DRONE-RELATED CYBERSECURITY THREATS TO AUSTRALIA'S CRITICAL INFRASTRUCTURE

Simone Chitsinde, Andrew Giumelli, and Frank den Hartog

NOVEMBER 2025

Innovation Central Canberra

A collaboration led by cisco

FOUNDATION PARTNERS

cisco | UNIVERSITY OF CANBERRA

PART OF THE NIIN National Industry Innovation Network

This independent white paper was commissioned by

DRONESHIELD

CONTENTS

Executive Summary

Cybersecurity attacks delivered via drones present an emerging concern for Australia's critical infrastructure. Drones increasing capability and accessibility, as well as the distinct advantages they offer make them an attractive tool for operators, and actors wishing to interrupt Australian critical infrastructure. This report examines whether such threats are practical, and whether limited deployment of drone detection capabilities across Australian critical infrastructure may be obscuring an understanding of the threat landscape.

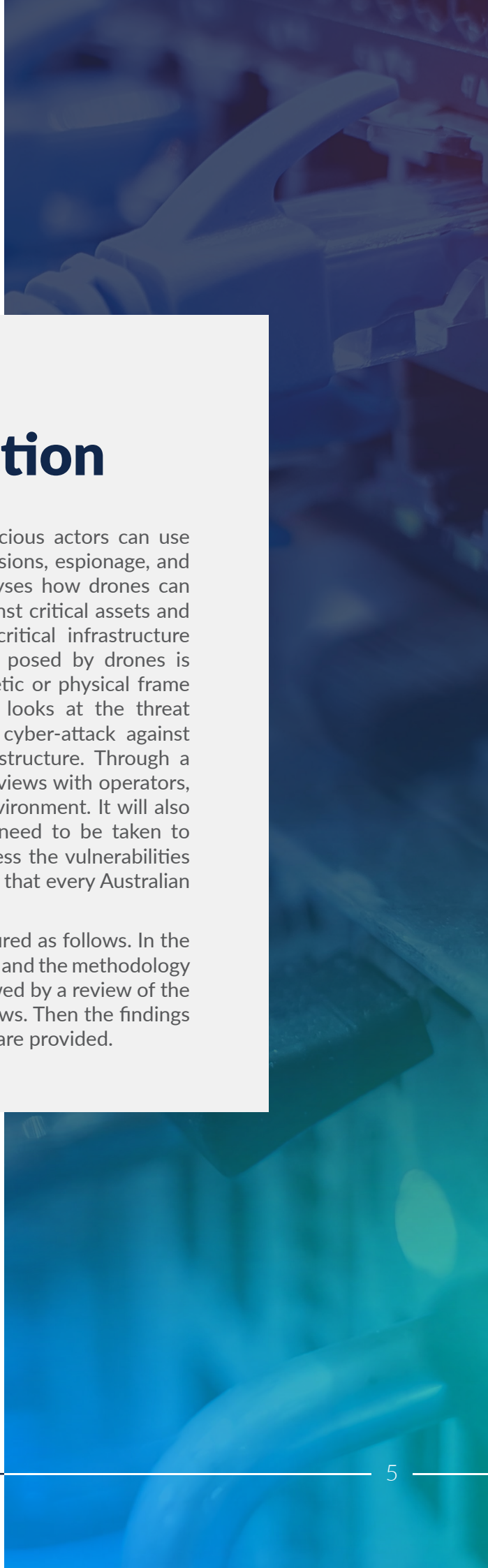
To address this question, this report combines a review of existing literature with eight case study interviews involving Australian critical infrastructure operators across six out of eleven sectors regulated under the Security of Critical Infrastructure Act 2018: energy, transport, healthcare and medical, data storage and processing, water and sewage, and communications sectors.

The literature review revealed that current research often focuses on the vulnerabilities within drones and their protocols rather than drone-enabled cybersecurity threats. It also revealed that security concerns are still primarily framed in terms of kinetic attack vectors, such as physical disruption. One recorded incident of drone-enabled cyber compromise was identified accentuating both the rarity of publicly available cases and the lack of sustained scholarly attention to this threat pathway.

Interviews with critical infrastructure operators revealed that this lack of awareness and attention in the literature is mirrored in practice. Many operators expressed limited awareness of drone-enabled cyber threats, treating them as a currently low-probability scenario. This perception is reinforced by the absence of recorded incidents in Australia, and the assumption that adversaries would likely use more conventional means of cyber intrusion. Government guidance was also cited as minimal, leaving operators without structured frameworks for assessment or effective defensive solutions.

We outline six key recommendations.

1. Targeted education and knowledge sharing initiatives are required to raise awareness of the threat among operators.
2. Threat modelling undertaken by operators should explicitly incorporate drones as potential vectors, moving beyond traditional assumptions of kinetic drone attacks.
3. Government, industry and operators should collaborate on developing mitigation strategies that align with Australian regulatory constraints.
4. Operators should critically review their own adoption of drones in day-to-day operations and employ the same risk governance as with other security measures.
5. Government, operators and researchers should collaborate to facilitate simulation exercises to generate real-world data.
6. A sustained program of research is needed to establish a stronger evidence base on the threat vector and consequences of drone-enabled cyber threats.



1. Introduction

As drone technology advances, malicious actors can use these systems to execute cyber intrusions, espionage, and service disruptions. This report analyses how drones can be used to launch cyber-attacks against critical assets and reviews the current awareness of critical infrastructure operators to the threat. The threat posed by drones is typically considered from only a kinetic or physical frame of reference. This report, however, looks at the threat of drones being used as part of a cyber-attack against operators of Australia's critical infrastructure. Through a structured literature review and interviews with operators, this report will assess the current environment. It will also provide recommended actions that need to be taken to further examine the threat and address the vulnerabilities to protect the essential infrastructure that every Australian relies on.

The remainder of the report is structured as follows. In the next sections, definitions are provided and the methodology undertaken is described. This is followed by a review of the literature and detailing of the interviews. Then the findings are presented and recommendations are provided.

2. Definitions

2.1. CYBERSECURITY

Cybersecurity refers to the protection of digital systems, networks, data, and devices from unauthorised access, disruption, or destruction (NIST 2015). It is underpinned by the CIA Triad of Confidentiality, Integrity, and Availability (NIST 2020; SentinelOne 2024):

- Confidentiality ensures that data is accessible only to authorised individuals
- Integrity involves preserving the accuracy and completeness of data across its lifecycle from modification or destruction
- Availability ensures that data and systems remain reliably operational or accessible when needed.

