/dji-statement-on-ice-bulletin`.
3. Da Jiang Innovations. *DJI Creates High-Security Solution For Government Drone Programs* press release. 24th June 2019. `https://www.dji.com/newsroom/news/dji-creates-high-security-solution-for-government-drone-programs`.
4. Department of Homeland Security. *Cybersecurity Risks Posed by Unmanned Aircraft Systems* Critical Infrastructure Security and Resilience Note (Office of Cyber, Infrastructure Analysis (OCIA), National Protection and Programs Directorate, 22nd May 2018). `https://info.publicintelligence.net/OCIA-UnmannedAircraftRisks.pdf`.
5. Kesteloo, H. Department of Defense bans the purchase of commercial-over-the-shelf UAS, including DJI drones effective immediately. *Drone DJ.* `https://dronedj.com/2018/06/07/department-of-defense-bans-the-purchase-of-commercial-over-the-shelf-uas-including-dji-drones/` (7th June 2018).
6. Shortell, D. DHS warns of 'strong concerns' that Chinese-made drones are stealing data. *CNN International Edition.* `https://edition.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html` (20th May 2019).
7. Department of the Navy. *Operation risks with regards to DJI family of products* Ser PMA-263/17-183. 24th May 2017. `http://www.documentcloud.org/documents/6579727-Navy-DJI-Assessment-2017.html`.
8. Department of the Army. *Discontinue Use of Dajiang Innovations (DJI) Corporation Unmanned Aircraft Systems* For Official Use Only. 2nd Aug. 2017. `https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment/`.
9. Australian Defence Force. *Australian Defence Force us of DJI drones and Hikvision and Dahua Surveillance Cameras* FOI 304/18/19 (29th Jan. 2019), 30–35. `http://www.defence.gov.au/FOI/Docs/Disclosures/304_1819_Documents.pdf`.
10. Levick, E. Army targets drone literacy with Phantom delivery. *Australian Defence Magazine.* `https://www.australiandefence.com.au/land/army-targets-drone-literacy-with-phantom-delivery#HpMFXlYVBfPXYExx.99` (23rd Aug. 2018).
11. Department of Homeland Security. *Da Jiang Innovations (DJI) Likely Providing U.S. Critical Infrastructure and Law Enforcement Data to Chinese Government* Intelligence Bulletin (Homeland Security Investigations,SAC Intelligence Program Los Angeles, 9th Aug. 2017). `https://info.publicintelligence.net/ICE-DJI-China.pdf`.
12. Bayer, K. NZDF has no plans to ground drones banned by US military allies over cyber-safety fears. *NZ Herald.* `https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12005158` (2nd Mar. 2018).
13. Babb, C. & Xie, H. US Military Still Buying Chinese-Made Drones Despite Spying Concerns. *Voice Of America.* `https://www.voanews.com/usa/us-military-still-buying-chinese-made-drones-despite-spying-concerns` (17th Sept. 2019).
14. National Defense Authorization Act for Fiscal Year 2020. S.1790 - 116th Congress. `https://www.congress.gov/bill/116th-congress/senate-bill/1790/text` (2019).

15. Nikkei staff. Japan Coast Guard to 'eliminate' Chinese drones. *Nikkei Asian Review.* https://asia.nikkei.com/Politics/International-relations/Japan-Coast-Guard-to-eliminate-Chinese-drones (9th Dec. 2019).

16. Da Jiang Innovations. *DJI To Offer 'Bug Bounty' Rewards For Reporting Software Issues* press release. 28th Aug. 2017. https://www.dji.com/newsroom/news/dji-to-offer-bug-bounty-rewards-for-reporting-software-issues.

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

18. Da Jiang Innovations. *Statement About DJI's Cyber Security and Privacy Practices* press release. 25th Nov. 2017. https://www.dji.com/newsroom/news/statement-about-dji-cyber-security-and-privacy-practices.

19. Vanunu, O., Barda, D. & Zaikin, R. *DJI Drone Vulnerability* 8th Nov. 2018. https://research.checkpoint.com/dji-drone-vulnerability/.

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

21. Da Jiang Innovations. *Independent Study Validates DJI Data Security Practices* press release. 23rd Apr. 2018. https://www.dji.com/newsroom/news/independent-study-validates-dji-data-security-practices.

