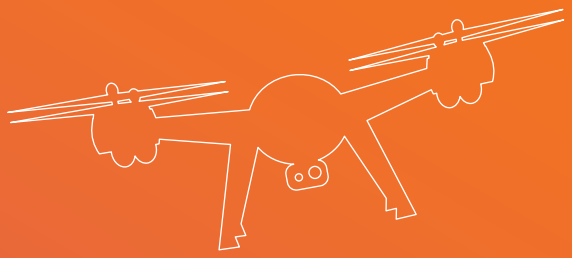
FLIGHT CRITICAL:

DRONES, CYBER SECURITY AND CRITICAL INFRASTRUCTURE



omni

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

THIS PROJECT WAS A COLLABORATION BETWEEN THE CSCRC AND OMNI

CYBER SECURITY COOPERATIVE RESEARCH CENTRE

omni

WITH THE SUPPORT OF

Australian Government
Department of Industry, Science and Resources

Cooperative Research Centres Program

CONTENTS

WHAT'S THE PROBLEM? 4

WHAT'S THE SOLUTION? 4

INTRODUCTION 5

WHAT ARE UAVS? 6

CRITICAL INFRASTRUCTURE SECTORS 8

HOW ARE UAVS USED ACROSS AUSTRALIAN CRITICAL INFRASTRUCTURE? 9

WHERE ARE UAVS MANUFACTURED? 10

WHAT CYBER THREATS ARE RELATED TO UAVS? 12

WHAT DOMESTIC REGULATIONS AND STANDARDS EXIST FOR UAVS IN AUSTRALIA? 14

WHAT CYBER-RELATED REGULATIONS AND STANDARDS EXIST FOR UAVS GLOBALLY? 16

CONCLUSION AND RECOMMENDATIONS 19

WHAT'S THE PROBLEM?

Despite their rapid proliferation and increasing use in critical infrastructure applications, there are no regulations or standards related to the cyber security of unmanned aerial vehicles (UAVs) in Australia.

WHAT'S THE SOLUTION?

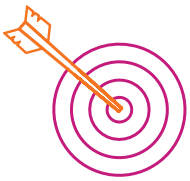
As the use of UAVs – which are often internet connected devices - becomes ubiquitous across the economy, especially in relation to their use for critical infrastructure monitoring and operations, it is vital cyber security guidance or standards are considered and implemented as a matter of priority.

INTRODUCTION

Australia's geography is vast, presenting unique challenges in relation to the monitoring and oversight of national critical infrastructure assets, which are dotted coast to coast across this wide brown land. Therefore, in an Australian context, the rise of sophisticated drone unmanned aerial vehicle (UAV) technology has the potential of being a game changer.

The use of UAVs has altered the way critical infrastructure is monitored, maintained and secured. UAVs have lowered costs, increased safety for workers, offer improved accessibility and save time. However, as it stands, there are no cyber security regulations or standards relating to UAVs in Australia which, as internet connected devices and/or devices that required internet connection for software updates and data uploads, are vulnerable to cyber exploitation. This is an issue that has been tackled firmly by the US Government's Cybersecurity and Infrastructure Security Agency (CISA), which has released several key guidances, the most recent in January 2024, specifically related to UAV cyber security and critical infrastructure applications.

With significant reforms to *Australia's Security of Critical Infrastructure Act 2018* (SOCI Act) now in force and amendments in train, and the number of systems of national significance (SoNS) continuing to grow, there is clear impetus to address the cyber security risks associated with the use of UAVs across domestic critical infrastructure assets. Furthermore, there is a need to investigate how UAVs and their cyber security integrity could be improved in Australia via regulation or guidance, especially in relation to their critical infrastructure applications. Therefore, this paper sets out to:



Define what UAVs are and how they are used to monitor Australia's critical infrastructure

Investigate where UAVs are manufactured and the potential cyber security risks this could pose

Explore potential cyber threat vectors that could impact the security and operations of UAVs

Explore the current domestic regulatory environment and consider international best practice

Present key recommendations to help improve the cyber security of UAVs used to monitor critical infrastructure assets

WHAT ARE UAVS?