2.2 DRONES

Unmanned Aerial Systems (UAS), commonly known as drones, are integrated platforms combining an unmanned aerial vehicle (UAV), ground control station, communications links, and supporting infrastructure (Gillis et al 2024). This integrated design means drones operate as more than aerial platforms; they are networked systems that combine hardware, software and dataflows. Drones are being incorporated into broader technological and commercial settings, which shapes both their opportunities for use in various settings and the challenges they present (Deloitte Access Economics 2020).

Civilian and commercial (Group 1 and 2) drones form the focus of the report, in contrast to military drones. Military drones are typically designed with bespoke security features, operate under tightly controlled conditions, and are subject to advanced defensive oversight. By contrast, civilian drones are mass-produced, widely available, and often reply on open communication protocols and off-the-shelf components (Labib et al 2021). Their accessibility means that complex, networked systems which were once restricted to governments and state actors can now be acquired and operated by individuals, hobbyists, or even malicious actors with minimal technical training. This diversity of purpose situates civilian drones within a broader technological and regulatory landscape that demands careful consideration in terms of vulnerabilities and governance (The Cyber Security Cooperative Research Centre and Omni 2024).

The operation of drones in Australia is regulated by the Civil Aviation Safety Authority (CASA) and is primarily legislated the Civil Aviation Safety Regulations 1998 (Part 101) . These regulations detail the acceptable use of drones across both civilian and commercial scenarios including flying near restricted airspace, in populous areas, maintaining line of sight, maintaining licenses and registration. Under Australian aviation laws drones are classified as aircraft and it is a criminal offence to damage or interfere with them in both kinetic and non-kinetic means. However, exemptions exist for authorised entities such as law enforcement and defence agencies, which may deploy counter-drone technologies under specific legal frameworks.

2.3 CRITICAL INFRASTRUCTURE

Critical infrastructure is defined in the 2023 Critical Infrastructure Resilience Strategy 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." (Critical Infrastructure Security Centre 2023).

The Security of Critical Infrastructure (SOCI) Act 2018 defines 11 critical infrastructure sectors that operate critical infrastructure assets and the security obligations on those operators of critical infrastructure that Australian residents rely on (Critical Infrastructure Security Centre 2018). The 11 sectors defined are:

- Communications
- Data storage and processing
- Financial services and markets
- Water and sewage
- Energy
- Health care and medical
- Higher education and research
- Food and grocery
- Transport sector
- Space technology
- Defence industry

For this research a high-level assessment about the potential vulnerability of each sector was conducted to narrow the scope and enable greater insights. From this, the below sectors were selected to focus on through the interview section of the research:

- Communications
- Data storage and processing
- Water and sewage
- Energy
- Health care and medical
- Transport

Within critical infrastructure, cybersecurity extends beyond conventional Information Technology systems (IT) and extends to Operational Technology (OT), Industrial Control Systems (ICS), and increasingly, Internet of Things (IoT) devices (The Cyber Security Cooperative Research Centre and Omni 2024). Unlike purely digital systems, these technologies govern physical processes: the operation of electricity grids, the flow of water, or the management of hospital equipment. The risk is therefore not confined to data loss or espionage but to service interruption with direct societal and safety consequences.

This interdependence is significant when considering the potential cybersecurity threat posed by drones. Civilian-operated drones, which are cheap and widely available across the nation, represent new avenues of accessibility to critical infrastructures that were once considered insulated. The extent to which these new avenues translate into genuine cybersecurity threats for critical infrastructure nationally will form this report.

3. Methodology

Two research approaches were utilised in conducting this project. First, a structured review of the written literature describes any theoretical or actual use of drones in cyber-attacks especially those related to critical infrastructure. The findings of this literature review were combined with the results of several informal, unstructured, qualitative stakeholder and subject matter expert interviews. This developed a rich understanding of how drones can act as platforms for cyber-attacks against critical infrastructure. The literature review and informal stakeholder meetings consequently informed the more structured approach taken in conducting in-depth interviews with various critical infrastructure operators.

A structured literature review was conducted at the beginning and throughout the project to build an understanding of existing work that has been undertaken in this area and the concepts at play. Searches were carried out across Google Scholar and University of Canberra library databases: Scopus, IEEE Xplore, MDPI, ACM Digital Library and arXiv. To widen coverage, we also inspected reference lists of shortlisted papers and ran forward citation searches.

Database searches employed combinations of key terms including variations of ("drone" OR "UAS OR "UAV") AND ("cyber*" or ...) AND ("critical infrastructure" OR "energy", "transport", "telecommunications", "health"). These phrases were refined iteratively by adding synonyms encountered during screening (for example "evil twin" or "GNSS spoofing"). Australian-specific searches added terms such as "Australia", "Security of Critical Infrastructure Act", "CASA", and "ACSC".

Primary data collection involved informal meetings with subject matter experts (both locally and internationally) and interviews with critical infrastructure operators across Australian critical infrastructure sectors. Potential organisations suitable for interviews were selected to cover six out of the eleven sectors defined under the Security of Critical Infrastructure Act 2018: communications, transport, energy, health care and medical, water and sewerage, and data storage and processing. These sectors were selected based on the perceived vulnerability they may have to a drone enabled cyber attack. Typical factors that were considered include geographical dispersion of assets, IT and OT reliance of assets, inter-relatedness of critical infrastructure, and the scope of the project. The final interview cohort comprised of eight participants represents six critical infrastructure sectors.

Interviews were conducted between 7 July 2025 to 25 July 2025. The questions addressed six key areas: awareness of cyber and kinetic drone threats, assessment of the risk (including impact and likelihood), existing security practices, industry and sector preparedness, and potential vulnerabilities to the four identified attack types across both information and operational technologies. Although the set of structured interviews were guided by a set of questions, the format still allowed for further exploration of sector-specific concerns while maintaining consistency across core topics. The questions posed to the interviewees are provided in the Appendix.

