National Protective Security Authority

GUIDANCE DOCUMENT

Uncrewed Aerial Systems (UAS) for Protective Security

Managing UAS security risks

Publication date: September 2023

Contents

Overview and aim of guidance

This guidance is intended to be read by security professionals across both public and private organisations, sensitive sites and crowded places who are preparing to use commercially available Uncrewed Aerial Systems (UAS) for protective security operations.

It forms part of a suite of guidance documents on UAS for protective security that provides the reader with end-to-end advice from the early stages of creating an operational requirement, right through to preparing for UAS operations and managing the associated security risks.

The use of UAS in protective security has many benefits, but like all technology solutions, it is important to ensure that the security risks associated with new technologies are properly understood and mitigated.

This document focuses specifically on **understanding the security risks of using UAS and how these can be managed**. The guidance will help organisations understand the breadth of risks that need to be considered and develop operating procedures to mitigate the risks associated so that the use of UAS does not in itself become a vulnerability, exploitable by malicious actors to cause physical or cyber enabled damage.

Pre-flight risks

Pre-flight risks can be forecasted and planned against prior to purchase or before each flight. Pre-flight risks focus on UAS acquisition and place of manufacture, UAS flight planning software, UAS vendor data storage, and UAS vendor user agreements.

Determining the country of origin

When considering using UAS in or around sensitive sites or in any security operation, organisations should familiarise themselves with the increasing capability and connectivity of UAS systems being deployed. Some of the most sophisticated, intuitive, and low-cost commercial off the shelf (COTS) UAS and associated software on the market today are manufactured in countries with coercive data sharing practices that could lead to the loss of sensitive data.

As data-loss security risks can be hard to detect and mitigate, the first line of defence for organisations wishing to use UAS may be restrict UAS and associated component procurement from countries which pose a risk to security and, in particular, through data theft. For this reason, organisations should ensure that the relevant procurement departments are consulted at the earliest stages of developing UAS operations.

Where possible, procurement should seek to develop stringent security criteria to identify and prevent high risk vendors from progressing through the procurement process. This should require transparency clauses to mandate firms responding to any tender process to share country of origin information.

As part of any evaluation process, special attention should be paid to the use of UAS made by firms who by virtue of their country of origin could be obliged to support, cooperate with, or collaborate on national intelligence work which could be harmful to UK interests.

Organisations should thoroughly review product user agreements related to data, review open-source information available on previous state-sponsored cyber incidents originating from the country of manufacture, conduct open-source research on the manufacturer’s cyber security record, and any indication of a decline in trust between the country and the UK prior to making any purchase decisions.

UAS manufacturers with links or obligations to countries associated with cyber-attacks, data leaks, and industrial espionage may use re-branding or changes to the locations of their supply

chain in an attempt to conceal their country of origin and to work around any procurement regulations in place.

Therefore, organisations should look beyond the selling entity and require information during any tendering process on the place of origin of key components within the software, hardware, and communication infrastructure of the UAS system.

This includes the UAS airframe itself as well as key equipment and sensors such as flight controllers, radios, cameras, the ground control system, operating software, and the data storage location.

It is through hardware, software, and communication infrastructure that “backdoors” are commonly introduced. These backdoors, either deliberate or accidental, could give rise to unauthorised or malicious users being able to circumvent normal security measures and gain high level user access to computer systems, networks, or software.

Primary cyber risks associated with UAS

- Hardware
- Software
- Communications

If components are identified that could create a risk, it is advised the system is not connected to the internet without taking additional cyber security precautions with the organisation’s relevant Information/ Cyber Security teams.

The table below describes some of the more critical components of a UAS system which require an understanding of place of manufacture. In cases where organisations cannot satisfactorily determine the place of manufacture or believe that attempts have been made to obfuscate this, strong consideration should be given to excluding those firms from progressing in any tendering process.

UAS Critical Components Which Require an Understanding of Place of Manufacture
1. **Flight controller:** The combination of embedded software on computing hardware that issues commands to the UAS.
2. **Radio:** The device that enables communication by packaging, transmitting, and/or receiving signals into or from electromagnetic waves in the radio frequency (RF) spectrum.
3. **Data transmission device:** Electronic hardware that actively transfers electronic information from one system to another.
4. **Camera**: The device that captures and can record visual images in the form of photographs, film, or video signals.
5. **Gimbal:** The mechanism which rotates about one or more axes to stabilize and properly orient cameras or other sensors.
6. **Ground control system:** The hardware that enables a human operator to transmit commands and data to influence the actions of the UAS remotely and to monitor the status and health of the UAS.
7. **Operating software:** The program(s) that direct the computer's basic functions.