UAVs, also known as drones, are aircraft that operate without a human pilot onboard, vary in size and weight and, due to their cost effectiveness and efficiency, are being deployed across industry for a myriad of purposes. They can be controlled by a human or operate autonomously, using pre-programming and automation (known as an autonomous UAV or AUAV).[1]

The global proliferation of UAVs has been rapid and significant. It is estimated the global UAV market size will hit US$67.64 billion by 2029,[2] with the number of UAVs produced set to grow from 2 million units in 2021 to 6.5 million in 2030.[3]

There are two main categories of UAVs - fixed wing and rotary wing.

Fixed wing UAVs look similar to regular aircrafts and are able to fly faster and longer. This makes them more energy efficient and ideal for mapping and monitoring large areas.[4]

Rotary wing UAVs, which have iterations including helicopters, quadcopters and hexacopters, have multiple rotors and are more mechanically complex.[5] They are easier to operate than fixed-wing UAVs and are more manoeuvrable, able to hover and fly closer to structures and buildings.[6] However, they have limited endurance and speed, requiring more energy to remain in the air.

As UAV technology continues to evolve, they are becoming increasingly sophisticated, fitted with state-of-the-art sensors, cameras and image processing software to provide more efficient and accurate data. Much larger UAVs with the ability to carry significant payloads are also being developed and deployed. As internet of things (IoT) devices and/or devices that required internet connection for software updates and data uploads, however, this also makes them vulnerable to cyber exploitation. Data that is collected and stored needs to be downloaded, UAV software needs to be updated, and UAVs are often operated via other IoT devices, for example, mobile phones.[7]

1. What is an Unmanned Aerial Vehicle (UAV)? - Definition from Techopedia
2. Drones Market Share, Report, Forecast & Analysis (mordorintelligence.com)
3. Emerging and Cross-cutting Aviation Issues — Increased use of unmanned aircraft systems (UAS) (icao.int)
4. Economic Benefit Analysis of Drones in Australia – Deloitte report (infrastructure.gov.au)
5. Ibid 4
6. Drone Types: Multi-Rotor, Fixed-Wing, Single Rotor, Hybrid VTOL (auav.com.au)
7. The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles | IEEE Journals & Magazine | IEEE Xplore

The SOCI Act

Over the past several years Australia's critical infrastructure regime has undergone significant reform. The number of captured sectors has been expanded from three to 11 and enhanced security obligations have been enacted for the nation's most critical assets.

Critical infrastructure is defined by the Department of Home Affairs' Cyber and Infrastructure Security Centre (CISC) as: "those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security".[8]

Under the SOCI Act, captured entities are required to take an 'all hazards' approach to risk management across their operations, especially in relation to cyber security. Those assets identified as SoNS have enhanced cyber obligations under the SOCI Act, requiring them to adopt, maintain and comply with a written risk management program, develop a cyber incident response plan, undertake vulnerability assessments, run cyber security exercise and provide system information to develop and maintain a near real-time threat picture.[9]

Certain entities are also required to lodge a board-attested Risk Management Program (RMP) with the CISC. The RMP's role is to identify all hazards that present a material risk to a critical infrastructure asset's availability, integrity, reliability and confidentiality, outlining measures that have been undertaken to prevent or mitigate each risk.[10] For example, mitigations could include enhanced cyber security controls, background checking of critical personnel and having back-ups of key systems.[11]

Given this holistic approach to risk, there is clear scope for critical infrastructure entities employing the use of UAVs in the operations of critical assets to assess the risks associated with UAV use. While physical risks associated with UAV use should be assessed, there is also an impetus for the cyber security integrity of UAVs to be considered and, where appropriate, associated risks mitigated.

8. Security of Critical Infrastructure Act 2018 (SOCI) (cisc.gov.au)
9. Ibid 8
10. Draft Risk Management Program Guidance for Industry (homeaffairs.gov.au)
11. Ibid 10

CRITICAL INFRASTRUCTURE SECTORS

COMMUNICATIONS

FINANCIAL SERVICES AND MARKETS

DATA STORAGE AND PROCESSING

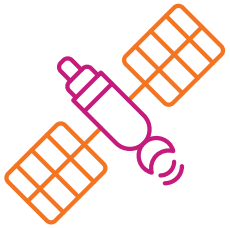
DEFENCE

HIGHER EDUCATION AND RESEARCH

ENERGY

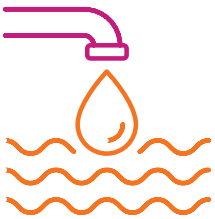
FOOD AND GROCERY

HEALTHCARE AND MEDICAL



SPACE TECHNOLOGY

TRANSPORT



WATER AND SEWERAGE

HOW ARE UAVS USED ACROSS AUSTRALIAN CRITICAL INFRASTRUCTURE?