4. Literature Review

4.1 FINDINGS

This review synthesises current literature since 2018 on the cyber threats posed to critical infrastructure through the malicious use of civilian or commercial drones. It primarily focuses on drones acting as enablers or vectors for cyber-attacks rather than kinetic threats, their operational impacts, and the practical implications for critical infrastructure operators in Australia. In the remainder of this section recent research and case studies are described to showcase the vulnerabilities in critical infrastructure that enable drones to exploit using various cyber pathways.

Market growth and low entry costs have expanded the accessible threat surface, with recent analyses by Deloitte Access Economics (2020) estimating the Australian drone sector to contribute around AU$14.5 billion to national GDP by 2040, generating cost savings of up to $9.3 billion by 2040, with sustained annual employment of around 5,500 jobs. Uptake is expected across multiple industries related to critical infrastructure including agriculture, government, transport and more. While these projections emphasis an economic opportunity, they also imply a rapid expansion in the number and variety of drone platforms operating in and around critical infrastructure, creating a richer opportunity structure for cyber intrusion for non-state actors and opportunistic threat actors. Best et al (2020) analyse cyber threats from drones and position them as potential cyber-attack vectors when used for proximity-enabled access, data exfiltration, and timing deception that bypass perimeter-centric-security measures. They also caution that when drones used in critical infrastructure operations are compromised, they can be repurposed for cyber-physical attacks on the very assets they were intended to protect. While Best et al.'s (2020) case study focuses on U.S. federal agencies such as the Cybersecurity & Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA), the principle is equally applicable in Australia, where drones are increasingly integrated into inspection, monitoring and logistics roles within SOCI-regulated sectors.

The Cyber Security Cooperative Research Centre and Omni (2024) also observe that drones are now the norm across Australian critical infrastructure operations but sit outside any cybersecurity-specific drone regulation or standard, leaving critical infrastructure operators to manage any drone risks under generic all hazards obligations within the SOCI. More importantly, they argue that the cyber threat is not confined to critical infrastructure owned drones as even drones operated by individuals or hobbyists can be equipped with mini-computers and flown from outside site boundaries, providing proximity access for "GPS spoofing, command and control (C2) interception, downlink interception, distributed denial of services (DDoS), signal jamming, [and] data exploitation" (The Cyber Security Cooperative Research Centre and Omni (2024), without the human operator ever crossing a fence line.

This threat has been demonstrated in a 2022 incident where threat actors allegedly used two modified civilian drones equipped with Wi-Fi pineapple devices and Raspberry Pi to infiltrate a United States-based financial services firms' network and harvest staff credentials by bypassing the firm's perimeter security (Claburn 2022; Ray 2024). This incident demonstrates that drone-borne cyber-attacks have moved beyond proof of concept into operational use against high-value targets, and that physical perimeter controls for certain critical infrastructure can offer little protection against aerial delivery of network intrusion tools. Concerningly, it further illustrates how commercially available hardware can be weaponised with minimal technical barriers, lowering the entry threshold for a wider range of threat actors.

These cases also showcase an important finding that success was not dependent on exploiting novel vulnerabilities, but on adapting established cyber-attack techniques to a drone. This aligns with Best et al.'s (2020) framing of drones as mainly proximity enabled vectors capable of bypassing traditional security postures. However, where Best et al. presents a conceptual model, Schneider et al. (2021) undertake a scenario-based analysis of threats posed to critical infrastructure by civilian drones, identifying that the detectability and risk of an attack are shaped by their on-site geometry, attacker intent and time available for defenders to act. While their cyber-attack coverage is high level and lacks empirical disruption data, their modelling offers an operational lens for understanding how drones could deliver jamming or spoofing payloads against critical infrastructure.

The energy sector has been cited by Kootala et al. (2023) as the most vulnerable to drone threats due to its distributed assets and reliance on precise communications and timing systems. They report multiple incidents of low-cost drones probing or attacking substations, including attempts to induce short circuits and disrupt radiofrequency communications. While the report places considerable weight on the physical disruption of such attacks, the methods they describe could support cyber-attacks such as GNSS spoofing or wireless compromising, illustrating the sector's potential vulnerability to drone-enabled cyber threat. A recent example of this is found in a 2020 incident in the United States, where a modified civilian drone was recovered after crashing into the roof of a Pennsylvania substation (Lyngaas 2021). The FBI alongside the Department of Homeland Services and National Counterterrorism Centre concluded that the device was customised to create a short circuit and was the first recorded case in the United States of a drone being used to deliberately target energy infrastructure (Lyngaas 2021). While the intent in this case was physical sabotage, the operational pathway of bypassing perimeter security to deliver a customised payload to operational equipment could equally be leveraged for cyber-attacks.

As of August 2025, there are no publicly verified cases of drone-delivered cyber compromise of Australian critical infrastructure and peer-reviewed English-language literature on the topic remains sparse. However, the 2022 Pennsylvania drone cyber-attack incident (Claburn 2022; Ray 2024), demonstrates the technical prerequisites for such an attack already exist. The absence of recorded incidents nationally may reflect both the inherently impracticality of executing such attacks over traditional cyber-attack methods and the lack of open-source reporting, rather than a lack of capability. Additionally, the potential impact of a drone-enabled cyber-attack is highly dependent on the operational and geographical characteristics of the target which varies by each sector. For example, air-gapped industrial control systems maybe insulated from directed wireless compromise whereas facilities using short-range wireless protocols for control or monitoring, especially those in open, accessible terrain, may be more exposed. Similarly, remote or sparsely staffed facilities may reduce the capacity for rapid on-site detection and response whereas densely populated, physically secure sites may present fewer opportunities for prolonged proximity (Best et al. 2020).

Overall, post-2018 literature suggests that while publicly documented cases of drone-enabled cyber threats against critical infrastructure remain sparse, with explored accounts relying on proof-of-concept demonstrations and theoretical modelling. While those works have established the technical feasibility of such attacks, empirical, publicly available data on recorded occurrences, especially in Australia, is limited. This gap presents a need for further research particularly into sector specific vulnerabilities, and the operational conditions under which drones could be used to mount a cyber-attack. Without substantial evidence, the risk assessments of critical infrastructure operators for this problem may continue rely on extrapolation rather than observed trends, leaving blind spots in policy and security planning.

