UNIVERSITY OF CANBERRA

ON THE THREAT OF AERIAL DRONES TO THE CYBER SECURITY OF AUSTRALIAN CRITICAL INFRASTRUCTURE

RESPONSE TO THE AUSTRALIAN GOVERNMENT'S "DRONES SECURITY PUBLIC CONSULTATION PAPER" (APRIL 2026)

Author: Prof Frank den Hartog (University of Canberra)

Date: 24 May 2026

Abstract: This document is a submission for the Australian Government's Public Consultation regarding the "Drones Security Public Consultation Paper" from April 2026. It answers various questions stated in that paper, drawing from our research as described in the white paper "Drone-Related Cybersecurity Threats to Australia's Critical Infrastructure" that was published by the National Industry Innovation Network (NIIN) in November 2025.

TABLE OF CONTENTS

INTRODUCTION

This document is a submission for the Australian Government's Public Consultation regarding the "Drones Security Public Consultation Paper" from April 2026 [1]. It answers various questions stated in that paper, drawing from our research as described in the white paper "Drone-Related Cybersecurity Threats to Australia's Critical Infrastructure" that was published by the National Industry Innovation Network (NIIN) in November 2025 [2].

The research was commissioned by DroneShield (ASX:DRO) and carried out by the University of Canberra. The scope of the research was limited to the **threat of aerial drones to the cyber security of Australian critical infrastructure.** The main research question was whether such threats are practical, and whether limited deployment of drone detection capabilities across our critical infrastructure may be obscuring an understanding of the threat landscape.

For the definition of critical infrastructure, we have adopted the one provided by the Critical Infrastructure Security Centre in 2023: 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 and economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security [3]. Cyber security is defined as the protection of digital systems, networks, data, and devices from unauthorised access, disruption, or destruction.

The remainder of this submission is laid out as follows. In the next section we provide the executive summary of [2] verbatim. The subset of questions provided in [1] that directly relates to our research is then answered in subsequent sections, followed by a brief conclusion.

EXECUTIVE SUMMARY OF "DRONE-RELATED CYBERSECURITY THREATS TO AUSTRALIA'S CRITICAL INFRASTRUCTURE"

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 [4]: 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 cyber security 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.

ANSWERS TO SELECTED QUESTIONS IN "DRONES SECURITY PUBLIC CONSULTATION PAPER"

Proactive management of growing drone threats

As our research was limited to the threat of aerial drones to the cyber security of Australian critical infrastructure, we did not study threats such as the ones that under-water drones could pose to our continental and intercontinental data communication networks. In this submission, we, therefore, do not attempt to answer questions about mode-agnostic or all-modes approaches.

Strengthened counter-drone capabilities to protect the community and infrastructure

What safeguards or oversight do you think are important to ensure counter-drone technologies are used safely, proportionately, and appropriately?

Currently drones are legally classified as aircraft under Civil Aviation Safety Authority (CASA) regulations, and interfering with them is generally restricted. This creates strict limits on the use of counter-drone measures (e.g., jamming), which are typically only permitted for authorised entities such as law enforcement. There was a general understanding among our interviewees, though, that drones may provide a more imminent threat to the cyber security of our critical infrastructure than regular aircraft. Clearer legal frameworks and guidance are, therefore, needed about what counter-drone actions are permissible and how. This may include policy changes, operational guidance, and coordinated approaches to defence.

The report does not specify in detail which safeguards or oversight are important to ensure counter-drone technologies are used safely, proportionately, and appropriately, but it suggests that counter-drone technologies should be governed by:

- Clear legal and regulatory constraints
- Defined authority and limited use of disruptive measures
- Government-led guidance and oversight
- Collaboration across stakeholders
- Proportionate tools such as detection, no-fly zones, and enforcement
- Improved clarity on lawful use to avoid misuse or inaction

Who should be authorised (with appropriate training and approvals) to deploy drone detection or counter-drone technologies?

Our research did not explicitly answer this question. Law enforcement and defence are the clearly authorised and trained actors today, and critical infrastructure operators are not authorised (or are uncertain about being authorised) to deploy active counter-drone technologies. The report suggests that authorisation could be extended to operators, but it would need to be done through policy and regulatory changes.

What role should industry and the public play in reporting or helping to identify emerging drone threats?

Currently, industry and the public play an underdeveloped role in identifying and reporting emerging drone threats. Our research makes clear that formal detection reporting guidelines are limited. 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. On which, so some interviewees pointed out, there was no consistent follow up, as such reducing deterrence.

This implies that both industry staff and the public act as the first line of detection, particularly in the absence of widespread technical drone detection and counter-drone systems. Therefore, as there are no recorded drone-enabled cyber incidents in Australia, this may be more a reflection of our limited monitoring capabilities than of those incidents actually not happening whilst being undetected or unreported, in particular because there has been an incident reported in 2022 in the United States: a drone was able to intrude into a Wi-Fi network of financial firm [5].

This directly suggests that better reporting by industry personnel and the public is essential to surface otherwise invisible or ambiguous drone activity, build an evidence base of incidents and near-misses, and reduce “blind spots” in national threat awareness. This, consequently, requires better education and knowledge sharing across sectors, for instance by making greater use of information-sharing mechanisms (e.g., the Trusted Information Sharing Networks (TISN)).