8. **Network connectivity:** The hardware and software required for communication between computers over the internet or other distributed and separately administered systems, for example, using routers, switches, and gateways.

9. **Data storage:** The collective methods and technologies that capture and retain digital information on storage media.

Installing UAS controller apps on mobile phones, tablets, and laptops

Many UAS are now able to be controlled or monitored either partially or in part by software applications downloaded on to existing mobile phones. The most common example is the use of proprietary apps to control the UAS and stream full motion video from the UAS camera to a tablet or phone.

Some of the apps on the market today by default will continue to run in the background on the phone or tablet to which it is installed even after the user is finished and closes the application. Terms and conditions the user signs up to when installing the app may enable the app to collect sensitive data from the user's tablet or phone without knowledge. This may include access to contacts, images, microphone, camera, current and previous location, storage, change network connectivity, browser history and more.

Figure 1 - Operating a UAS using a proprietary app to stream full motion video to a mobile phone.

It is **strongly recommended that separate phones, tablets, and laptops devices are purchased, and ring fenced solely for UAS operations**. To avoid accidental or deliberate data leakage, these devices should never be registered to individuals and never used for any other personal or business purpose. Where registered to a business, organisations should consider whether it would be appropriate to use an alias name. Legal advice should be sought in cases where that is considered to ensure that this does not inadvertently impact any other feature such as the product warranty.

Phones, tablets, and laptops used as dedicated UAS controllers or monitors could be used as a method by which to compromise an organisations UAS operations. Operators may be tempted to use the controller device to contact friends or family, download non-essential or third-party apps, or access personal email or social media on the device. Multipurpose use could make devices vulnerable to malware, spam or phishing which could lead to unauthorised access. While computers commonly have software such as firewalls, antivirus, and/or anti-malware, mobile devices often just employ the operating system and the security of their apps for protection. If the **controller device and software is not properly protected, malware could be introduced causing significant risk to the UAS and associated IT networks.**

Dedicated phones, tablets and laptops used for UAS operations should wherever possible be disconnected from the internet. If this is not possible, **consideration should be given to connecting via a secure Wi-Fi or an encrypted virtual private network (VPN).**

Even where separate devices are used, prior to commencing any UAS operations or using proprietary apps for the first time, organisations should familiarise themselves with the application settings and **ensure that any data sharing settings that are not essential for UAS operations are disabled**. This will help prevent any unwanted capture and storage of information.

It is important to note, however, that even with careful planning not all risks can be fully mitigated. Some data sharing settings will not be configurable and may lead to unwanted information being made available to the UAS manufacturer and onwards to third parties. An example of this is flight information. Details such as UAS flight dates and times, routing, flight controller location may all be collected even when application settings are locked down as far as practically possible. This may enable the manufacturer and any third party with whom that data is shared to build pattern of life information around UAS operations.

Organisations should consider the operational security risks associated with this type of information being made available and seek to lock down phone settings as far as possible to mitigate this. **Mobiles, tablets, and laptops used for UAS operations should be regularly inspected and digitally cleaned as part of a standard operating procedure.**

Data/cloud storage and the use of web-based forums

Many UAS use cloud-based services to store data ranging from flight analysis information through to copies of full motion video.

Organisations enabling cloud-based data storage should check with their cyber security team and ensure that any use of the cloud is compatible with cyber security procedures in place. This will likely include restrictions on the location of cloud data centres.

Previous reported security breaches involving UAS cloud-based storage have involved adversaries gaining access to vendor cloud-based platforms by gleaning information on users from popular UAS forums where users post questions, comments, and receive feedback from vendors.

In some reported instances penetration testers were able to gain complete control over users' cloud-based data including flight records, photos, videos, telemetry, and flight logs. In more serious cases, user credentials that were harvested from web forums have been known to include real-time map views of UAS in flight with real-time camera views accessed.

Organisations should make sure that strict policies are in place to limit participation in open UAS forums, even those associated directly with the equipment vendor.

Pre-Flight Best Practices to Mitigate UAS Cyber Risks:

- Understand the manufacturer's privacy policy before purchasing, including how and where your data will be stored and shared.
- Update the UAS firmware regularly.
- Use a strong password for your base station app.
- Keep tablet/phone controller free from other downloads such as gaming apps.
- Subscribe to an antivirus program.
- Connect to secure Wi-Fi, employ a Virtual Private Network (VPN), or enabling airplane mode whenever possible.
- Turn on Local Data Mode (LDM) to block your data from being transmitted or shared.
- Set a limit of one for the number of devices that can connect to your base station.