Summarising, the literature review integrates both academic and non-academic perspectives, spanning different national contexts. The four core sources summarised in Table 1 collectively provide insight into the evolving role of drones as enablers of cyber threats to critical infrastructure. The first paper: Flight Critical: Drones, Cyber Security and Critical Infrastructure provides a non-academic policy-oriented report that explores drone cybersecurity threat scenarios and offers strategic recommendations for operators and policy makers. How to Analyze the Cyber Threat Against Drones from RAND provides a conceptual framework to drone cybersecurity threats while the two academic studies Scenario Analysis of Threats Posed to Critical Infrastructures by Civilian Drones and Drones Are Endangering Energy Critical Infrastructure apply structured methodologies to assess specific drone threats vulnerabilities.

While all address drones' cybersecurity threats in relation to critical infrastructure, only three explicitly examine the cybersecurity dimension to varying degrees, presenting a persistent gap in empirical, incident-based research on the topic. Table 1 outlines the scope, focus and evaluated relevance of each work to the intersection of drones, critical infrastructure and cybersecurity.

	Publisher	Year	Academic/Non-Academic	Country of Focus	Drones	Critical Infrastructure	Cybersecurity
Flight Critical: Drones, Cyber Security and Critical Infrastructure	Cyber Security Cooperative Research Centre & Omni	2024	Non-academic	Australia	Y	Y	Y
How to Analyze the Cyber Threat Against Drones	RAND	2020	Non-academic	United States	Y	Y	Y
Scenario Analysis of Threats Posed to Critical Infrastructures by Civilian Drones	Research Publishing	2021	Academic	Germany	Y	Y	Y
Drones Are Endangering Energy Critical Infrastructure	MDPI	2023	Academic	United States	Y	Y	N

Table 1: Summary of key literature reviewed

4.2 MAPPING DRONE CYBER-ATTACK VECTORS

	What the drone does	MITRE ATTACK Enterprise technique	MITRE ATT&CK ICS technique
Wireless compromise	Broadcasts a fake access point and cracks local wireless protocols to gain network entry to mount a cyber-attack within the network	T1557 Adversary-in-the-Middle T1557.004 Evil Twin T1498 Network Denial of Service T1498.002 Reflection Amplification	T0830 Adversary-in-the-Middle
GPS/GNSS Spoofing	Transmits counterfeit GNSS signals that alter position, navigation and timing data.	T1565 Data Manipulation T1565.002 Transmitted Data Manipulation	T0856 Spoof Reporting Message
Signal Jamming	Emits a high power radio frequency noise that blocks legitimate wireless communications.	T1498 Network Denial of Service	T0814 Denial of Service
Reconnaissance	Conducts aerial scans and radio frequency mapping to catalogue devices, networks and layouts. Relays captured data over its own RF hardware (WiFi, LTE, or other) to external infrastructure	T1595 Active Scanning T1595.002 Vulnerability Scanning T1041 Exfiltration Over C2 Channel T1040 Network Sniffing	T0840 Network Connection Enumeration T0884 Connection Proxy T0842 Network Sniffing

Table 2: Common drone cyber-attack vectors mapped to MITRE ATT&CK Framework

Table 2 Common drone cyber-attack vectors mapped to MITRE ATT&CK Framework to capture the dominant drone-enabled cyber threats discussed across literature and examined through subsequent case study interviews. Attack types are then mapped to MITRE ATT&CK (The MITRE Corporation 2025) techniques and sub-tactics to make the behaviours comparable with enterprise and ICS threat models. This dual mapping showcases risks where IT and OT environments intersect, a vulnerability Australian critical infrastructure operators may face where legacy industrial control systems increasingly interface with enterprise networks.

4.3 CLASSIFICATION OF RECONNAISSANCE AND SIGNAL JAMMING AS CYBER ATTACKS

Modern drone operations are computer-to-computer interactions: they concern processors and software that target other information systems and data. According to the NIST (2015), a cybersecurity threat comprises any unauthorised act that jeopardises the confidentiality, integrity or availability (CIA) of a digital system, information technology or the information itself. When drones specifically target networked systems or digital infrastructure, their operations can constitute cyber threats.

Reconnaissance activities qualify as confidentiality breaches when they involve the unauthorised acquisition of sensitive digital information such as network channels, communication protocols, device behaviours alongside visual observation. Signal jamming represents an availability breach when it deliberately disrupts digital communications, timing feeds or other systems that operators rely on. These operations may therefore qualify as cyber-attacks because they use technological means to exploit vulnerabilities in digital infrastructure, even when conducted through wireless methods.

What this categorisation reveals is that drone-enabled cyber threats may not constitute entirely novel attack types but, instead, showcase a shift in how established cyber techniques can be deployed against critical infrastructure by different vehicles. It raises the question of whether defensive measures within various critical infrastructure built around traditional intrusions can cope when those same tactics are executed through drones. It also establishes a foundation on which operators themselves to consider further analysis and empirical testing.

5. Interviews

Eight interviews were conducted with critical infrastructure operators or companies that provide services to critical infrastructure operators, representing a cross-section of the critical infrastructure sectors that were considered most vulnerable to a cyber-attack from drones.

Table 3 presents a summary of the high-level findings from the interviews and demonstrates the broad awareness, understanding and level of vulnerability that each interviewee indicated to the attack types discussed in this report.

A commonality in all interviews was the consideration of drones as a kinetic threat to critical infrastructure. All operators interviewed indicated they are actively considering how drones could cause damage or interruptions to their operations by mounting a payload or nuisance attack. Some indicated awareness of fly-overs or flights near their operations which have been attributed to hobbyists or video content creators (Interview 4 cited specific example of video content appearing on YouTube). However, none have reported a drone related incident causing physical damage or known interruption to their facilities. Although the kinetic threat posed by drones is not a consideration of this research, it established a baseline of understanding with each interviewee.

Operators varied in their consideration of the cyber threat that drones pose. Some have not given this any formal consideration, and discussions often triggered them to think on the spot. Interviewees that had considered the cyber threat of drones had typically considered one or more of the attack types that were presented and were able to discuss more structurally how these attacks may or may not be relevant for them.