Operator-controlled UAVs are increasingly being deployed across Australian critical infrastructure, generally for surveillance, monitoring and inspection purposes. They offer real-time remote monitoring, wireless coverage, and remote sensing, delivering efficient and cost-effective data collection and surveillance.[12] Across sectors like energy and transport, which manage complex networks of assets than span large distances, UAVs are especially useful, providing both cost and safety benefits.[13]

A Deloitte report commissioned by the Federal Government in 2020 states that: "The precision of work from the estimation/design phase to the construction phase (of infrastructure) can be improved through the use of drone technology, by providing investors and professionals (particularly managers) with real-time high-resolution videos and images, reducing the costly nature of current work practices based on in-person inspection, a slow and costly process that is often delayed, yields incomplete results and impacts on asset performance. This is also true for the maintenance of assets, where for example, cost savings on standard wind turbine inspection, inspections of bridges and tunnels, were identified as potentially 50%".[14]

The report also highlights specific UAV infrastructure use cases. For example, in both open cut and underground mining operations, operator-controlled UAVs are being used to replace more labour intensive methods of inspection, mapping and surveying, as well as enhancing worker safety. Across manufacturing infrastructure, UAVs can be deployed for maintenance and monitoring of facilities, ultimately optimising processes and increasing efficiencies. as well as increasing operating efficiencies. The use of UAVs is not limited to outdoor applications. And in challenging environments, UAVs fitted with imaging systems and sensors can conduct difficult inspection tasks.[15]

In terms of the economic benefits that could be realised through the increased adoption of UAVs across Australian industry, the report found it could:

- support of the creation of 5,500 full time equivalent jobs;
- increase GDP by $14.5 billion by 2040, with $4.4 billion flowing to regional communities; and
- equate to cost savings of $9.3 billion to 2040.[16]

Drones in agriculture

Across Australia, UAVs are being used to help primary producers manage water and assets, like livestock, buildings and dams. They help map water flows, survey crops and distribute fertilisers more effectively. Aerial photography can also identify issues, such as weed or pest infestations or any geographic issues. This can be followed up by ground analysis to determine specific soil or pest issues. It is estimated By 2028, the Asia Pacific market for agricultural drone systems is projected to grow by more than 300 per cent to $2.9 billion.

Source: www.drones.gov.au

12. UAVs for industrial applications (sciencedirectassets.com)
13. Ibid 4
14. Ibid 4
15. Ibid 12
16. Ibid 4

WHERE ARE UAVS MANUFACTURED?

China has established itself as the world's UAV manufacturing powerhouse, with one company, DJI, holding approximately 70% of total global market share.[17] China is followed by US and European manufacturers in terms of greatest volume of drone output.[18]

DJI drones are primarily manufactured in China's Shenzhen and Tianjin but the company has also established international manufacturing sites.[19] It also has retail shopfronts all over the world.

Chinese dominance of global UAV supply chains has driven concerns domestic Chinese laws could result in UAVs operating in different jurisdictions being used for nefarious purposes, like surveillance and intellectual property (IP) theft.

Under Article 7 of China's National Intelligence Law: "Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work".[20] Under this statute, Chinese-owned companies are bound – or could be compelled – to provide intelligence to the Chinese Communist Party (CCP). In the case of UAVs, this could include, for example, injecting spyware or malware, interception of collected data, and the manufacturing of UAVs with 'back door' vulnerabilities and the ability to surreptitiously communicate with third parties.