Operating system updates

Software updates are essential tools used as standard industry practice to rectify bugs or security vulnerabilities identified after a software versions release. Backdoors can be accidental or deliberate. Whilst the best protection against deliberate backdoors is via a strong procurement process to identify and deselect high risk vendors, accidental backdoors are best mitigated through a strong cyber security programme that includes regular software updates as soon as they become available.

Previous reported backdoor incidents include malware script taking control of a Commercial Off The Shelf (COTS) UAS through an accidental backdoor vulnerability on its operating system, allowing the adversary to remotely fly the UAS. This example showed that all UAS using that operating system were at risk to backdoor vulnerabilities.

Organisations managing UAS should maintain awareness on their specific UAS operating system, ensuring updates are available and installed to help stay one step ahead of malicious actors that may take advantage of outdated firmware vulnerabilities.

Organisations should ensure that a UAS configuration management and reporting plan is implemented which records the current versions of UAS firmware and app software for the any UAS fleet as well as their physical location and storage requirements. As change updates are rolled out by the UAS vendor, **organisations should download and record all updates to firmware, apps, and software**.

Vendor terms and conditions

Before procuring any UAS, organisations should ensure the legal department carefully reviews the UAS user agreements to identify areas that may fall out of line with the organisation's cyber and data security policies. Some UAS on the market today contain terms that in some instances allow others to potentially share, view, or edit an organisations data.

Any review should take into consideration how those vendor terms interact with any national laws associated with the vendors country of origin. Some countries, for example, require companies to provide information they obtain, or information stored on their networks, to local authorities if requested. Laws such as this demonstrate that even if the vendor has in place strong security structures, sensitive data can still be requisitioned by the state.

Secure physical and cyber storage

UAS are the same as any other computer system, complete with component parts, operating systems, software, Wi-Fi connections, and hardware. The same cyber considerations, such as **strong password policies** that apply to more traditional networks and systems should be equally applied to UAS.

Just like other computer systems, **physical security controls should be in place to prevent unauthorised access.** UAS and UAS controllers should be secured safely in either a locked cabinet or drawer when not in use and physical access should be restricted. The use of USB sticks and third-party software should be prohibited or if essential, tightly controlled in line with existing cyber security regulations.

Processes should be in place to ensure that UAS camera and sensors including microphones are turned off before UAS are taken into any sensitive buildings for storage to avoid accidental capture of security sensitive information.

As UAS becomes integrated into an organisation's infrastructure, it remains a possibility that they **may be used to gain access to the organisation's infrastructure network**. A hacked UAS can potentially build a backdoor into an organisation's wireless network, causing network interference and resulting in data theft and operational disruption.

As organisations begin integrating UAS into operations, consideration should be given as to how UAS are managed. Ensuring UAS components are secure, maintaining a clean ground control station that is not infected with malware, performing frequent firmware updates, and using a virtual private network in some instances can all reduce the likelihood of a UAS from being hacked or interfered with.

A security control room should be the central point where all aspects of security activity using a UAS are planned and supervised. UAS operations should be integrated into existing security control rooms where possible.

Security control rooms allow staff to manage security operations more efficiently by providing a means to communicate with security personnel, deliver support, and communicate with outside public organisations, such as local law enforcement. To support UAS operations, a security control room might require updated computing capabilities for mapping, large hard-drive storage capacity to store and view UAS streamed video and other security sensitive information such as maps, and patrol plans related to UAS operations. Organisations should establish organisational guidance on information security to safeguard against malign service disruptions, data loss, unauthorised access, network abuse, and identity fraud.

In-flight risks

UAS employ a variety of communication links to maintain flight control, video monitoring, navigation, and geo-positioning. These communication links consist of radio frequency, GNSS, Bluetooth and Wi-Fi and often work in combination to maintain flight control, provide geo-spatial updates, and improve the user experience.

UAS hacking or remote interference

COTS UAS have in the past been subject to interference attacks exploiting known security vulnerabilities. Some of these have been capable of hacking the UAS protocol used to maintain a communication link between the radio controller and UAS, or transmit fake GNSS signals to the UAS so that it manoeuvres off course or crashes. Others have been designed simply to intercept the Full Motion Video (FMV) feed.

UAS can be remotely accessed mid-flight by malicious actors using a variety of tools, some of which are available free online or for purchase. Organisations using UAS should be alert to these risks and seek to mitigate them wherever possible.