	Interview 1	Interview 2	Interview 3	Interview 4	Interview 5	Interview 6	Interview 7	Interview 8
Sector	Communications	Communications	Data storage and processing	Data storage and processing	Health	Transport	Transport, Energy, Water and Sewage	Energy
Considered Kinetic threat of drones	Y	Y	Y	Y	Y	Y	Y	Y
Considered cyber threat of drones	N	Y	Y	Y	N	N	Y	Y
Processes to detect and respond to drones	N	N	N	N	N	N	N	N

Table 3: Summary of interview results relating to the awareness and preparedness of drone related attacks

Table 4 is an assessment of the risk that critical infrastructure run given their vulnerability to each attack type. The assessment ratings were formed based on the discussions during the interview. The rating is based on the type of assets that are operated (including function, geography, operational technology, and information technology), the current protections that are in place, and the potential impact of an attack. All operators were assessed as low or medium for each attack type. The table indicates that none of the interviewees perceive that there is a high risk of their critical infrastructure to be compromised by a drone-assisted cyber attack.

	Interview 1	Interview 2	Interview 3	Interview 4	Interview 5	Interview 6	Interview 7	Interview 8
Sector	Communications	Communications	Data storage and processing	Data storage and processing	Health	Transport	Transport, Energy, Water and Sewage	Energy
Risk of GPS/GNSS spoofing attack	Med	Low	None	None	Low	Low	Low	Low
Risk of signal jamming attack	Med	Med	None	None	Low	Med	Low	Low
Risk of wireless compromise attack	Low	Low	None	None	Low	Med	Low	Low
Risk of reconnaissance attack	Med	Med	Med	Med	Low	Med	Med	Med

Table 4: Assessment of level of risk of each attack type to critical infrastructure operator based on interview responses

Many operators indicated that they do not currently have any viable options for defending themselves against drones. Some operators had considered the problem more deeply than others. One commented they had researched counter drone solutions, their efficacy and their legality, and determined that they would not be suitable due to their understanding of current technology and legislation. Several interviewees expressed that they understood that defending against drones was made difficult due to their classification as an aircraft by CASA and the subsequent protection that comes with this classification. Interviewees indicated that their only mechanism for the detection of drone activity was CCTV and sightings by personnel or the public, and their only response available was to report the sighting to the police or other relevant authorities. However, there was also a perception that these authorities often did not follow up with appropriate enforcement, leading to a lack of deterrence for hobbyists and attackers.

Many interviewees mentioned that the use of drones as a vehicle to mount a cyber-attack seems unlikely, because a threat actor would have access to easier, more direct, or more practical means to attempt to breach an organisation's cyber security. One interviewee expressed that attackers are typically using volume (such as Distributed Denial-of-Service attacks, i.e. DDoS), human factors, and (increasingly) Artificial-Intelligence (AI) enabled attacks, rather than drone attacks. Another mentioned that there is a requirement in the Telecommunications Act 1997 that retailers and distributors are to be allowed access to telecommunications exchanges to install the required equipment for provision of their services. Another example was the healthcare sector, which is broadly open to the public and is therefore hardened against attacks that might occur in proximity.

It was evident through many interviews the interconnectedness of critical infrastructure. Many operators cited their reliance on other critical infrastructure and their lack of control over the delivery of the services upon which they rely. This reliance on external services typically resulted in operators having redundancy or backup options. For example, if an asset was reliant on electricity it might have several independent power supplies, battery storage, and generators. These contingency systems ensure continued operation even if the services provided by another critical infrastructure operator were interrupted. This approach of building resilience into the interdependent systems would appear to also have the effect of preventing a cascading failure of critical infrastructure should an attack be successful on one.

Interviewees indicated strong cyber security posture, several reflecting that their organisation and their sector had made significant advances in their cyber security in recent years. One interviewee referenced a significant cyber security breach two years prior that had initiated investment and improvements in their cyber security. Much of the investment and improvement would increase their defence against a drone enabled attack in addition to traditional cyber-attacks. Defences such as detection/monitoring software, air-gapping, network segmentation, removal of wireless networks, and user privilege reviews were cited as just some of the steps taken to improve security.

One interviewee directly mentioned their reliance on government advice and guidance as a key driver for the physical and cyber security action they take. Other interviewees alluded to this indicating that they actively engage in government information sharing such as Trusted Information Sharing Network (TISN) managed by the Critical Infrastructure Security Centre (CISC) within the Department of Home Affairs. CISC also provides risk guidance, white papers and other resources to operators of critical infrastructure. Some interviewees demonstrated an active scanning of the available resources while others showed a more passive engagement. One interviewee held a position that covered several facilities in the APAC region and demonstrated a strong understanding of regulatory environments and advice across the region. This interviewee reflected on the stronger regulation of drones in many countries in the APAC region including Japan and Singapore.

The operation of critical infrastructure assets is sometimes contracted out to vendors that cover some or all aspects of the operation but are not the owner of the assets. One vendor that falls into this category referenced their contractual obligations to ensure the ongoing operation of the assets under their care, and the significant penalties in place should they fail to meet their obligations. One of the penalties referenced was a financial penalty calculated based on downtime, this appeared to be a significant motivator for operators to take action to protect against any threat that might cause an interruption to services.

6. Findings

This research report examined the cybersecurity threats drones pose to Australia critical infrastructure through an extensive literature review, threat assessment and stakeholder interviews with various critical infrastructure operators across telecommunications, water, transport, energy, health, and data centre sectors. The findings reveal significant gaps between theoretical threat potential and current operational reality within Australian contexts.

This research report examined the cybersecurity threats drones pose to Australia critical infrastructure through an extensive literature review, threat assessment and stakeholder interviews with various critical infrastructure operators across telecommunications, water, transport, energy, health, and data centre sectors. The findings reveal significant gaps between theoretical threat potential and current operational reality within Australian contexts.

Stakeholder interviews revealed minimal awareness and formal consideration of drone-enabled cyber threats among critical infrastructure operators. Of eight interviewed organisations, three reported no formal consideration of drones as potential cyber-attack vectors. Those aware of the theoretical threat had not yet translated this awareness into drone-specific operational security measures.

Stakeholders typically categorised drone threats under physical security rather than cyber security domains. Security against drones often focused on preventing unauthorised drone flights or payloads over facilities rather than considering drones as platforms for wireless compromise, GPS spoofing, jamming, or reconnaissance. Several stakeholders expressed confidence that they had security measures in place such as zero trust architecture or air gapped operational networks that would block such cyber attacks, assuming compromise could only occur with on-site access.

The limited awareness within critical infrastructure can be attributed to a few causes:

1. There are currently no recorded incidents in Australia of drones being used as a mechanism for delivering a cyber attack.
2. There is currently very minimal guidance provided in this area by government and regulators.