In this context, industry actors (and indirectly the public via designated reporting channels) should be able to feed observed drone incidents into shared reporting frameworks, contribute to collective situational awareness across sectors, and help identify patterns (e.g., repeated reconnaissance flights, unusual behaviour). This would greatly help with building a body of real-world data that can be used for further research and simulations for the sake of identifying new tactics (e.g., reconnaissance, spoofing, wireless attacks delivered by drones) and to enable faster recognition of evolving threat patterns.

Enhanced identification and tracking through electronic conspicuity

Should drone detection equipment only be available to law enforcement and security agencies only, or extended to new user groups such as emergency services, prison operators, critical infrastructure operators and event organisers?

Our research indicated that the current (real or perceived) restriction to law enforcement/defence is insufficient, and that additional user groups, particularly critical infrastructure operators as defined by the Security of Critical Infrastructure Act 2018 [4] should be empowered to operate advanced technical drone

detection equipment. This expansion must occur within a regulated, collaborative, and legally defined framework.

Balanced enforcement that deters misuse, and enables innovation

What reporting obligations should apply when abnormal or unauthorised drone activity is detected (e.g., mandatory incident reporting by infrastructure operators), and how should information be shared with authorities?

Our research provided evidence that reporting is currently informal (to police/authorities), inconsistent and limited. We recognised that under-reporting and lack of monitoring are key problems and that existing information-sharing systems do not adequately cover drone threats. The report does not define what reporting obligations or structured information-sharing frameworks should be put in place. However, we do recommend that industry actors feed observed drone incidents into shared reporting frameworks, contribute to collective situational awareness across sectors, and help identify patterns. This would greatly help with building a body of real-world data that can be used for further research and simulations for the sake of identifying new tactics and to enable faster recognition of evolving threat patterns. How much and in what way this should be mandated should be a matter of public-private consensus building.

Drone classifications and operating restrictions

Should specific no-use or enhanced-monitoring zones be designated around certain assets (e.g., hospitals, correctional and energy facilities)?

Our research clearly supports the creation of no-use (no-fly) zones around critical infrastructure assets, backed by enforcement and penalties. However, it only addresses this at a high level and does not provide a detailed framework for which specific assets require no-fly zones, or how enhanced-monitoring vs full restriction should be balanced.

Build public and industry awareness

What information would help the public better understand risks associated with drones across land, air, and maritime domains?

We believe that the public would benefit from information explaining that drones can conduct cyber reconnaissance, enable wireless intrusion, and perform GPS spoofing or jamming. And not just cause physical damage. Drones can do this because the can bypass many physical perimeters and provide proximity-based access to networks and systems. The incident reported in 2022 in the United States (a drone was able to intrude into a Wi-Fi network of financial firm [5]) should get more attention as a real-world example. The public should understand why certain locations (e.g. substations, hospitals, data centres) are sensitive to cyber drone attacks, and why drone activity near these sites may be suspicious or risky.

The white paper does not specify public-facing communication strategies, or formal guidance on how the public should respond. For instance, our research found that critical infrastructure operators use their own drones for remote inspections and maintenance. The public should, somehow, learn that this is not suspicious, to avoid over-reporting.

CONCLUSION

Our research as described in the 2025 white paper “Drone-Related Cybersecurity Threats to Australia’s Critical Infrastructure” enabled us to answer various questions stated in the Australian Government’s “Drones Security Public Consultation Paper” from April 2026. However, also many questions could not (or only partially) be answered. We believe this is not because the scope of our research was limited to the threat of aerial drones to the cyber security of Australian critical infrastructure: most of the questions were still relevant for this subset of use cases. Instead, we believe that there is simply not enough data available yet to answer those questions in a scientifically responsible way. We, therefore, **strongly** recommend that government, operators and researchers first collaborate to generate real-world data by means of a sustained program of research. This would establish a stronger **evidence base** on which future government policies could be based.

We would also like to highlight two further recommendations that are mentioned in the 2025 white paper but which we believe the “Drones Security Public Consultation Paper” has not asked for:

- Threat modelling undertaken by critical infrastructure operators should explicitly incorporate drones as potential vectors, moving beyond traditional assumptions of kinetic drone attacks. This could find a place in future government cyber security guidelines.
- Critical infrastructure 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. Drones Security comprises security against drones as well as security of drones.

REFERENCES

[1] Australian Government, *Drones Security: Public Consultation Paper*, April 2026, https://www.homeaffairs.gov.au/forms-subsite/files/drone-security-consultation-paper-2026.pdf

[2] Simone Chitsinde, Andrew Giumelli, Frank den Hartog, *Drone-related cybersecurity threats to Australia's critical infrastructure*, White Paper, Innovation Central Canberra, NIIN, November 2025, https://icentralau.com.au/canberra/drone-enabled-cybersecurity-threats-to-australias-critical-infrastructure/

[3] Cyber and Infrastructure Security Centre, *Critical Infrastructure Resilience Strategy*, February 2023, https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf

[4] Australian Government, *Security of Critical Infrastructure Act 2018*, Federal Register of Legislation, April 2005, https://www.legislation.gov.au/C2018A00029/latest/text

[5] Thomas Claburn, *How Wi-Fi spy drones snooped on financial firm*, The Register, October 2022, https://www.theregister.com/security/2022/10/12/wi-fi-spy-drones-used-to-snoop-on-financial-firm/561837