In most cases, the signs that a UAS has been hacked or remotely interfered with (i.e. jamming) are the same, irrespective of the method used. UAS operators may notice the UAS not responding to flight controls. Video feed may also be affected. Both the feed and UAS control may be continually or intermittently disrupted during the jamming process.

In most cases, if transmission is disrupted, the UAS manufacturer will have developed a ‘fail safe’ setting. For example, if control signal is lost and Return To Home (RTH) functions are enabled prior to flight, most UAS will RTH if they still have GNSS. UAS operators may notice the UAS remains stationary for a period of up to 10 seconds before the functionality takes effect.

Organisations should ensure that UAS operators are aware of interference risks and the signs to look out for, with protocols in place to manage a loss of control. For example, having RTH enabled prior to flight. UAS operators might also choose to assign the RTH to be another designated safe recovery location, which isn’t the same as the take-off point.

In the event of suspected interference, UAS operators should seek to trigger the RTH function manually, if possible, rather than waiting for any automatic function to take effect. It is important to ensure that RTH details are kept regularly updated with the correct identified home location saved.

UAS operators should also ensure that they are kept abreast of any intelligence that may indicate a hacking or interference attempt that may take place prior to flight. If intelligence is known that such a threat vector exists, UAS operations should be amended to limit the risks or suspended if the risk is too high.

Where hacking or interference was suspected, post flight scans for malware should be made to rule out any computer virus driven attack.

Global Navigation Satellite System jamming and interference

In addition to Wi-Fi hacking, a UAS Global Navigation Satellite System (GNSS) can potentially be vulnerable to jamming using COTS GNSS jammers. GNSS jamming units can be purchased online and are occasionally available on mainstream marketplaces for a short period of time before being taken down. A GNSS jammer could contribute to an operator losing control of the UAS during flight or disruption to an autonomous waypoint flight due to signal dropout.

Reduced stability may cause the UAS to fall out of the air, requiring the operator to manually intervene to regain stable flight. Additionally, without GNSS signal the UAS cannot initiate the return to home (RTH) function or fly using waypoints.

In more sophisticated cases, loss of control due to jamming could enable UAS to be flown to a different location when used in conjunction with a technique called spoofing.

Methods to mitigate UAS interference or hacking

- Ensure Return to Home is updated.
- Establish strong GNSS signal before take off.
- Update UAS firmware regularly.
- Connect to secure wi-fi, your cell phone hotspot, or VPN.
- Disable 'discovery features,' and never connect to a source you are unfamiliar with.

The best protection against GNSS jamming and interference is to ensure that robust pre-flight checks are in place that include checking that UAS firmware is up to date, and a strong GNSS signal is present before take-off.

GNSS based attacks tend to be operated from nearby. Typically, only military grade equipment can jam from far distances with more common hand-held jammers requiring the user to see the UAS and orient the jammer at the UAS.

This means the UAS operator could potentially capture the jammer (or person operating the jammer) on video or even see the person / jammer nearby if flying within Visual Line Of Sight (VLOS).

Security patrols, UAS operators and those involved in VLOS operations should be made aware of these attack vectors and briefed to look out for suspicious behaviour.

Radio Frequency jamming, interference, and eavesdropping

Radio Frequency (RF) uplink/downlink communication between the ground control station and the UAS can be vulnerable to being jammed causing loss of command and control (C2) or theft of the UAS.

UAS using Wi-Fi, if uncontrolled, may lead to the UAS flight being hacked or the data stream being intercepted. The best defence against this is to procure high quality COTS UAS that do not solely rely on open Wi-Fi for flight control. Where this is not possible, the UAS should connect to secure Wi-Fi with strong passwords. This is particularly important when streaming FMV of sensitive sites.

Some COTS UAS employ frequency hopping techniques to mitigate RF jamming and disruption. Whilst a determined malicious actor could overcome this, it is recommended that frequency hopping capabilities are enabled if suitable.

Technology now also exists to hack an RF uplink and downlink communication of the UAS for it to be copied and analysed for later decryption. This is called eavesdropping. Once the signal is understood, a determined malicious actor can potentially replay the RF frequency using a transmitter to take control, disrupt the flight, or eavesdrop on UAS data transmission.

Whilst this type of sophisticated attack is rare, organisations should continue to practice good cyber hygiene by ensuring the RTH location is up to date and UAS software and firmware updates are continually installed.