6.1 NO RECORDED INCIDENTS IN AUSTRALIA

The most striking finding is the lack of documented incidents where drones served as vectors for cyber-attacks against Australian critical infrastructure. None of the operators interviewed had heard of examples of incidents occurring in Australia and none of the literature reviewed documented actual incidents occurring. This contrasts with an international incident documented in the United States - the alleged 2022 Pennsylvania financial services firm attack (Claburn 2022).

The lack of recorded incidents carries multiple implications for Australian cybersecurity posture. First, it suggests current physical and cyber security measures may be adequate to deter opportunistic attacks. Second, the lack of incidents may indicate Australian critical infrastructure presents less attractive targets compared to international counterparts, possibly due to geographic isolation, geo-political environments, scale of economy, or lower threat actor presence. Third, and most concerning, incidents may be occurring but may remain undetected or unreported due to limited monitoring capabilities specific to drone-based vectors.

6.2 MINIMAL GUIDANCE PROVIDED BY GOVERNMENT

Operators that were interviewed indicated that they relied on advice and policy from government and regulators to help shape their physical and cyber security priorities. There is currently a lack of information provided by government to raise the awareness of this threat within critical infrastructure sectors.

6.3 MORE PRACTICAL WAYS TO MOUNT A CYBER-ATTACK WITH THE SAME IMPACT AGAINST CRITICAL INFRASTRUCTURE

Critical infrastructure operators consistently assessed traditional cyber-attack methods as more practical and higher probability than drone-based approaches. Respondents cited factors including lower technical barriers for conventional attacks, established tool availability, reduced physical exposure for attackers, AI enabled attacks, and proven success rates for existing methods.

While this pragmatic assessment reflects current threat landscapes, it may underestimate the unique advantages drones offer for specific attack scenarios. Drones can bypass physical perimeters, position themselves for optimal signal interception or jamming, access air-gapped systems through proximity attacks, and provide persistent reconnaissance capabilities difficult to achieve through traditional methods.

Some operators highlighted the fact that their infrastructure is open to the public or third parties and as such their existing cyber security processes were designed to protect against attacks mounted near their facilities. In these cases, the advantages provided using drones are greatly reduced and an adversary would likely employ technologies that have a much lower barrier to entry or higher chance of success.

6.4 OPERATORS INCREASING USE OF DRONE TECHNOLOGY CREATES NEW CYBER SECURITY THREATS THAT MAY NOT HAVE BEEN CONSIDERED

The use of drones in the management of critical infrastructure has the potential to streamline operations, improve safety and reduce costs. Many operators that participated in interviews expressed a desire to increase their use of drones for these reasons. However, the introduction of this new technology also presents new risks that must be fully considered by critical infrastructure operators as they deploy this technology. Although not a new finding, it is significant enough to highlight in this paper.

There is increasing concern about the origin, manufacturing and supply chain of commercially available drones that might be deployed in the management of critical infrastructure. Australia currently has very limited sovereign capability in the manufacturing of drones leading to a risk of compromised equipment being used due to its advanced capability and broad availability.

The data captured by drones deployed in the management of critical infrastructure presents a strong target for adversaries. If compromised, these drones could provide an adversary with unprecedented reconnaissance on Australian critical infrastructure including technical and physical vulnerabilities. Not only this, if a device is compromised and connected to a network it could be used to mount a cyber-attack in a similar way that an adversary drone could be used for a wireless compromise attack. These risks must be considered by operators as they increase their usage of drones and other unmanned or automated machines.

6.5 LIMITED AWARENESS AND UNDERSTANDING OF SOLUTIONS TO DEFEND CRITICAL INFRASTRUCTURE FROM A DRONE RELATED ATTACK

A consistent observation noted during interviews and identified in literature is the lack of awareness and understanding of solutions or response frameworks available to critical infrastructure operators to respond to the threat presented by drones, in terms of both cyber and kinetic. The challenges experienced by operators in considering strengthening their security against drones include: the number and dispersion of their sites (some operators have thousands of sites spread across Australia), the limited understanding regarding what action can be taken against drones, and the understanding of suitable counter-drone technology that can be operated in domestic environment.

Number and dispersion of sites

While some operators have a small number of sites that can be effectively protected with strong physical security, they could adopt counter drone technologies with relative ease. Other operators have many sites geographically dispersed across the country with little awareness or understanding of effective enterprise-wide counter drone technology being available.

Drones' classification as aircraft

The classification of drones as aircraft was highlighted by many critical infrastructure operators as a concern due to the protections afforded to aircraft by CASA. This classification and protection mean that operators believe they cannot use jamming equipment to protect themselves against an attack from drones.

Availability of counter-drone technology compliant with regulation

Some critical infrastructure operators were aware of drone detection and defeat technologies available to defence and law enforcement however assumed that these technologies could not be used in the context that they operate.

Lack of understanding of current legal options available

Interviews did not raise that drone detection combined with timely security response to locate and neutralise the operator is sufficient to manage the threat. While technologies like radio frequency jamming may not be currently legal to operate in Australia outside of defence and law enforcement use due to radio frequency licensing regulations, a grey zone around drone detection utilisation and broader misunderstanding of what constitutes an effective counter-drone posture may be limiting the uptake of viable, lawful detection solutions.

7. Recommendations

The lack of documented incidents, limited stakeholder awareness, and lack of authoritative guidance create conditions for potential surprise from drone-based cyber-attacks against Australian critical infrastructure. Therefore, the following recommendations are provided to support addressing these vulnerabilities within the critical infrastructure sectors through practical measures that build awareness, establish solutions, integrate drone cyber threats into risk assessment practices, and develop further knowledge and research on the evolving threat.

7.1 INCREASED EDUCATION AND KNOWLEDGE SHARING TO CRITICAL INFRASTRUCTURE OPERATORS

To target the limited awareness and response among critical infrastructure operators, it is essential that further education and knowledge sharing is established. Stakeholder interviews revealed that this topic has not featured in existing resources or knowledge sharing mechanisms such as the Trusted Information Sharing Network (TISN). White papers, round-tables, or conferences should bring light to the cyber security threat posed by drones. Knowledge sharing across critical infrastructure sectors should be encouraged as there was very different consideration given to the topic across sectors but similar challenges in many cases.