22. Brush, D. A. *UAV Data Transmission & Storage* letter to DJI Research LLC. 14th Feb. 2018. https://www.dropbox.com/s/u221xdd3w0tkde6/Kivu%20summary%20of%20DJI%20report.pdf.

23. Cameron, D. DJI Releases Security Findings It Hopes Will Quash 'Chinese Spying' Fears. *Gizmodo.* https://www.gizmodo.com.au/2018/04/dji-releases-security-findings-it-hopes-will-quash-chinese-spying-fears/ (24th Apr. 2018).

24. Bathrick, M. L. & Koeckeritz, B. *DJI Unmanned Aircraft System (UAS) Mission Functionality and Data Management Assurance Assessment* tech. rep. (U.S. Department of the Interior, Office of Aviation Services, 2nd July 2019). 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.

25. Detweiler, C. & Beachly, E. *Evaluation of DJI's specialized systems for the Department of the Interior* tech. rep. Appendix D to [24] (Drone Amplified, INC, 27th Nov. 2018).

26. Idaho National Laboratory. *Aviation Cyber Initiative Unmanned Aircraft System Information Security Risks Limited Scope Test & Evaluation* Unclassified // For Official Use Only (INL-LTD-19-55545 Revision 2. Prepared for the U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, Contract DE-AC07-05ID14517, Oct. 2019). https://www.documentcloud.org/documents/6579764-INL-Drone-Report-Oct-2019.html.

27. Bradbury, D. Critical Android flaws patched in February bulletin. *Naked Security.* https://nakedsecurity.sophos.com/2020/02/05/critical-android-flaws-patched-in-february-bulletin/ (5th Feb. 2020).

28. Android Open Source Project. Android Security Bulletin—February 2020. https://source.android.com/security/bulletin/2020-02-01 (5th Feb. 2020).

29. Newcomer, E. Interior Department Will Stop Using Non-Essential Chinese Drones. *Bloomberg.* https://www.bloomberg.com/news/articles/2019-10-30/interior-department-will-stop-using-non-essential-chinese-drones (31st Oct. 2019).

30. Secretary of the Interior. Temporary Cessation ofNon-Emergency Unmanned Aircraft Systems Fleet Operations. Order No. 3379, US Department of the Interior. `https://www.doi.gov/sites/doi.gov/files/elips/documents/signed-so-3379-uas-1.29.2020-508.pdf` (29th Jan. 2020).

31. Da Jiang Innovations. *DJI Develops Option For Pilots To Fly Without Internet Data Transfer* press release. 14th Aug. 2017. `https://www.dji.com/newsroom/news/dji-develops-option-for-pilots-to-fly-without-internet-data-transfer`.

32. Da Jiang Innovations. *DJI Launches Privacy Mode For Drone Operators To Fly Without Internet Data Transfer* press release. 2nd Oct. 2017. `https://www.dji.com/newsroom/news/dji-launches-privacy-mode-for-drone-operators-to-fly-without-internet-data-transfer`.

33. Da Jiang Innovations. *Your Data Is Not Our Business* 23rd May 2019. `https://content.dji.com/your-data-is-not-our-business/`.

34. Privacy Commissioner. Privacy Impact Assessment Toolkit. Office of the Privacy Commissioner. `https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/` (7th July 2015).

35. GCSB. *New Zealand Information Security Manual* tech. rep. V 3.3 (Government Communications Security Bureau, Feb. 2020). `https://www.nzism.gcsb.govt.nz/`.

36. Da Jiang Innovations. *GEO Zone Map* `https://www.dji.com/nz/flysafe/geo-map`.

37. Da Jiang Innovations. *DJI FlightHub Enterprise User Guide v 1.0* Mar. 2019. `http://dl.djicdn.com/downloads/FlightHub/20190308/FlightHub_Enterprise_User_Guide_v1.0_EN.pdf`.

38. Da Jiang Innovations. *Matrice 600 Pro User Manual* tech. rep. V 1.0 (Apr. 2018). `https://dl.djicdn.com/downloads/m600%20pro/20180417/Matrice_600_Pro_User_Manual_v1.0_EN_.pdf`.