On 17 January 2024, CISA release a cyber security guidance related to the use of Chinese-manufactured UAVs in critical infrastructure applications. The guidance states "the use of Chinese-manufactured UAS requires careful consideration and potential mitigation to reduce risk to networks and sensitive information" that could result in "significant consequences to critical infrastructure security and resilience".[21]

These risks include:

- Exposing intellectual property to Chinese companies and jeopardising an organisation's competitive advantage.
- Providing enhanced details of critical infrastructure operations and vulnerabilities increasing the PRC's capability to disrupt critical services.
- Compromising cybersecurity and physical security controls leading to potential physical effects such as theft or sabotage of critical assets.
- Exposing network access details that enhance China's capability to conduct cyber-attacks on critical infrastructure.[22]

The guidance recommends that critical infrastructure operators procure UAVs that follow secure-by-design principles; understand where UAVs are manufactured and domestic laws that may apply to the manufacturer; and consider integrating cyber security and physical security functions to achieve a unified approach to risk management.[23]

17. World's largest drone maker DJI is unfazed by challenges like US blacklist (cnbc.com)
18. Ranking the Leading Drone Manufacturers 2023 | Droneii Insights
19. Where Are DJI Drones Made? | Drones Survey Services (dronesurveyservices.com)
20. Huawei and the ambiguity of China's intelligence and counter-espionage laws | The Strategist (aspistrategist.org.au)
21. Cybersecurity Guidance: Chinese-Manufactured UAS (cisa.gov)
22. Ibid 21
23. Ibid 21

The world's top five civil drone manufacturers

1. DJI, China
2. Skydio, USA
3. XAG, China
4. Parrot, France
5. Jouav, China

DJI bans in Australia and beyond

In May 2023, the Australian Defence Force (ADF) suspended the use of DJI-manufactured UAVs, pending completion of a security audit.[24] The suspension came after it was revealed 3114 drones, cameras and other DJI-manufactured devices were being used across Federal Government departments and agencies.[25] Following the ADF ban, the Department of Home Affairs also wholly suspended its use of DJI-manufactured products, and the Australian Federal Police said it was "transitioning'' away from the technology.[26]

The Australian suspensions came several years after US Department of Commerce announced DJI had been added to its 'Entity List'. While this does not prevent DJI selling its products to US consumers it does restrict the company's use of US technologies, potentially impacting its supply chains and product development. Huawei was placed on the list in 2019. While the specifics regarding DJI's addition to the list were not revealed, the US Government cited human rights abuses related to the misuse of surveillance technologies within China and repressive regimes.[27] Several months later, in October 2022, the US Department of Defence blacklisted DJI from its projects due to alleged links to the Chinese military.[28]

24. Defence grounds China's DJI drones pending security audit | The Australian
25. Risky Chinese-made DJI drones found right across government | The Australian
26. Ibid 25
27. DJI ban: what it means for drone fans and the future of DJI | TechRadar
28. After product ban, the US DoD formally blacklists drone giant DJI [Update] (dronedj.com)

WHAT CYBER THREATS ARE RELATED TO UAVS?

As the use of UAVs continues to expand, new cyber threat vectors have emerged, with UAVs vulnerable to cyber attack as well as being able to be deployed to undertake a cyber attack.

There are five major cyber-related threats that relate to the use of UAVs.

These include:

- GPS spoofing
- Command and control (C2) interception
- Downlink interception
- Distributed Denial of Service (DDoS)
- Signal jamming
- Data exploitation.

GPS spoofing of an UAV "is the act of replicating or falsified production of the (UAV's) GPS signals to deceive a targeted GPS unit or receiver, in particular, manipulating its position, velocity and timing".[29] Put simply, GPS spoofing enables a threat actor to take control of a UAV, diverting its course or causing it to crash. According to researchers, due to "the emergence of low-cost user tunable software defined radios and online open-source projects and tutorials for hobbyist and newbies, launching of GPS spoofing attacks against UAVs have become practical".[30] Research has also shown that a hijacked drone can be used to hijack other drones, potentially resulting in a drone swarm under the control of cyber criminals.[31]

C2 interception occurs when a UAVs communication link is intercepted by hackers seeking to hijack the device.[32] C2 links are an essential part of UAV drone operations, whether the UAV is remotely piloted by a human or programmed to fly autonomously. Researchers from the Massachusetts Institute of Technology (MIT) have successfully illustrated how this occurs on a popular UAV model, using network-mapping tools to capture outgoing packets from its camera, and its controller. They gained root access by exploiting poor password security, which allowed them to crash the device.[33]