7.2 CRITICAL INFRASTRUCTURE OPERATORS SHOULD UNDERTAKE ENHANCED THREAT MODELLING TO INCLUDE THE CYBER SECURITY THREAT POSED BY DRONES

Threat modelling is commonly used in cyber security to consider the types of threats, threat actors and level of threat posed. This method of considering the threat posed by drones should be employed regularly by critical infrastructure operators to strengthen their security posture and respond to the evolving threat that drones pose. Although the risk might be considered low now, the fast-evolving technology and ever-changing threat landscape mean that this needs to be regularly reviewed. The cyber security threat posed by drones could be included in existing threat modelling undertaken by operators or could be considered in a separate exercise. It is our recommendation that for operators with a higher vulnerability to wireless compromise, signal jamming, GPS spoofing or reconnaissance, this threat modelling is done in a separate exercise to ensure that the specific cyber threats from drones are considered in a meaningful way. Operators should also include the use of drones within their operations in their threat modelling; this is explored further in another recommendation below.

7.3 GOVERNMENT, OPERATORS, AND INDUSTRY SHOULD COLLABORATE TO DEVELOP EFFECTIVE MITIGATION STRATEGIES AGAINST DRONE ASSISTED CYBER ATTACKS

Overcoming the challenges faced by critical infrastructure operators in defending against drones requires significant collaboration with government and industry. Technological and policy changes will be required to implement viable solutions to protect Australia's critical infrastructure from the kinetic and cyber threat posed by drones. Collaboration could include the education and knowledge sharing recommended above, developing insights and strategies that inform government and industry solutions. Mitigation strategies might include granting powers for operators to detect and defend critical infrastructure against drones, and implementing no-fly zones and penalties for interfering with airspace around critical infrastructure.

7.4 USE OF DRONE TECHNOLOGIES IN THE OPERATIONS OF CRITICAL INFRASTRUCTURE SHOULD BE REVIEWED TO ENSURE NEW VULNERABILITIES ARE NOT INTRODUCED

As operators incorporate the use of drones in their operations, there is some awareness of the new vulnerabilities that could be introduced. In a similar way that drones could be deployed by a threat actor in an attack against critical infrastructure, the compromise of drones deployed by operators could result in many of the same attack types and impacts. Critical infrastructure operators should review the use of drones in their operations and ensure appropriate cyber security measures are taken to protect their assets and information. This should be a comprehensive review that includes communication protocols, security protocols, manufacturing and supply chain, and sovereign control and capability. The information collected by drones and access they might have to a network could create an attractive target to those wishing to attack Australia's critical infrastructure. The compromise of drone technologies deployed by operators could provide unprecedented access to information and systems of critical infrastructure operators. It is, therefore, essential that operators consider these in their threat modelling.

7.5 GOVERNMENT, OPERATORS AND RESEARCHERS SHOULD COLLABORATE TO FACILITATE A SIMULATION EXERCISE TO GENERATE REAL-WORLD DATA

The facilitation of a simulation exercise to demonstrate the cyber threat that drones pose would offer significant learnings for government, operators, industry, and researchers to support the development of effective risk mitigation strategies. Due to the lack of recorded incidents, a simulation exercise could be used to collect real world data and demonstrate the threat in a practical way. This is an excellent opportunity for researchers to work with operators to setup a realistic exercise that considers current technologies and capabilities of both drones and operators. The outcomes of this exercise would be rich findings and recommendations that support the development of mitigation strategies. They could lead to further research, development of new technologies and solutions, evolution of policy, and greater consideration given in threat modelling.

7.6 FUTURE RESEARCH SHOULD BE CONDUCTED INTO THE USE OF DRONES IN A CYBER ATTACK

This project has considered the current awareness of critical infrastructure operators and the current literature available about the cyber security threat that drones pose. Due to the fast-evolving nature of this technology, and the growing availability and accessibility of drones, the threat posed will need to be regularly reviewed. This project could be considered a baseline for future work to be undertaken to track the evolution of this threat as both threat actors and the available technologies change. Research should be conducted that considers the level of threat posed including the threat actors that might deploy drone technology to mount a cyber-attack. Taking a practical approach to future research could be beneficial in demonstrating the threat to all stakeholders and assisting with the development of effective mitigation strategies.

8. Conclusion

The cyber security threat that drones pose to critical infrastructure is an emerging threat in Australia. Our research considered this problem through a structured literature review and stakeholder interviews with eight critical infrastructure operators, representing six of the eleven critical infrastructure sectors in Australia. The literature review provided strong contextual information building a solid foundation for interviews and findings that are grounded in theoretical knowledge. Critical infrastructure operators interviewed for the research provided rich insights and responses that have ensured findings and recommendations that are practical and focused on protecting Australia's critical infrastructure.

Our key findings are:

- Operators have limited awareness of the threat due to a lack of recorded threats in Australia and limited government advice.
- The increasing use of drones in operations introduces new cyber security concerns for operators.
- There is limited awareness and understanding of the solutions available to protect Australia's critical infrastructure from cyber or kinetic drone attacks.

These findings highlight the need for further action across government, operators, researchers, and industry to ensure the security of critical infrastructure in Australia. Six recommendations have been made as to how this can be achieved. They include: increase the knowledge sharing about this topic, enhance threat modelling practices, collaborate to create viable solutions, critically review use of drones in operations, undertake simulation exercises, and conduct further research.

Drone technology and availability is growing rapidly and the threat posed to Australia's critical infrastructure through both cyber and kinetic attacks will continue to evolve. The research established here is just the beginning and must be built upon, using this as a baseline for considering that evolution of the threat.

References

Best KL, Schmid J, Tierney S, Awan J, Beyene NM, Holliday MA, Khan R and Lee K (2020) How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools, https://apps.dtic.mil/sti/html/trecms/AD1095539/.

Civil Aviation Safety Authority (2021) Part 101 of CASR Unmanned aircraft and rockets, Civil Aviation Safety Authority, https://www.casa.gov.au/rules/regulatory-framework/casr/part-101-casr-unmanned-aircraft-and-rockets#Rulestatus, accessed 20 July 2025.

Claburn T (2022) How Wi-Fi spy drones snooped on financial firm, Theregister.com, https://www.theregister.com/2022/10/12/drone-roof-attack/, accessed 20 July 2025.

Critical Infrastructure Security Centre (2018) Cyber and Infrastructure Security Centre Website, Cyber and Infrastructure Security Centre Website, https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018, accessed 18 July 2025.

Cyber and Infrastructure Security Centre (2023) Critical Infrastructure Resilience Strategy, https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf, accessed 18 July 2025.

Cyber and Infrastructure Security Centre (2024) Factsheet for Critical Infrastructure: Positioning, Navigation and Timing, https://www.cisc.gov.au/resources-subsite/Documents/pnt-factsheet.pdf, accessed 1 August 2025.

Deloitte Access Economics (2020) Economic benefit analysis of drones in Australia, Deloitte, https://www.deloitte.com/au/en/Industries/government-public/analysis/economic-benefit-analysis-drones-australia.html, accessed 29 July 2025.

Gillis AS, Lutkevich B and Earls AR (2024) What Is a Drone (UAV)?, TechTarget, https://www.techtarget.com/iotagenda/definition/drone, accessed 12 July 2025.

Kidd C (2025) What's The CIA Triad? Confidentiality, Integrity, & Availability, Explained | Splunk, Splunk, https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html, accessed 20 July 2025.

Kootala, Mousa A and Philip (2023) 'Drones are Endangering Energy Critical Infrastructure, and How We Can Deal with This', Energies, 16(14):5521–5521, doi:https://doi.org/10.3390/en16145521.

Labib NS, Brust MR, Danoy G and Bouvry P (2021) 'The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles', IEEE Access, 9:115466–115487, doi:https://doi.org/10.1109/access.2021.3104963.

Lyngaas S (2021) Drone at Pennsylvania electric substation was first to 'specifically target energy infrastructure,' according to federal law enforcement bulletin, CNN, https://edition.cnn.com/2021/11/04/politics/drone-pennsylvania-electric-substation, accessed 1 August 2025.

NIST (2015) Cybersecurity - Glossary | CSRC, Nist.gov, https://csrc.nist.gov/glossary/term/cybersecurity, accessed 15 July 2025.

NIST (2020) NIST SP 1800-26A - Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events, Nist.gov, https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html, accessed 9 July 2025.

Omni and Cyber Security Cooperative Research Centre (2024) Flight Critical: Drones, Cyber Security and Crtiical Infrastrcture, https://cybersecuritycrc.org.au/remote-assets/sites/default/files/2024-05/Flight%20Critical.pdf, accessed 20 May 2025.

Ray R (2024) The Rise of Hacker Drones, Drone Vortex, https://thedronevortex.com/the-rise-of-hacker-drones/, accessed 24 July 2025.

Schneider M, Lichte D, Witte D, Gimbel S and Brucherseifer E (2021) 'Scenario Analysis of Threats Posed to Critical Infrastructure by Civilian Drones', European Safety and Reliability Conference, 31, doi:https://doi.org/10.3850/978-981-18-2016-8.

SentinelOne (2025) What is Cyber Reconnaissance?, SentinelOne, https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-cyber-reconnaissance/, accessed 3 August 2025.

The MITRE Corporation (2025) MITRE ATT&CK®, Mitre.org, https://attack.mitre.org/, accessed 8 July 2025.

Van J (2025) Eyes over the paddock: farm monitoring with Chinese drones is a national security risk | The Strategist, The Strategist, https://www.aspistrategist.org.au/eyes-over-the-paddock-farm-monitoring-with-chinese-drones-is-a-national-security-risk/, accessed 5 August 2025.

Appendix

Questions posed to critical infrastructure interviewees

Question
Have you considered the threat that drones pose to your critical infrastructure?
Have you considered the **cyber security** threat that drones pose within the broader threat? How familiar are you or your organisation with the potential for drones to be used as cyber-attack platforms rather than just physical or kinetic threats?
In your assessment of this risk, what makes your infrastructure attractive to attackers using drones? In your assessment (if any), what makes your infrastructure attractive to attackers using drone-delivered cyber-attacks? What advantages would drones have over more traditional attacks?
What level of risk do you think drones pose to cyber security of critical infrastructure? (Low, medium, high?) How did you come to this assessment?
What would be the potential impact if a drone successfully compromised your infrastructure?
In your opinion, how aware of this threat do you think other organisations in your sector are?
How do you think the sector or regulators should respond to this threat?
Have you experienced any suspicious drone activity around your facilities? How has your security posture evolved based on actual or potential drone threats?
What mechanisms do you have in place to detect drone related threats? (Especially those related to cyber security)
How confident are you in your organisation's ability to detect a drone-enabled cyber-attack?
In your experience how mature are CI operators in their approach to cyber security? Do you think CI operators give similar weighting to cyber security and physical security?
How does your organisation learn and respond to emerging cyber security threats? And how much of a priority is this?
Do you have operational technology or industrial control systems in your organisation? What sorts of OT/ICS do you have? Have you taken steps to ensure the cyber security of this technology? Is your OT and IT interconnected?

INNOVATION CENTRAL CANBERRA

a collaboration led by Cisco with University of Canberra, part of the
National Industry Innovation Network

ADELAIDE

Flinders University · Adelaide University

- Innovation Central Adelaide
- Digital Health Research Chair
- Cisco-Flinders Digital Health Design Lab
- Networking Academy

CANBERRA

University of Canberra

- Innovation Central Canberra
- Critical Infrastructure Research Chair
- Networking Academy

BRISBANE

QUT · The University of Queensland

- Innovation Central Brisbane
- Sport Research Chair
- Securing Future Networks Chair
- UQ Centre for Future Networks

SYDNEY

UTS

- Innovation Central Sydney
- Renewable Technology and Sustainability Chair
- Networking Academy

PERTH

Curtin University

- Innovation Central Perth
- Networking Academy

MELBOURNE

RMIT · La Trobe University

- Innovation Central Melbourne
- IoT & AI Research Chair
- Centre for AI and IoT
- Cisco-RMIT Health Transformation Lab
- Networking Academy

innovationcentral@canberra.edu.au
icentralau.com.au/canberra/

Innovation Central Canberra

A collaboration led by cisco

FOUNDATION PARTNERS

cisco | UNIVERSITY OF CANBERRA

icentralau.com.au/canberra/

Email
innovationcentral@canberra.edu.au

Address
Innovation Central Canberra
Level 1, Building 27
University Of Canberra
BRUCE ACT 2617

PART OF THE NIIN National Industry Innovation Network