RF based attacks tend to be operated from nearby. Typically, only military grade equipment can jam from far distances, with more common hand-held jammers requiring the user to see the UAS and orientate the jammer at the UAS.

If operating near congested areas with tall buildings or large crowds, organisations should carefully consider the risks of unintentional RF interference. “Drone fly-aways” are caused when UAS transmissions are accidentally disrupted caused by line-of-sight interference (i.e. tall buildings), or “RF congested” areas drowning out the signal. UAS operators should have protocols in place to enable them to call off flights in congested areas or ensure that they have their risk mitigations with RTH tactics, techniques and procedures established.

Protecting FMV transmissions during flight

Most use cases for UAS for protective security requires the ability to stream data, often full motion video (FMV) back to control rooms or operators.

Typically, this does not require extra or third-party software to set up. Most reputable UAS come with FMV software as part of a UAS package that can connect back to existing monitoring stations.

When employing UAS to provide support for security operations, it is possible for the FMV feed to be transmitted both to the controller and to a television screen inside of the control room. This FMV feed can provide real-time data to staff to better support decision making and support requests.

As well as protecting that data once in an organisations possession it is important that data is adequately encrypted during transit from the UAS to the controller and to the control room to protect operational security. This is particularly important where UAS camera systems may, as part of their routine activity, capture imagery that may be useful to hostile actors if uncontrolled.

The use of UAS without encrypted FMV feeds will mean this information becomes easier to read remotely. Encryption during data transit can be an additional, rather than a routine feature, and is often not the default setting.

Organisations should be aware of this fact and procure and activate services that enable encryption of data in transit. Wherever possible transmissions are secured via the use of secure Wi-Fi.

Hostile reconnaissance

Wireless and radio communication between UAS operators could be targeted for jamming and interference. Furthermore, the pattern of communications, total numbers of personnel, patrol schedules, and call signs can be understood and collected for planning purposes for future attack planning purposes.

In this context, UAS should be considered like any other security technologies. Security personnel and others site users should be made aware of the risks to those technologies from

hostile reconnaissance. Appropriate response procedures should be in place where hostile reconnaissance is suspected.

Security patrols, UAS operators, those involved in VLOS operations and other site users should be briefed to look for suspicious people at vantage points (i.e. on hill tops), or vehicles parked near likely launch sites. Procedures should be put in place for anyone paying particular attention to UAS operations, seen loitering around UAS operations, or in the possession of unusual electronic equipment. Suspicious activity should be reported immediately to the UAS operations team.

Post-flight risks

Post-flight security risks generally occur from poor data handling procedures or complacency related to UAS data storage. Multi-use smart devices used to control UAS, wireless transfer/download of data to organisations computers for analysis, and removable storage devices all contribute to the post-flight risks associated with UAS.

Data captured/ stored from stills and videos

UAS are very capable data collection tools. However, the advantages that a UAS brings can also open an organisation to risk if the UAS is exploited and the data is stolen or leaked to malicious actors. To maintain data security after each flight, UAS operators must control any removable storage devices for the UAS, and erase collected data from the UAS after transfer to secure data storage.

Organisations should be aware of where and how UAS data is stored, especially when using an overseas manufactured UAS with cloud storage facilities. Data captured from UAS will include sensitive information, which increases the risk of uncontrolled distribution of this information to third parties. For example, in situations where cloud servers are in an overseas country, there may be an increased risk of uncontrolled distribution due to security laws of the host nation.

It is important to note that data stored by UAS vendors may be far more than that used by the purchasing organisation. Flight data logs, log-in details and telemetry are just some examples of administrative data captured by many COTS vendors.

For further information, please refer to *NCSC Cloud Security Guidance*.

The use of Secure Digital (SD) cards

Many COTS UAS have an SD card slot to store data taken from the EO/IR sensor during flight. SD cards installed on the UAS are the size of postage stamps or smaller and can store several hours of full motion video data and a significant number of high-resolution photos, making them critical for UAS operations, physical security, equipment inspections, and staff planning.

UAS operator installing the micro-SD cards to store high resolution photos and video taken during flight.

SD cards can be a vector for malware, able to transfer malicious code from the SD card to the UAS and onward to an organisation network, making an organisation or its equipment vulnerable to cyber-attack.

USB removable storage devices have become widely recognised as a common method to spread malware and are often highlighted as risk areas within organisational anti-malware and data loss prevention policies. SD cards may traditionally be overlooked and not specifically mentioned in security policies.

Organisations seeking to build UAS operations should familiarise themselves with the vulnerabilities associated with UAS SD cards as a possible carrier of malware.