Downlink interception occurs when a threat actor accesses data transmitted data between a UAV and its controller.[34] This can occur when the transmitted data is not encrypted, making it more easily hackable. Obviously, such a threat vector presents a significant threat to critical infrastructure, potentially providing a threat actor with key data relating to an asset that could be used maliciously. To counter interception robust encryption between a UAV and its controller should be used, strong authentication and access controls put in place and software and firmware should be regularly patched.[35]

29. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions - PMC (nih.gov)
30. Ibid 29
31. 'SkyJack' Software Finds and Hijacks Drones (pcmag.com)
32. The Anatomy of Drone Hacking: How Attackers Intercept Radio Signals | by Syed Zain M Abidi | ILLUMINATION | Medium
33. How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools (rand.org)
34. Protect Your Drone Program with a Strong Cybersecurity Strategy | Drone Nerds Enterprise
35. IoT empowered smart cybersecurity framework for intrusion detection in internet of drones | Scientific Reports (nature.com)
36. What is a distributed denial-of-service (DDoS) attack? | Cloudflare

Distributed denial of service attack (DDoS) attacks occurs when an information exchange or network is overwhelmed by a flood of rapid requests, which prevents legitimate requests being fulfilled.[36] In the case of a UAV, a DDoS attack could result in an inability to receive control signals, resulting in the UAV crashing or being overridden by a threat actor.[37]

Signal jamming disrupts the communication between a drone and its controller. It involves the intentional use of a transmission-blocking signal, which can be achieved via a GPS jammer, a frequently jammer, a camera-blocking laser or and anti-surveillance jacket, which reflects a signal sent out by a UAV back the UAV itself.[38] This could render a UAV unable to receive or interpret commands properly, potentially sending it off course or resulting in it crashing.

As noted above, UAVs can also be used to enable malicious cyber activity. This is the case when it comes to data exploitation attacks, with UAVs able to penetrate physical protections and be utilised for data exfiltration. This can occur if a small UAV is fitted with a minicomputer, which can "mimic a wi-fi network to steal data, hijack Bluetooth peripherals, perform keylogging operations to steal sensitive passwords, as well as compromise access points, unsecured networks, and devices".[39]

This is not without precedent, as highlighted by a recent (unconfirmed) case in the US. According to cyber researcher, Greg Linares, a US financial firm detected unusual network activity and began an incident response, which found the media access control address of the device being used to access the network was connected to the company's wi-fi. Incident responders went to the roof of the company's premises, where they found two small drones, each fitted with a device that was spoofing the company's wi-fi. This resulted in an employee connecting to the spoofed wi-fi network, with threat actors then able to intercept data.[40]

Finally, it is worth noting emerging risks that may arise through the increased use of AUAVs. According to research undertaken by RAND Corporation, cyberattacks on AUAVs are more difficult to detect because, by removing the human in the loop, it is less likely unusual or unauthorised system behaviour will be noticed.[41] As a result, there is increased difficulty in separating anomalous - possibly malicious – activity from normal activity.[42]

37. Game theoretic solution for an Unmanned Aerial Vehicle network host under DDoS attack - ScienceDirect
38. How To Jam Drone Signals (4 Effective Methods) (discoveryoftech.com)
39. Cybersecurity and Drones: How to Address the Security Threats | Tripwire
40. The Drone Cyberattack That Breached a Corporate Network (blackberry.com)
41. How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools | RAND
42. Ibid 41

WHAT DOMESTIC REGULATIONS AND STANDARDS EXIST FOR UAVS IN AUSTRALIA?

In Australia, there are regulations related to the registration of UAVs drones and remote pilot licencing (RPL). There are no regulations or standards related to the cyber security or design or UAVs, despite the Civil Aviation Safety Authority (CASA) prioritising the publication of "acceptable cybersecurity standards for UAVs" as an "immediate" concern in its 2022 *The RPAS and AAM Strategic Regulatory Roadmap* (the Roadmap).[43] According to the Roadmap, this work was to be completed by 2023, however, thus far no standards have been published.

In Australia, UAVs must be registered to fly if they are being used for business or as part of a person's job. This applies to all UAVs, regardless of size, that provide any type of service.

This includes for activities like:

- selling photos or videos taken from a drone
- inspecting industrial equipment, construction sites or infrastructure
- monitoring, surveillance or security services
- research and development
- any UAV activities undertaken on behalf of an employer or business.[44]

Licencing is not required for UAVs that are flown for recreation.

In addition, individuals require a remotely piloted aircraft (RPA) operator accreditation to fly a UAV for business or in the course of employment.[45] However, RPA operator accreditation is not required for those who fly UAVs for recreational purposes or hold a remote pilot licence (RePL).

An RePL is a more specialised licence, required by individuals who work for or operate a business that holds a remotely piloted aircraft operator's certificate or fly a UAV weighing more than 25kg but less than 250kg. An RePL is also required, regardless of use case, for UAVs more than 150kg. RePLs show the type and weight category of the UAV a holder can fly.[46]

Currently, no design standards exist for UAVs sold or in operation in Australia. In the absence of domestic standards, CASA has at times used a specific operations risk assessment (SORA) developed by international body, the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) to identify and set minimum operational and technical requirements to achieve an acceptable level of safety for UAV operations in Australia.[47]

The Australian Government has paused the planned introduction of a registration scheme for recreational UAVs weighing more than 250g, which was due to commence on 1 July 2023.[48] Such a scheme would bring domestic regulation into line with the US and UK.

43. The RPAS and AAM Strategic Regulatory Roadmap | Civil Aviation Safety Authority (casa.gov.au)
44. Register your drone | Civil Aviation Safety Authority (casa.gov.au)
45. Operator accreditation | Civil Aviation Safety Authority (casa.gov.au)
46. Remote pilot licence | Civil Aviation Safety Authority (casa.gov.au)
47. In-flight break-up involving Airbus Zephyr unmanned aerial vehicle, near Wyndham Airport, Western Australia, on 28 September 2019 | ATSB
48. Registration | Civil Aviation Safety Authority (casa.gov.au)

Significant UAV-related safety investigations in Australia

The Australian Transport Safety Bureau (ATSB) is responsible for investigating reportable occurrences related to drone safety issues. While there is not a high number of UAV-related investigations, those below relate to some significant incidents that have occurred over the past several years.

14/07/23: During an RPAS UAV swarm light show at Docklands in Melbourne, multiple UAVs experienced un-commanded movement. This resulted in multiple errors presenting on the ground control station, failsafe mode activations, collisions with water, each other and multiple aircraft escaping the geo-fence. In total, 440 of the UAVs were lost. The investigation is ongoing.

28/09/2019: A large fixed-wing UAV operated by Airbus was launched from Whyndam in Western Australia to conduct beyond visual line of site, high-altitude aerial work. While climbing through 8,000 ft above mean sea level, the UAV experienced a series of uncommanded turns. It self-recovered from two uncommanded turns, however, the third resulted in the aircraft entering an uncontrolled spiral descent. Despite attempts to return to controlled flight, the UAV sustained an in-flight break-up.

9/01/2019: A large fixed-wing UAV was launched to conduct aerial survey work in the Woleebee Creek area of Queensland. The flight crew consisted of two pilots and two ground crew. Shortly after launch, one of the ground crew observed the UAV pitch up and enter an aerodynamic stall before self-correcting. However, the UAV stalled again from a height insufficient for recovery and crashed.

Source: ATSB

WHAT CYBER-RELATED REGULATIONS AND STANDARDS EXIST FOR UAVS GLOBALLY?

Across the world, several jurisdictions have moved to provide clear guidance in relation to enhancing UAV cyber security, including as it relates to critical infrastructure applications. This includes the EU, which has mandated secure-by-design principles for IoT devices, including UAVs.

For the purposes of this report, guidance provided in the United States (US), the European Union (EU) and the United Kingdom (UK) is considered. It should be noted that in both the US and UK, drones weighing more than 250g must be registered regardless of whether they are used for business of recreation purposes.