Organisations can lower the risk of their UAS and network being compromised by conducting the following safe removable storage practices:

- Do not share SD cards or swap cards used for other devices.
- Ensure that the UAS has a dedicated SD card, not used for other purposes or on personal devices.
- Use a physical connection to the device to upload pictures and video and do not use UAS wireless transfer capability.
- After each use, erase any personal data from the UAS and any removable storage devices.
- Ensure organisational network antivirus programs scan endpoint devices such as SD card readers or in this case the UAS where it is plugged into a computer to transfer data.
- Use caution when purchasing SD cards. Fake SD cards claiming to be manufactured by legitimate manufacturers have infiltrated the market. Make sure they are purchased from a trusted vendor.
- For further information, refer to the NCSC website on how to '*use peripherals securely*' and how to complete '*secure sanitisation of storage media'*.

Managing accidental data capture

Data gathered by UAS is likely to be security sensitive. There are currently a few methods to modify imagery to remove security sensitive information prior to being shared.

Geo-clipping or blurring an image or video to cut out or modify security sensitive information is complex. A geo-clipped image or video may mask an image to show only those consented geographic locations owned or controlled by a user and may ensure privacy of security sensitive sites.

Organisations should ensure that all UAS FMV data is treated as potentially security sensitive information and protected in the same way in which other sensitive information like CCTV is controlled. By treating all footage as security sensitive, the need to geo-clip or blur footage will be limited to more specific extra sensitive circumstances. An example of where geo-clipping or blurring may be appropriate is in cases where UAS operations overfly particularly sensitive areas enroute to another task. In those instances, it may be appropriate to redact the sensitive overflight portion. Another example is where personal data is captured as part of any UAS operation, such as vehicle registration plates.

Organisations should ensure that a data retention and protection policy in place and that UAS operations are compliant with and specifically catered for in any policies.

Other Relevant NPSA products

The NPSA website – www.npsa.gov.uk - provides more information on using UAS for protective security.

This document is part of a series of guidance on using UAS for protective security, including:

- UAS for protective security: Developing your operational requirement
- UAS for protective security: Preparing for operations

For cyber security advice, refer to the National Cyber Security Centre (NCSC) website.

Handling of this Document
Information provided in this report has been given a security classification. You must ensure that you store, handle and transmit the report in the manner appropriate to its security classification.

This document is intended for use by the direct recipient only and **should not be reproduced or passed to any third party in any form without prior written agreement from the National Protective Security Authority (NPSA).**

Freedom of Information Act (FOIA)
This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Disclaimer
This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.

Annex A: UAS threat vectors, potential risks and key mitigation activity

UAS COMPONENT	THREAT VECTOR	POTENTIAL RISK OUTCOME	MITIGATION
Hardware	UAS SD Memory Card	Malware introduced if used for multipurpose. Data could be stolen if SD card is misplaced.	Isolated SD card for UAS, remove data after each flight, maintain antivirus software that scans endpoint devices
	Supply-chain risk	Hostile State Activity or malicious tampering.	Procure from trusted vendor
	Multi-use of UAS controller	Malware introduced through 3rd party app download or controller multipurpose use	Restrict use of controller device to UAS only and limit apps downloaded to device
	Physical tampering	Stolen data, tampering	Store in locked drawer or cupboard with access controls in place
Software	Malware	Data leaks, eavesdropping, flight disruption, or UAS crash/theft, and unauthorised access	Connect only to secure Wi-Fi, do not download 3rd party apps, employ VPN
	Backdoors	Data leaks, eavesdropping, flight disruption, or UAS crash/theft, and unauthorised access	Maintain awareness of flight app security patches and regularly update firmware
	User Agreements/Terms of use	Employees may inadvertently agree to data sharing due to UAS user agreement	Integrate legal staff to review UAS terms of use before UAS procurement.
Communication link	GNSS Jamming or Spoofing	UAS loss of control due to jamming. UAS could be flown to undisclosed location and stolen due to spoofing	Change UAS flight patterns routinely to avoid setting patterns and be aware of personnel in vicinity of flight that could operate jammers
	RF jamming	UAS video may be observed/eavesdropped or C2 signal disrupted causing loss of control/ crash	Procure UAS w/encrypted communication links and update Return to Home location.
	Wi-Fi disruption	UAS flight can be hacked, or data stream intercepted	Procure quality COTS UAS that do not rely on open wi-fi for flight control. Connect to secure Wi-Fi with strong passwords if streaming video to outstation.