United States

In the US, CISA has produced a number of key guidance documents to help manage cyber security risks associated with UAVs. These include a *Secure your drone: Privacy and data protection guidance*, *Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges* and the previously noted *Cybersecurity Guidance: Chinese-Manufactured UAS*. According to CISA, providing risk mitigation guidance and sharing threat and vulnerability information is key to mitigating cyber risks associated with UAVs.[49]

CISA notes that "the safe and secure integration of UAS, or drones, into the national airspace system and across critical infrastructure organizations is essential to maintain the security and resilience of our national critical functions … A whole-of-government approach is required to incorporate cybersecurity and physical security into the policies and procedures that support secure drone operations, reliable threat discrimination through air domain awareness, and the effective mitigation of credible threats to national security and public safety".[50]

CISA's *Secure your drone: Privacy and data protection guidance*, released in January 2023, provides a comprehensive guidance for drone users to protect their data and privacy before, during, and after flying their drone.[51] It warns that as IoT devices, UAVs "take on many of the vulnerabilities of these connections and are susceptible to cyberattacks and privacy violations".[52]

The guidance covers key areas including:

- Pre-flight security: UAV purchase; setting up a digital account and associated applications; connecting to the internet and/or other devices; and downloading and maintaining software and firmware.
- During flight security: Utilising GPS while in flight; using a camera to take pictures or recordings during flight; and commanding and controlling a UAV via ground control stations (e.g., hand controller, laptop, tablet, or smartphone).
- Post-flight security: Storing UAV data; UAV companies may collect and retain data including personal data, photos, and videos.[53]

CISA's *Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges* guidance specifically addresses UAV security risks as they relate to critical infrastructure. It notes that "because of their physical and operational characteristics, UAS can often evade detection and create challenges for the critical infrastructure community".[54]

49. Unmanned Aircraft Systems | Cybersecurity and Infrastructure Security Agency CISA
50. Ibid 49
51. Secure Your Drone: Privacy and Data Protection Guidance | CISA
52. Ibid 51
53. Secure Your Drone: Privacy and Data Protection Guidance (cisa.gov)
54. Unmanned Aircraft Systems: Addressing Critical Infrastructure Security Challenges Fact Sheet (cisa.gov)

The guidance defines key threats as:

- Weaponised or smuggling payloads: UAVs may be capable of transporting contraband, chemical, or other explosive/weaponised payloads.
- Prohibited surveillance: UAVs can silently monitor a large area from the sky for nefarious purposes.
- IP theft: UAVs can be used to perform cybercrimes involving theft of trade secrets, technologies, or sensitive information.
- Intentional disruption: UAVs may be used to disrupt critical infrastructure operations.[55]

European Union

In October 2023, the EU release its *Communication on countering potential threats posed by drones* (the Communication), a key action related to its Drone Strategy 2.0 for a *Smart and Sustainable Unmanned Aircraft Eco-System in Europe*.

The Communication highlights the need to establish a common understanding of applicable procedures to face the continuously evolving threats possibly posed by UAVs and account for rapid technological developments.[56] It notes that "the rapidly advancing capabilities of drones pose a growing security risk" … "especially true for private operators of critical infrastructure", which should consider UAV threats in risk assessments.[57] It also cites examples of terrorists attempting to use UAVs, sightings of suspicious drones around critical infrastructure, such as energy facilities, airports and ports, and the use of UAVs for digital reconnaissance.[58]

A central tenet of the Communication is the recommendation that standardisation and certification of UAVs, especially from non-EU countries, be considered. It notes that "there remains uncertainty over how well protected the data are that are gathered by certain detection systems … in addition, it is important to prevent as much as possible the hacking and misuse of counter-drone systems by ensuring the cyber resilience of their components".[59]

The Communication also ties into *EU Cyber Resilience Act* (the Act), which has introduced mandatory cyber security requirements for IoT devices manufactured and sold in the EU.[60] The Act enforces secure-by-design principles and requirements to address cyber vulnerabilities, with UAVs "covered as products with digital elements by these new rules, with the exception of those developed exclusively for national security or defence purposes".[61]

In relation to critical infrastructure, in 2023 the EU published a key guidance, *Protection against Unmanned Aircraft Systems - Handbook on UAS protection of critical infrastructure and public space: A five phase approach for C-UAS stakeholders*.[62]

The guidance notes that UAVs "can pose a cybersecurity threat by targeting local wireless networks and disrupting communications, delivering malware, hijacking and/or manipulating sensitive data", and can, in fact, also become the target of cyber attack as threat actors "may gain control and alter its route, gain access to its data or destroy it".[63]

The guidance takes a five-phased approach, covering risk and threat analysis through to solution implementation and operation. It also encourages a holistic approach to UAV risk management, taking an 'all hazards' hazards approach, as contained within the SOCI Act.

In 2023, the EU also published a specific guidance to help protect buildings and sites from UAV risks. The guidance, *Protection against Unmanned Aircraft Systems - Handbook on UAS risk assessment and principles for physical hardening of buildings and sites.*[64] It provides insight into various proactive physical protective measures to protect against UAV threats, focusing on their typology, performance, challenges and constraints.[65]

55. Ibid 54
56. EUR-Lex - 52023DC0659 - EN - EUR-Lex (europa.eu)
57. Ibid 56
58. Ibid 56
59. Ibid 56
60. EU Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
61. EUR-Lex - 52023DC0659 - EN - EUR-Lex (europa.eu)
62. Protection against Unmanned Aircraft Systems - Publications Office of the EU (europa.eu)
63. Ibid 62
64. Ibid 62
65. Ibid 62

United Kingdom

Currently, no UAV-specific cyber security regulations or standards are in operation in the UK. However, the Civil Aviation Authority (CAA) has proposed an overhaul of existing UAV laws in the UK, which are currently being consulted.

Under the proposed changes, the UK would move to align with EU class-marking and product standards, implementing specific technical standards developed by the British Standards Institute.[66] They would also introduce compulsory Remote ID to communicate the identification and location of a UAV during a flight, enabling intervention when a UAV is being used for malicious purposes.[67]

While no mandatory standards exist, the CAA does provides guidance regarding the implementation of security and privacy requirements as they pertain the UAVs.[68] The CAA states "these security measures and controls are designed to be reasonable and proportionate … to protect the system from unauthorised modification, interference, corruption or command/control action".[69] Appropriate actions may include the development of a cyber security policy, cyber awareness training, manufacturer security updates, a patching policy and third-party and supply chain oversight.[70]

It should also be noted that in 2023, UAV attacks on UK critical infrastructure were added to the National Risk Register, which notes that "drones are a novel vector to commit crimes and attacks".[71]

How to make a UAV more cyber secure

- Update the UAV's firmware and apply a manufacturer's patches
- Use strong passwords for the base station application
- Use updated anti-virus software for your UAV controller device
- Subscribe to a VPN service to encrypt the UAV's connection
- Limit the number of devices that can connect to the base station[72]

66. Review of UK UAS Regulation - Consultation (caa.co.uk)
67. Ibid 66
68. Cyber Security Certification | Civil Aviation Authority (caa.co.uk)
69. Ibid 68
70. Ibid 68
71 Drone attacks on UK critical infrastructure "relatively small but possibly significant" - Unmanned airspace
72. Cybersecurity and Drones: How to Address the Security Threats | Tripwire

CONCLUSION AND RECOMMENDATIONS

There is no doubt the increased use of UAVs to monitor and maintain Australia's critical infrastructure offers significant advantages and is an opportunity that should be harnessed. However, to fully realise the potential of UAVs, cyber security risks associated with their critical infrastructure applications must be addressed.

As this report highlights, there are significant cyber risks associated with the use of UAVs. But, through the implementation of clear guidance and secure-by-design principles, many of these risks can be mitigated.

Therefore, it is recommended that:

- The CISC publishes guidance related to the cyber threats associated with the use of UAVs across Australia's critical infrastructure assets. This would encourage critical infrastructure operators to consider UAV cyber security and mitigate potential risks. The guidances provided by CISA in the US provide a key blueprint for such guidance.
- UAV manufacturers operating in the Australian market should be made aware of and be encouraged to comply with the Federal Government's voluntary *Code of Practice: Securing the Internet of Things for Consumers*, a set of 13 principles for IoT manufacturers that addresses issues vulnerability disclosure and security updates.[73]
- Cyber security impact assessments could be considered for all UAVs sold in Australia, with vulnerabilities disclosed to manufacturers for remediation. This would include ongoing assessments to ensure vulnerabilities have been addressed. If a UAV type was deemed as having significant cyber security vulnerabilities, it should be removed from sale and recalled from use.

73. Code of Practice, Securing the Internet of Things for Consumers (homeaffairs.gov.au)

omni

CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE