Distance Is Not a Defence

Australia’s Vulnerability to Small Drones

A white paper for industry leaders, critical infrastructure operators and government stakeholders

September 2026 | Version 8 — Draft

Title	Distance Is Not a Defence – Australia’s Vulnerability to Small Drones
Version	8
Status	Draft
Date	September 2026
Source basis	Open-source research
Prepared by	Shelby Glaskin

At a glance

Six findings run through this paper.

1. For most Australian civilian operators, the near-term constraint is lawful authority, not technology.

Jamming equipment is subject to a permanent ban, and the exemption pathway is not available to private operators. Active electronic and kinetic defeat are therefore not generally available to a critical infrastructure operator without specific authority.

2. The threat is already present in the Australian record.

In July 2026 Defence confirmed multiple uncrewed aircraft over RAAF Base Williamtown and referred the matter to police, and has not disclosed whether any was intercepted or identified. Drone-delivered contraband is routine in Australian prisons, and drones have repeatedly grounded aerial firefighting.

3. Ambiguity produces operational and economic consequences without a proven attack.

Gatwick lost around 30 hours and roughly £50 million with no drone recovered, no photograph produced and no corroborating sensor return. Two later waves of sightings closed airports and moved military assets without an operator being publicly identified in either.

4. Geographic distance offers less protection here than against the threats Australian planning is built around.

The point of employment needs to be near the target, not near the sponsor. Remoteness, protective against conventional threats, works in the opposite direction: fewer people are present to notice.

5. Detection is the investment that is both lawful and useful today.

It is also, on the evidence available, the one least often made outside Defence and the major airports — an assessment rather than a measurement, since no Australian deployment survey has been published. Separately, and internationally, over half the commercial counter-drone market sells single-sensor systems. Detection is not unconditional either: radar generally requires a transmitter licence, and sensor deployment engages privacy obligations.

6. A posture set today is likely to be materially out of date within one to two years.

Jamming was largely defeated by fibre-optic control inside a year. Fibre-optic control was answered by high-power microwave within roughly another. Neither regulation nor procurement has kept pace.

What this paper is, and is not

It is a strategic assessment. It identifies the threat, explains its Australian implications and sets out governance and protection principles.

It is not a site-specific vulnerability assessment, a threat intelligence product, a procurement specification, legal advice, an operational counter-drone manual, or a forecast of a specific attack on Australian soil.

Recommendations at a glance

Set out in full at section 15.2 (industry) and section 15.3 (government), where each government recommendation also identifies an owner and the obstacle. The government recommendations are sequenced in section 15.3 and are not given a time horizon here.

Recommendation	Audience	Time horizon
Assign named executive ownership	Industry	Immediate (0–90 days)
Establish and test police, ADF and CASA notification pathways	Industry	Immediate (0–90 days)
Start a pattern-of-activity register	Industry	Immediate (0–90 days)
Build a behaviour-based escalation matrix that does not depend on attribution	Industry	Immediate (0–90 days)
Draft the communications position in advance	Industry	Immediate (0–90 days)
Commission a site-specific vulnerability assessment inside SOCI obligations	Industry	Near term (3–12 months)
Specify and procure detection against outcomes, not products	Industry	Near term (3–12 months)
Exercise the decision, not the equipment	Industry	Near term (3–12 months)
Model a pure-disruption continuity scenario	Industry	Near term (3–12 months)
Put four questions to your insurance broker	Industry	Near term (3–12 months)
Design protection into capital works	Industry	Medium term (1–3 years)
Bring your own fleet and supply chain inside the risk framework	Industry	Medium term (1–3 years)
Build a technology refresh assumption into budgeting	Industry	Medium term (1–3 years)
Engage the regulatory reform process while it is open	Industry	Medium term (1–3 years)
Reform the counter-drone exemption pathway so that eligibility turns on asset criticality, not profession	Government	—
Extend the regulatory momentum from Defence to the civilian side	Government	—
Make uncrewed traffic management data usable for security, not only for safety	Government	—
Harmonise state and territory law where it intersects with drone operation	Government	—
Address drone cyber security and data standards	Government	—
Set expectations for Remote ID honestly	Government	—

Contents

Executive Summary

For most of the last century, air power belonged to states. That is no longer the case. Persistent aerial surveillance and the ability to place an explosive charge precisely on a target used to require an air force, and an air force required airfields, trained pilots, a maintenance chain and a significant national budget. Both capabilities can now be bought, assembled and flown by individuals with a few thousand dollars and an internet connection. This paper examines what that shift means for Australian industry, critical infrastructure, and government, and sets out a practical framework for responding to it within the law as it currently stands.

The evidence base is no longer speculative, and the incidents that matter most involve the cheapest aircraft. On the 1st of June 2025, Ukraine's Security Service launched over 100 first-person-view drones from concealed compartments in cargo trucks parked near Russian air bases, striking more than a dozen strategic bombers and airborne early-warning aircraft at four locations, one of them more than four thousand kilometres from Ukrainian territory.[1] On the 7th of October 2023, small commercial quadcopters were flown ahead of a ground assault to drop munitions on the generators powering communications towers, and on the remotely operated weapon stations, along one of the most heavily monitored borders in the world, leaving the soldiers watching it without signal or alarms in the minutes before fighters breached the barrier.[2] And in December 2018, without a single drone ever being recovered, photographed, or corroborated by any pilot report or by the counter-drone equipment eventually deployed, reported sightings closed London Gatwick Airport across three days of the busiest travel week of the year, affecting around 140,000 passengers and roughly a thousand flights, resulting in over £50 million in losses.[3] [4]

On the industrial side, in September 2019, a coordinated salvo the Saudi Defence Ministry put at eighteen drones and seven missiles (aircraft well beyond the class this paper addresses[5]) struck two Saudi oil processing facilities, temporarily disrupting 5.7 million barrels a day of production, over half of Saudi Arabia's output and roughly five percent of global supply.[6] [7] It is included not as a threat model for Australia but because it is the only case on record in which the target was concentrated industrial processing plant, which is a category Australia has a great deal of.

Those are the incidents that make headlines. The pattern that should concern Australian readers more is the quieter one that emerged across 2024, 2025 and 2026 in countries that were not at war. Between mid-November and late December 2024, hundreds of drone reports

[1] Center for Strategic and International Studies, "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare," 2025.

[2] Middle East Institute, "The October 7 Hamas attack: An Israeli overreliance on technology?"

[3] Airprox Reality Check, "Gatwick 2018," a documentary review assembled from UK Airprox Board records, National Police Air Service flight records, Ministry of Defence and Sussex Police freedom-of-information responses, and Civil Aviation Authority and Department for Transport correspondence.

[4] *Fortune*, "Gatwick's December Drone Closure Cost Airlines $64.5 Million," 22 January 2019, recording around £50 million in airline costs, easyJet's £15 million, more than 1,000 cancellations, approximately 140,000 passengers affected and a 33-hour closure.

[5] *Arab News*, "Saudi Arabia's Defense Ministry displays Iranian drones, cruise missiles used in Aramco attacks," reporting Col. Turki Al-Maliki's press conference account of eighteen drones and three cruise missiles against Abqaiq and four missiles against Khurais.

[6] Congressional Research Service, "Attacks on Saudi Oil Facilities: Effects and Responses," In Focus IN11173, 2019.

[7] Arab News, *Saudi Arabia's Defense Ministry displays Iranian…*, see reference 14.

across the northeastern United States, concentrated around military installations in New Jersey, produced weeks of public alarm, congressional pressure and shifting official explanations before investigators concluded they had found nothing anomalous.[8] The commander of NORAD subsequently disclosed that United States military installations had recorded 350 drone detections across 100 sites during 2024 alone.[9] From September 2025, a wave of drone sightings closed airports and overflew military bases and nuclear facilities across Denmark, Norway, Germany, Belgium, the Netherlands and France, prompting the Danish Prime Minister to describe it as the most serious attack on Danish critical infrastructure to date, and prompting the deployment of allied counter-drone teams into Belgium.[10] [11] In none of those cases was an operator identified.

Australia has its own version of this record, and it is further developed than many Australian executives realise. Between 11-13th of July 2026, the Department of Defence confirmed multiple uncrewed aircraft in restricted airspace over RAAF Base Williamtown, home to Australia's F-35A and E-7A Wedgetail fleets, and referred the incidents to the New South Wales Police Counter-UAS Unit.[12] Defence has not disclosed whether the aircraft were intercepted, identified or recovered. Defence Minister Pat Conroy confirmed the incident publicly a month later, noting both the $7 billion counter-drone investment and the 2025 regulations permitting Defence to seize, disable or destroy a drone, neither of which was brought to bear at Williamtown.[13] Drone-delivered contraband is now routine in Australian prisons: Victoria recorded 97 drone-related security incidents in roughly eight months of 2020, a 246% increase,[14] four Queensland high-security prisons were locked down simultaneously after drones overflew all of them on a single afternoon,[15] and in May 2026 a single drone intercepted at the Townsville Correctional Complex was carrying an estimated one million dollars in contraband.[16] Drones have repeatedly grounded aerial firefighting operations in Australia, most recently at the Manypeaks fire in Western Australia in January 2025, where the state's aviation superintendent likened the effect to taking fire trucks off the ground.[17] In May 2026, eighty-nine of a thousand drones in a professionally operated display at Vivid Sydney fell into

[8] Department of Homeland Security, Federal Bureau of Investigation, Federal Aviation Administration and Department of Defense, "Joint Statement on Ongoing Response to Reported Drone Sightings," 16 December 2024.

[9] United States Senate Committee on Armed Services, *Stenographic Transcript: Hearing to Receive Testimony on the Posture of United States Northern Command and United States Southern Command*, 13 February 2025, recording General Gregory Guillot's evidence on 350 drone detections across 100 military installations in 2024 and his request for authority extending beyond the installation boundary.

[10] CNN, "Denmark links drones at Copenhagen airport to hybrid attacks across Europe," 23 September 2025, reporting the Copenhagen and Oslo closures, Prime Minister Mette Frederiksen's statement and the Danish police assessment.

[11] Arms Control Association, *Arms Control Today*, "Drone Incursions in Belgium Spark Probes, NATO-EU Response," December 2025.

[12] *Newcastle Herald*, "RAAF Williamtown: drones reportedly breached restricted airspace," 10 August 2026, carrying the Department of Defence statement on uncrewed aircraft near Newcastle Airport and RAAF Base Williamtown between 11 and 13 July 2026, the referral to the New South Wales Police Counter-UAS Unit, and Defence Minister Pat Conroy's refusal to detail the response.

[13] Australian Aviation, "Australia must learn from Williamtown drone incident, experts say," 11 August 2026, reporting Defence Minister Pat Conroy's confirmation of the incident on ABC Newcastle on 10 August 2026 and expert commentary from Dr Oleksandra Molloy, Robert Potter and Jennifer Parker.

[14] Australian Aviation, "Drone incidents at Victorian prisons rise 250%," November 2020, reporting freedom-of-information data obtained by *The Age*.

[15] Queensland Corrective Services, undated statement, "High security prisons locked down after drone incursion."

[16] ABC News, "Drone with $1 million worth of contraband intercepted at Townsville prison," 28 May 2026.

[17] ABC News, "Anger after drones ground water bombers at Manypeaks bushfire in WA," 15 January 2025.

Cockle Bay and onto public boardwalks after what the operator attributed to radio interference.[18]

Six findings run through this paper. Each is developed and evidenced in the parts that follow.

For most Australian civilian operators, the principal near-term constraint is lawful authority and governance, not the availability of technology. Under the *Radiocommunications Act 1992* (Cth), drone jammers are subject to a permanent ban, with penalties of up to $330,000 and two years' imprisonment for possession, supply or operation, rising to $1.65 million and five years where significant interference results.[19] Exemptions under section 27 are available only to a narrow range of defence, national security, law enforcement and emergency services roles; the instrument that lets Australian police use counter-drone equipment is the *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022*.[20] For most critical infrastructure operators, active electronic and kinetic defeat options are therefore not generally available. Lawful responses centre on detection, identification, passive protection, investigation and notification: a narrower set than international counter-drone doctrine assumes.

The threat is already present in the Australian record. The aforementioned figures are not projections. They describe drone activity over Australian defence establishments, prisons, fire grounds and public events that has already occurred, in most cases without the operator being identified, regardless of any hostile intent or physical damage.

Ambiguity produces operational and economic consequences without a proven attack. Gatwick lost around 30 hours and roughly £50 million with no drone recovered, no photograph produced, no pilot airprox report filed, and no corroboration from the counter-drone equipment eventually deployed. Two subsequent waves of sightings, one American and one European, closed airports, raised national alert postures and moved military assets without an operator being publicly identified in either. This is the scenario most Australian organisations are likely to face, and it is not addressed by hardening a target.

Geographic distance offers less protection against this threat than against those Australian planning is built around. The point of employment needs to be near the target, not near the sponsor. Remoteness, which is protective against conventional threats, works in the opposite direction here, because fewer people are present to notice.

Detection is the investment that is both lawful and useful today. It is also, on the evidence available, the one least often made outside Defence and the major airports. Airservices Australia has been building a drone surveillance network covering 29 controlled airports,[21] and Defence has committed up to $7 billion over a decade to counter-drone capability within a $22

---

[18] ABC News, "Why drones fell from the sky during Sydney's Vivid light show," 27 May 2026; and "Vivid Sydney drone shows cancelled for now after malfunction saw 89 drones fall into the harbour," 26 May 2026.

[19] Australian Communications and Media Authority, "Jammers are illegal in Australia," setting out the permanent ban under subsection 172(3) of the *Radiocommunications Act 1992* and the applicable penalties.

[20] Australian Communications and Media Authority, "Exemptions for banned equipment," describing the section 27 exemption pathway and current determinations including the *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022*.

[21] Unmanned Airspace, "Airservices Australia publishes tender for drone surveillance network covering 29 airports," 22 September 2023, reporting the Airservices approach to market and quoting the *Australian Aviation Network Overview* on detections in airport no-fly zones.

billion drone and autonomous systems envelope in the 2026 Integrated Investment Program.[22] Outside those two programs, most Australian facilities would learn of a drone over their site from a phone call, not from a sensor. That is an assessment, not a measurement: no Australian survey of counter-drone deployment has been published, which is itself part of the problem. Detection nonetheless comes with conditions: radar generally requires an ACMA transmitter licence, and sensor deployment engages privacy obligations discussed at section 13.6.

The threat changes faster than any single technology or regulation can hold. Jamming was the default response until fibre-optic-controlled drones, first fielded at scale by Russian forces around August 2024 and matched by Ukraine within a year, removed the radio link there was to jam; those drones now operate at ranges of thirty to forty kilometres.[23] High-power microwave systems, which attack a drone's electronics rather than its control link, were demonstrated against a fibre-optic-controlled drone in December 2025, under eighteen months later.[24] A security posture set today and not revisited is likely to be materially out of date within one to two years.

The paper is organised in six parts. Part I traces the technology and why it matters. Part II profiles the actors using it and reviews the international record, including the three peacetime cases (Gatwick, the 2025 European wave and the 2024 United States sightings) that bear most directly on Australian conditions. Part III applies that record to Australia, concentrating on the defence estate, aviation, ports, energy, prisons and public events. Part IV sets out what detection and response technologies can and cannot do, with the trade-offs stated explicitly. Part V covers the Australian regulatory environment and what boards are already obliged to do. Part VI sets out recommendations for industry and for government.

[22] The Hon Pat Conroy MP, Minister for Defence Industry, "Albanese Government to invest up to $7 billion in counter drone defence," 21 April 2026.

[23] Atlantic Council, "Fiber-optic drones have emerged as critical kit for both Russia and Ukraine," UkraineAlert.

[24] Epirus, "Epirus' Leonidas Demonstrates Successful Use of High-Power Microwave to Defeat Fiber-Optic Controlled UAS," describing a December 2025 demonstration.

Part I — Strategic Context

1. Introduction

The past decade has seen a proliferation of small uncrewed aircraft that has altered the security environment for military, government and critical infrastructure organisations worldwide. Advances in commercial technology have lowered the barrier to acquiring capable aerial platforms that were once limited to well-funded militaries, and there is no indication that this trend will slow. Small drones typically costing less than a laptop have been used to damage strategic bomber fleets, blind border surveillance systems, close major airports and deliver drugs into prisons. What was, a decade ago, a concern for military planners is now a live risk for anyone responsible for a large public event, a correctional facility, a port, or a piece of national infrastructure.

1.1 Purpose of this white paper

This paper is intended to build awareness of the risk small drones pose to Australia. Its purpose is to give stakeholders across industry, critical infrastructure, government and defence a broad understanding of the drone threat: where it came from, how drones have been used to date, what this means for Australia specifically, and what a lawful response to a drone incursion actually looks like in this jurisdiction.

There is no assumption that the reader is knowledgeable about, or experienced with, drone-based threats, and by design the paper does not require it. It assumes only that the reader is, in some capacity, responsible for the security or resilience of an organisation or asset(s) that could plausibly be affected.

A note on what this paper is not. It is not a procurement guide, and it does not recommend particular products. Where specific systems are named, they are named because they illustrate a capability or a limitation that is publicly documented, not because they are endorsed. Nor is it an operational manual: where a technique could plausibly assist a malicious actor if described in detail, the discussion stays at the level of policy and principle.

1.2 Intended audience

This paper is written primarily for three groups.

The first is executives and boards of organisations that own or operate critical infrastructure as defined under the *Security of Critical Infrastructure Act 2018* (Cth), which now covers eleven sectors and twenty-two asset classes[25] spanning energy, communications, data storage and processing, financial services and markets, water and sewerage, health care and medical,

[25] Australian National Audit Office, *Administration of Critical Infrastructure Protection Policy*, recording that amendments to the *Security of Critical Infrastructure Act 2018* expanded the asset classes covered from four to twenty-two across eleven sectors.

higher education and research, food and grocery, transport, space technology, and defence industry.[26]

The second is government and defence stakeholders with a policy, regulatory or operational interest in how Australia manages this threat.

The third is the security consultancies, technology vendors and insurers who advise, supply and underwrite the organisations in the first two groups.

Readers need no counter-drone expertise. They are assumed to be familiar with enterprise risk, governance and security planning concepts, because the paper frames the drone threat in those terms and not as a purely technical or military problem.

1.3 Scope

The word "drone" is used loosely enough in public discussion to describe almost anything that flies without a pilot on board, from a $50 toy to a military aircraft the size of a small jet. This paper narrows its focus deliberately.

It concerns small, commercially derived uncrewed aircraft, most often in quadcopter form, broadly within the Civil Aviation Safety Authority's sub-2kg categories and at the lower end of what the United States Department of Defense classifies as Group 1. These are systems built largely from commercial off-the-shelf (COTS) components and cheap enough to be acquired, modified, deployed and lost by individuals or small groups without state-level resources. A working definition is set out in section 2.1.

Larger systems appear in this paper only where they illustrate something that transfers. The Bayraktar TB2 and Harop loitering munitions used in Nagorno-Karabakh, and the Shahed-series one-way attack drones used against Ukraine and in the Middle East, are not the threat an Australian port or hospital should be planning against, and this paper does not suggest otherwise. They are used here for three narrow purposes: because they generate the only reliable published cost data on what it takes to intercept a drone, because they demonstrate saturation as a principle, and because they show what happens to concentrated infrastructure when a defence fails. Managing those threats is a matter for national air defence and sits outside this paper's scope, as does the use of small drones by military forces in combat, which is a different problem under a different legal framework.

Geographically, the paper draws on international incidents and, increasingly, domestic ones, to inform an Australian risk assessment and policy response set out in Parts III, IV and V.

1.4 Threat and hazard

One distinction is important to know and should be set out before anything else. A **threat** is a deliberate action intended to cause harm, disruption, surveillance or unauthorised access. A

[26] Cyber and Infrastructure Security Centre, "Security of Critical Infrastructure Act 2018 — obligations factsheet," setting out the sectors, asset classes and Positive Security Obligations including risk management program and reporting requirements.

hazard is otherwise lawful, negligent or accidental drone activity that produces a safety or operational consequence without hostile intent.

Separating them matters operationally. To a defender's sensors, the two are frequently indistinguishable, so the immediate problem is *classification* (threat or hazard), not *attribution*, which is a slower question and one that often remains unresolved. A negligent operator and a hostile one are not equivalent in intent, but there is potential on either side to cause damage or casualties.

1.5 Methodology, assumptions and limitations

This paper is built entirely from open-source material: government and regulatory publications, peer-reviewed and think-tank analysis, contemporaneous news reporting, court judgments, and public disclosures from technology vendors. Material factual claims are sourced to publicly accessible references with a live link, and analytical judgements are identified as such rather than presented as findings of fact.

Source hierarchy. Primary legislation, official investigations, regulatory publications and government statements are preferred for legal and factual claims. Peer-reviewed research and established analytical organisations are used for technical and strategic analysis. Media reporting is used where primary information is unavailable or where an incident record exists only in contemporaneous reporting. Vendor material is identified as such, is used only for claims about what a company has built or demonstrated, and is not treated as independent performance validation. Where a manufacturer's own test result is quoted, it is labelled *manufacturer-reported*.

Contested figures. Where a figure is materially disputed and the dispute affects the argument, the text gives the range and identifies who is claiming what, instead of presenting a single number as settled. The damage estimate for Operation Spiderweb at section 6.1.1 is the clearest example.

Where possible, figures relating to cost, casualties or damage have been checked against multiple sources. Under-reporting and over-reporting are both real possibilities in this field, particularly in the immediate aftermath of an incident and where sensitive military or commercial information is involved.

Restricting the paper to publicly verifiable information is deliberate. No claim here depends on the reader trusting the author, the paper is suitable for broad distribution without classification concerns, and it cannot assist a malicious actor with detail beyond what is already public.

Three assumptions underpin the analysis: that the pace of change will continue to outstrip regulatory and procurement adaptation; that the line between commercially available and military-grade capability will continue to blur; and that specific products, prices and capabilities referenced here will date, in some cases within months. A reader in 2028 should treat the technology sections as an explanation of categories and trade-offs and verify current capability independently.

2. The evolution of small drone technology

2.1 What is a small drone?

For the purposes of this paper, a small drone is an uncrewed aircraft built largely from commercial off-the-shelf components, most often in quadcopter form, cheap enough that its loss does not represent a significant investment to the operator. Table 1 gives a general guide to the current field. Outliers exist, and depending on the intended purpose, trade-offs are made: a faster or heavier drone will have shorter endurance, and a longer-range drone will usually carry less.

Table 1: Generalised specifications of common small uncrewed aircraft

Attribute	Typical range
Dimensions	Usually described by frame size; 7-inch is a common standard for FPV airframes
Weight	Sub-2kg, with most consumer camera drones between 250g and 1.5kg
Control link	Analogue (lower latency, cheaper) or digital (more expensive, better image quality). Under jamming, an analogue signal degrades progressively with jamming strength; a digital link is somewhat more resistant but can cut out entirely
Range	Commonly 5–8km for smaller airframes and up to 20km for larger ones. Fibre-optic-controlled military types now reach 30–40km
Payload capacity	Up to 1.5kg
Speed	Roughly up to 60km/h for camera drones; racing and attack FPV airframes are considerably faster
Flight time	Up to 45 minutes, and often under 20 for FPV airframes carrying payloads
Cost	$500–$2,500, more for advanced cameras or specific capabilities. FPV attack airframes sit at the lower end of this range; reconnaissance platforms at the higher end

Australia's own regulatory categories offer a useful guide. CASA does not require registration or a licence for recreational flying of drones under 250 grams; commercial use requires registration and either operator accreditation or a remote pilot licence; and drones over 25 kilograms require specific approval.[27] The archetypal example most readers will picture, a DJI Mavic-style camera quadcopter, sits at roughly one kilogram.

2.2 The evolution of commercial drone technology

Hobbyist radio-controlled aircraft have existed for decades, but they required real skill to fly and offered no stabilisation beyond the aerodynamic design of the aircraft itself. That changed in the early 2010s with the emergence of the consumer drone market, made possible by the convergence of four technology trends: flight controllers miniaturised and cheapened to the point of mass production; lithium-polymer battery energy density reached a level that supported useful flight times; smartphone-grade sensors, including accelerometers, gyroscopes, GPS chips and camera modules, became cheap enough to embed in a consumer product; and the software required to integrate all of it into a coherent product matured.

[27] Civil Aviation Safety Authority, "Drone safety rules," covering registration, accreditation, weight thresholds and operating requirements.

DJI's launch of the Phantom line is generally treated as the watershed moment. It was a drone that could be taken out of a box and flown, with GPS-assisted stability, by someone with no piloting experience. DJI went on to capture a dominant share of the global consumer and prosumer market, commonly cited at around 70 percent,[28] a level of concentration that matters beyond the commercial story because it underpins the supply chain concerns discussed at section 4.9. Over the following decade the same trend continued: capabilities that once cost tens of thousands of dollars, and sometimes required a crewed aircraft or helicopter, became available in a lighter and less capable but genuinely functional form for a few hundred dollars.

2.3 Military adoption

Military interest in uncrewed aircraft long predates the commercial drone boom. Israel's use of decoy drones to draw out and exhaust Egyptian surface-to-air missile batteries during the 1973 Yom Kippur War, and its more extensive use of UAVs for reconnaissance and suppression of enemy air defences in the 1982 Lebanon campaign, are generally credited as the first operationally significant use of uncrewed aircraft in modern warfare. The United States' development of the MQ-1 Predator and, later, the MQ-9 Reaper defined the public image of military drone use for the two decades following the September 11 attacks. Those aircraft were large, expensive, and flown by trained personnel in military and intelligence organisations.

What has changed more recently, and what matters most here, is a second and quite different pattern of adoption. Rather than waiting for purpose-built platforms delivered through long procurement cycles, state militaries and non-state armed groups have increasingly adapted commercially derived drones for military effect. The shift is driven by cost, by attritability, and by the speed at which commercial technology now outpaces defence acquisition. Ukraine's defence industry reached a stated capacity of more than eight million FPV drones a year, produced across more than 160 companies, and Ukrainian officials attribute around 60 percent of Russian losses to FPV drones.[29] This strategy does not necessarily equate to parity with those larger, more expensive systems, but does achieve a comparable level of traditional capabilities alongside genuinely new ones.

2.4 Civilian adoption, including in Australia

The overwhelming majority of small drones outside conflict zones have nothing to do with any of the above, and any regulatory response has to account for a legitimate industry that is both large and growing. Deloitte Access Economics, in analysis commissioned by the Department of Infrastructure, projected that drone adoption could expand Australian real GDP by $14.5 billion to 2040 and deliver $9.3 billion in direct cost savings over the same period in present-value terms, supporting roughly 5,500 full-time-equivalent jobs.[30]

---

[28] Cyber Security Cooperative Research Centre, *Flight Critical: Drones, Cyber Security and Critical Infrastructure*, 2024.

[29] National Security and Defence Council of Ukraine, "Results of Ukraine's Defense Industry in 2025: FPV Drones."

[30] Deloitte Access Economics, *Economic Benefit Analysis of Drones in Australia*, report for the Department of Infrastructure, Transport, Regional Development and Communications, 23 October 2020, projecting a $14.5 billion expansion in Australian real GDP to 2040 under a medium uptake scenario, $9.3 billion in direct cost savings in present-value terms at a 7 percent real discount rate, and 5,500 full-time-equivalent jobs.

Agriculture has been an early and substantial adopter, using drones for crop monitoring, precision spraying and livestock surveying across broadacre operations. Electricity, infrastructure utilities and surveying organisations increasingly use drones for powerline and asset inspection, replacing more expensive and higher-risk helicopter-based regimes. Real estate, media and event photography have all been reshaped by cheap aerial imagery. Emergency services, particularly search and rescue, use thermal-equipped drones to cover terrain that would take ground teams hours to search. New South Wales operates one of the largest civil drone programs in the country in its shark surveillance operation, which has flown more than 160,000 flights since 2017 and received a further $34 million in 2026 to expand its coverage.[31]

Perhaps the most visible field of drone adoption has been to delivery capabilities. There have been large trials in Australia by Alphabet-owned Wing, which delivered items ranging from groceries to pharmacy items. While these trials appear to have been unsuccessful from a business standpoint, there are clear international examples of humanitarian benefits to delivery drones. Zipline's medical drone delivery network is able to deliver blood and medical supplies to difficult to reach areas in Rwanda and Ghana.[32] Ultimately, a regulatory environment must account for a beneficial and fast-growing legitimate industry in a proactive manner, not simply in response to the threat and risks small drones pose.

2.5 Characteristics of small drone systems

Several characteristics distinguish small drones as a security problem. Each recurs as a specific technical challenge in Part IV.

The first is attritability. A defender cannot assume an attacker will be deterred by the prospect of losing the platform. This is the single most important difference between a drone and almost any other airborne threat a civilian site has previously had to consider.

The second is the detection profile. A small drone presents a low radar cross-section and flies a low, slow profile that places it in the same detection band as birds and ground clutter, which is exactly what legacy air surveillance radar is engineered to filter out as noise. This is discussed at section 11.1.

The third is the ease of acquiring and modifying small drones. Being built substantially from commercial components makes these aircraft easy to modify, whether to extend range, add a payload, or remove identifying features such as serial numbers or the geofencing that manufacturers apply by default.

The fourth is the signature question. Most consumer drones still depend on GNSS for navigation and a radio link for control, and both create detectable signatures. An increasing share do not,

[31] New South Wales Government, "Major boost to shark-spotting drones to improve beach safety with $120 million shark program," 28 June 2026, recording the $34 million drone allocation within a $120 million program.

[32] ABC News, "From food to medical supplies — what could the future of drone delivery look like in Australia?", 23 February 2024, recording Wing's world-first Canberra service established in 2019 and its subsequent concentration on Logan, and Zipline's medical delivery network.

which is the subject of the next two sections and which undermines the two most commonly deployed detection methods.

2.6 Advances in autonomy and artificial intelligence

Considerable investment on both the commercial and military sides has gone into making drones easier to fly. Waypoint navigation, object tracking, obstacle avoidance and improved flight stability are all examples. By reducing the demand for human input, these features allow an operator to control multiple aircraft, or to focus attention on the payload or camera instead of on flying.

The more consequential recent development is guidance that survives the loss of the operator's link. Onboard computer vision that matches terrain against pre-loaded satellite imagery allows navigation to continue in GNSS-denied environments, in a manner conceptually similar to terrain contour matching (TERCOM) in cruise missiles. Terminal guidance systems maintain a lock on a target after the radio link has been jammed, so that a drone which has been electronically defeated in the conventional sense may still complete its attack. The Ukrainian Saker Scout is the most widely reported example of a system applying computer vision to recognise and classify military equipment without operator involvement, and reporting from late 2023 onwards describes it operating in a mode that seeks and attacks targets without direct human oversight. The account originates with the developer and the extent of that autonomy has been questioned.[33] Open-source reporting suggests fully autonomous engagements have so far remained limited in scale, but the trend is one to watch.

The strategic, legal and ethical questions this raises are outside this paper's scope. The defensive implication sits inside it: a countermeasure that works by breaking the link between a drone and its operator has a shrinking window of usefulness.

2.7 Emerging technology trends

Three trends are most relevant to the protection discussion in Part IV. Figure 1 sets them against the countermeasures each has prompted.

[33] *Forbes*, David Hambling, "Ukraine's AI Drones Seek And Attack Russian Forces Without Human Oversight," 17 October 2023.

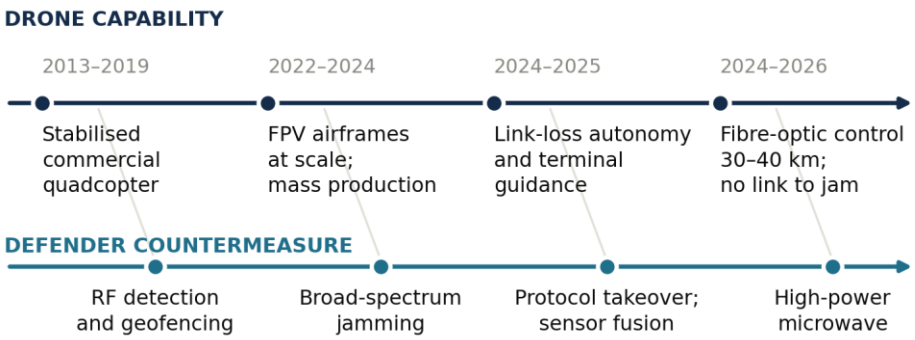

Figure 1: Drone capability and defender countermeasure, 2013–2026. Each capability step has been answered, and each answer has been overtaken.

Fibre-optic control. Fibre-optic-controlled drones transmit control and video signals down a physical cable spooled from the airframe rather than over radio, which makes them effectively immune to the jamming techniques that have been the mainstay of soft-kill response. They emerged at scale with Russian forces around August 2024 during Ukraine's Kursk incursion, and Ukraine had replicated the capability by mid-2025, with more than eighty Ukrainian-designed fibre-optic systems approved for use within months. Russian systems operate beyond 30 kilometres and Ukrainian units have reported ranges around 40 kilometres.[34] The drawbacks are real: the spool adds weight and reduces payload, the cable can snag, and the discarded fibre now litters large areas of Ukrainian farmland and forest, which also means a launch position can potentially be located by following the wire. In a peacetime setting those drawbacks matter more than they do at the front, but the defensive point holds either way: an entire category of countermeasure was rendered ineffective against an entire category of threat within a year.

Swarming. Coordinated multi-drone operations are designed to overwhelm a defender's capacity to detect, track and engage targets individually. In principle this is not new; large bomber formations in the Second World War applied the same logic. What has changed is the cost of achieving it, and the addition of onboard classification and target allocation between aircraft. The defensive implications are discussed at section 12.7.

The adaptation cycle. Every advance in drone capability has prompted a corresponding investment in countermeasures, and every countermeasure has prompted further adaptation. Where jamming was effective, manufacturers added frequency hopping. Where broad-spectrum jamming became common, developers added link-loss autonomy and terminal guidance. Where jamming stopped working entirely, defenders moved toward high-power microwave systems that attack the airframe's electronics rather than its control link, a capability its manufacturer reports demonstrating against a fibre-optic-controlled drone in December 2025.[35] The practical lesson for a buyer is that a counter-drone program built

[34] Atlantic Council, "Fiber-optic drones have emerged as critical kit for…", see reference 20.

[35] Epirus, "Epirus' Leonidas Demonstrates Successful Use of…", see reference 61.

around a specific technique, instead of around an outcome, will be overtaken. This is the reasoning behind the technology neutrality principle at section 10.4.

3. Why small drones matter

3.1 The democratisation of air power

Air power has, for most of its history, been almost the exclusive preserve of the state. Building and sustaining an air force (aircraft, trained pilots, airfields, logistics, maintenance) required a level of capital and institutional capacity that only a national government could typically muster. That scarcity is what gave control of the air its strategic value. It allowed a state to see across a battlefield its adversary could not see across, and to strike targets well behind the front line without first winning a ground campaign to get there.

That scarcity has broken down at the low end of the capability spectrum. A group with no air force, no formally trained pilots and no fixed infrastructure to defend can now field a genuinely useful aerial capability, meaning persistent overhead observation and precision or near-precision strike, for the cost of a handful of consumer electronics purchases. The clearest illustration is not a battlefield at all but a body of water. Since late 2023 the Houthi movement, which controls parts of Yemen and possesses neither an air force nor a blue-water navy in any conventional sense, has used drones alongside missiles and small-boat attacks to threaten and strike commercial shipping in the Red Sea and the Bab-el-Mandeb Strait. The effect was to push a large share of container traffic onto the longer route around the Cape of Good Hope. Suez Canal transits fell from more than 26,000 ships in 2023 to 13,213 in 2024, and canal revenue fell from US$10.3 billion to US$4 billion.[36] That is sustained interference with freedom of navigation on a route of global economic importance, of a kind that has historically required a state with real naval or air power.

3.2 The economics of the exchange

The second shift concerns not who can cause damage from the air, but how cheaply they can do so. Conventional security planning generally assumes that greater resources translate into greater capability, and that a well-funded defender can eventually outspend a poorly-funded attacker. Small drones disrupt that assumption in both directions. They allow an attacker to inflict damage disproportionate to what they spend, and they force a defender to spend disproportionately for the chance of stopping them.

Operation Spiderweb, examined at section 6.1.1, is the starkest illustration on the attacking side. The over 100 FPV drones used were individually inexpensive commercial or near-commercial platforms. Even accounting for the eighteen months of planning, logistics and personnel the operation required, which was substantial and should not be glossed over, the resulting damage to aircraft that Russia cannot readily replace represents a cost-exchange ratio with little historical precedent. The 2019 attack on Saudi Arabia's Abqaiq and Khurais facilities tells the same story from the defender's side: drones and missiles penetrated an air defence

[36] Euronews, "Egypt's Suez Canal revenue fell sharply in 2024 on regional tensions," 17 April 2025, reporting Suez Canal Authority figures.

network built around high-altitude ballistic intercepts and briefly removed roughly five percent of global oil supply.[37]

The defensive side of the equation has been quantified, though only for a larger class of aircraft, because that is where the published data exists. Analysis by the Center for Strategic and International Studies puts the unit cost of a Shahed-type one-way attack drone (a substantially larger and longer-ranged aircraft than anything this paper is otherwise concerned with) at around US$35,000, against roughly US$1 million for a NASAMS engagement using an AIM-9X and over US$3 million for a Patriot PAC-3 interceptor. Using a million-dollar interceptor against a thirty-five-thousand-dollar drone is clearly unsustainable long term, even when considering the value of the defended asset, and the analysis concludes that the United States is on the wrong side of the cost curve based on what Ukraine has learned.[38]

This arithmetic is one of the principal factors shaping the counter-drone principles set out in Part IV, and in particular the emphasis on low cost-per-engagement effectors over expensive one-shot solutions. It is also the reason a defender cannot reliably out-resource this threat: the attacker can often force the defender into an engagement whose cost is substantially greater than the cost of the attacking platform.

3.3 Why peacetime offers less protection than it appears

All of these examples come from wars, and Australia is not in one. Three case studies in Part II are included specifically to answer that. The Gatwick closure in December 2018 happened in a peaceful country, to a commercial airport, with no confirmed hostile actor ever identified, and cost the airport and its airlines tens of millions of pounds.[39] The wave of drone reports over the northeastern United States in late 2024 generated weeks of national alarm and congressional pressure without investigators ever finding anything anomalous.[40] The European wave that began in September 2025 closed airports in at least five countries, overflew nuclear power stations, air bases and ports, and produced the first instance in this record of a NATO military opening fire on a drone over its own territory, again without any operator being publicly identified.[41] [42]

What those three have in common is that the disruption did not depend on anyone being attacked; uncertainty was sufficient. An organisation that cannot tell whether the object over its site is a hobbyist, a journalist, a competitor or something worse is in the same operational position regardless of which it turns out to be, and it will make the same expensive decisions (stop operations, evacuate, call police, brief the media) in all four cases. That is the risk most Australian organisations will actually face, and it is entirely independent of whether Australia is ever a party to a conflict.

---

[37] Congressional Research Service, "Attacks on Saudi Oil Facilities: Effects and Responses", see reference 45.

[38] Center for Strategic and International Studies, "Calculating the Cost-Effectiveness of Russia's Drone Strikes."

[39] *The Week*, "Gatwick drone sightings 'cost airport and airlines £50m'," recording more than 1,000 flights affected across a 33-hour closure.

[40] Department of Homeland Security, "Joint Statement on Ongoing Response to Reported Drone…", see reference 56.

[41] NL Times, "Dutch military opens fire on unidentified drones over Volkel air base," 22 November 2025.

[42] Arms Control Association, *Drone Incursions in Belgium Spark Probes, NATO-EU Response*, see reference 16.

Part II — Understanding the Threat

4. Threat actors

Any assessment that treats "drone threat" as a single category will misallocate resources. The actors differ primarily in intent, capability, access and likelihood, not along a simple hierarchy of sophistication, and the categories that matter most to an Australian civilian operator are not the ones that dominate international reporting. Table 2 sets out the variables before the detail.

Table 2: Threat and hazard actors — indicative characteristics

Actor	Objective	Intent	Capability	Access	Most likely Australian manifestation
Negligent or unaware operator	Recreation, work, curiosity	None	Low	High	Aviation and emergency services disruption
Lone actor	Grievance, notoriety	Variable	Low	High	Airspace incursion, nuisance
Activist group	Publicity, embarrassment	Disruption	Low to moderate	Moderate	Site incursion, protest reconnaissance
Commercial competitor	Commercial advantage	Information gathering	Low to moderate	Moderate	Surveillance of sites, processes, executives
Criminal organisation	Profit	High	Moderate	Moderate	Contraband delivery, reconnaissance
Insider	Varies with sponsor	High	Potentially high	Very high	Enabling or conducting a targeted act
Terrorist organisation	Coercion, attention	High	Low to moderate	Variable	Payload delivery against a soft target
Proxy force	Sponsor's strategic aim	High	Moderate to high	Low in Australia	Not a realistic domestic scenario
Nation state	Intelligence, preparation	High	High	Variable	Intelligence collection; supply chain and data access

Indicative strategic assessment. Capability and access describe what an actor would need and could plausibly obtain, not an assessment of any specific group's current activity in Australia.

4.1 Nation states

States appear in this picture in three roles: as direct operators, as suppliers, and, in the role that matters most to a country that is not at war, as clandestine actors who would prefer not to be seen acting at all.

As direct operators, the mutual drone campaigns of Russia and Ukraine are the dominant current example, examined at section 6.1. As suppliers, Turkey's export of the Bayraktar TB2 to Azerbaijan and later to Ukraine, and Iran's supply of Shahed-series drones (subsequently produced under licence in Russia as the Geran-2) to Russia and to regional proxies, illustrate how one state's drone industry can shape conflicts far from its own borders. The related question of who manufactures the drones an Australian organisation flies itself, and where the data goes, is dealt with separately at section 4.9. The third role occupies the remainder of this

section, because it is the one that operates in peacetime and the one that survives the tyranny of distance.

Plausible deniability. A state that wants an effect on Australian soil without a war has to satisfy two conditions: the act should not be readily traceable to it, and, more importantly, it should not oblige anyone to respond. The second is easier than it sounds. Cormac and Aldrich argue that plausible deniability barely existed even in its supposed heyday, and that states routinely act unacknowledged in the full expectation of being identified; the purpose is not to prevent attribution but to leave the target government able to say formally that it does not know, and therefore free to choose not to act.[43] The United Kingdom's House of Commons Defence Committee defines the grey zone in the same terms (hostile activity below the threshold of direct state-on-state conflict, designed to coerce governments or erode their ability to function, and often plausibly deniable) and notes that states increasingly work through proxies precisely because it makes identifying the ultimate sponsor harder.[44] CSIS states the practical consequence more plainly than anyone: countries generally do not respond to actions below the threshold of conventional warfare by declaring war on the perpetrator.[45]

The blueprint exists, and is already here. Europe has spent four years demonstrating what that reasoning looks like in operation. Applying a standard of three credible sources per incident, CSIS counted three attributed Russian attacks in Europe in 2022, twelve in 2023 and thirty-four in 2024. Transport accounted for 27% of the targets and critical infrastructure a further 21%, and the most common weapons were explosives and incendiaries, nothing exotic.[46] The recruitment model is where the campaign's economics sit. RUSI's work on how that campaign is financed reports, on the account of a former Polish intelligence officer, that financial gain is the primary driver in approximately 95% of recruitment cases in Poland, with payments ranging from a few dollars for graffiti to around US$400 for installing a camera and up to US$10,000 for a murder: an arrangement RUSI describes as producing a dispersed, fragmented campaign that is highly deniable, cheap to maintain and easy to scale.[47]

The United Kingdom's first prosecutions under the National Security Act 2023 show the layering inside a single case. Dylan Earl made contact with the Wagner Group over Telegram, recruited Jake Reeves, and between them they arranged the arson of a warehouse in east London holding humanitarian aid and communications equipment bound for Ukraine, causing around £1 million of damage in March 2024. The men they recruited to carry it out did not know who was ultimately paying. Earl was sentenced to seventeen years in October 2025.[48] MI5's Director-General reported a 35% rise over the preceding year in individuals under investigation for state threat activity, and said his teams were routinely uncovering attempts by state actors to commission surveillance, sabotage, arson or physical violence in the United

[43] Rory Cormac and Richard J. Aldrich, "Grey is the new black: covert action and implausible deniability," *International Affairs* 94, no. 3 (May 2018): 477–494.

[44] House of Commons Defence Committee, *Defence in the Grey Zone*, Fifth Report of Session 2024–25, 9 July 2025.

[45] Center for Strategic and International Studies, "Russia's Shadow War Against the West," 18 March 2025, recording three attributed attacks in Europe in 2022, twelve in 2023 and thirty-four in 2024 against a three-source evidentiary standard.

[46] Center for Strategic and International Studies, "Russia's Shadow War Against the West", see reference 37.

[47] Royal United Services Institute, "Responding to Russian Sabotage Financing," 14 January 2026.

[48] Crown Prosecution Service, "How the CPS used new National Security Act legislation to prosecute the plot to sabotage Ukrainian aid warehouses on UK soil," updated with sentencing, 24 October 2025.

Kingdom.[49] None of that involved a drone but illustrates the playbook: the sponsorship, tasking, payment and disposal arrangements for deniable physical action against infrastructure in a Western democracy already exist and are in routine use.

What Spiderweb supplied was the other half. The operation examined at section 6.1.1 demonstrates method, not deniability; it was conducted by a state at open war and claimed by that state within a day. But the method is the part that transfers. Roughly eighteen months of preparation; components imported commercially and assembled in-country; concealment inside ordinary freight, in modular cabins on trucks indistinguishable from any other load; haulage to the target by drivers who did not know what they were carrying; and nobody belonging to the sponsor present at the moment of attack. Every link in that chain sits beneath the thresholds that border, aviation and air defence systems were built to detect, for the straightforward reason that none of those systems is looking for a shed on a truck.

Being precise about what has and has not been observed. Until very recently these three strands (covert pre-positioning, deniable proxy action, and drone incursions against national infrastructure) had not been publicly documented as a single case. Ukraine's pre-positioning is documented but acknowledged. Russia's European campaign is attributed but had not used drones. The 2025 European incursions at section 6.3 used drones against precisely the target set this argument concerns, nuclear plants, a submarine base, nuclear weapons storage and major airports, and have never been attributed to anyone.

That gap closed while this paper was being written. On the evening of 4 August 2026, a drone carrying professional explosive and a detonator was found near a parked Ukrainian Antonov An-124 cargo aircraft at Leipzig/Halle Airport, Germany's principal air freight hub. Police removed the detonator with a disposal robot; the Federal Prosecutor took the case over two days later, investigating attempted causing of an explosion and dangerous interference with air traffic against unknown persons.[50] Germany's interior minister initially described an explosives-armed drone at an airport as a new threat scenario and declined to name an origin.[51] On 1 September 2026 the federal government finally named Russia as being behind the attempted attacks.[52]

The significance for this section is not the diplomatic consequence but the shape of the operation. A state, acting in a country at peace, is said to have combined a professionally built explosive drone with a target of its own choosing and a deniable delivery layer of disposable local agents. That is the convergence the preceding paragraphs describe, and it took place at a

[49] Security Service (MI5), "Director General Sir Ken McCallum gives threat update," 16 October 2025.

[50] Der Generalbundesanwalt beim Bundesgerichtshof, "Übernahme der Ermittlungen nach Drohnenfund am Flughafen Leipzig/Halle," 6 August 2026, recording the assumption of jurisdiction on grounds of the case's particular significance, investigation for attempted causing of an explosion and dangerous interference with air traffic, and a drone carrying professional explosive and a detonator. No suspect or foreign state is named in the release.

[51] Associated Press, "Drone with explosives found at German airport, official sees 'new quality' of threat," 6 August 2026, reporting the discovery of the device at Leipzig/Halle Airport and Interior Minister Alexander Dobrindt's initial response. The Federal Prosecutor dates the incident itself to the evening of 4 August 2026.

[52] Associated Press, "Germany blames Russia for attempted drone attack at Leipzig airport," 1 September 2026, reporting the joint statement of Interior Minister Alexander Dobrindt and Foreign Minister Johann Wadephul, the characterisation of the perpetrators as lower-level operatives acting on behalf of Russian state entities, the closure of the Russian Consulate General in Bonn and the Russian House in Berlin, and Russia's rejection of the finding.

civil freight airport. Each component capability had been demonstrated separately before August 2026; what Leipzig supplies is a single case in which they appear together.

The opening phase of a sudden conflict. The reason this deserves attention beyond a single attributed incident is timing. Australia's distance is a valuable defence against most forms of attack and no defence whatever against a capability that is already here (section 7.1). A state anticipating a confrontation, and wanting an effect on Australian soil in the first hours of it, has essentially one option: to have put the means in the country beforehand, quietly, at a time when doing so attracted no attention and broke, at most, minor law. That is the same reasoning ASIO has described at length in the cyber domain (access is established before it is needed precisely because it cannot be established at the moment it is needed), with the difference that the object being pre-positioned here is physical, cheap, legally purchased and, until the moment it is used, indistinguishable from hobby equipment sitting in a storage unit.

The damage such a capability could do should not be estimated from the size of the aircraft. It falls well short of a strike campaign and cannot sustain one. What it can do is deliver a small number of precise attacks, at a moment of the sponsor's choosing rather than the defender's, against assets that are few in number, fixed in location, unhardened and slow to replace. Spiderweb's significance was never the 100-plus drones; it was that a third of Russia's strategic bomber fleet was parked in the open at bases whose operators had no reason to believe were within reach. The Australian equivalents (i.e. F-35s) are identified by the same test, not by speculation about any particular site: held in small numbers, at known coordinates, with long replacement lead times and no ready substitute (sections 8.1 and 9.2), albeit likely to be kept in hardened aircraft shelters. Damage to a handful of them would be strategically significant in a way that bears no relation to the cost of the drones, and, as section 9.4 sets out, the consequences would not stay with the operator of the site.

There is a further complication specific to the transition from peace to conflict. Deniability does not become irrelevant once a confrontation begins; it changes function. Action that cannot be attributed in the days before hostilities are acknowledged makes acknowledging them harder, and that difficulty is itself an objective. One unexplained drone over an Australian base is a security problem; several, in the same week as a regional crisis, is a political one. This is where the paper's recurring argument about attribution (sections 10.6 and 12.2) matters most and is hardest to hold: the decisions have to be made without it, and the pressure to wait will be greatest at exactly the moment waiting costs the most.

What the Australian record actually says. While narrower than Europe's record, ASIO's Director-General has warned since 2025 that sabotage will pose an increasing threat over the following five years, that this is not limited to defence assets, and that Australia is getting closer to the threshold for high-impact sabotage.[53] The 2026 assessment disclosed that nation-state actors had compromised the network of an Australian critical infrastructure provider and were maintaining access so that they could, in the Director-General's words, cripple it at a time of

[53] Australian Security Intelligence Organisation, "Director-General's Annual Threat Assessment 2025," delivered 19 February 2025.

their choosing.[54] Both statements concern cyber pre-positioning. ASIO has not publicly warned of physical drone pre-positioning in Australia, and nothing here should be read as suggesting it has, yet the strategic reasoning ASIO has described (establish the means in advance, hold them unused, keep the choice of timing) is not specific to a network.

4.2 Proxy forces

Proxy forces — armed groups operating with a state sponsor's material support and strategic direction while preserving a degree of deniability for that sponsor — are among the most consequential drone users active today.

The Houthi movement in Yemen, discussed at section 3.1 for its effect on Red Sea shipping, is the most visible current example. Iran-backed militias operating across Iraq and Syria are another. On 28 January 2024, a one-way attack drone struck Tower 22, a small United States logistics outpost on the Jordan–Syria border, killing three Army National Guard soldiers and wounding more than a hundred others.

The aircraft involved was a larger one-way attack drone, not the quadcopter class this paper is concerned with, and it is included here for the identification failure rather than the airframe. The subsequent investigation found that base defence operators had observed radar tracks to the south of Tower 22 and dismissed them as too distant, too slow, or possibly birds or rubbish, in what the report characterised as a negligent departure from procedure. The crew was at the time occupied with recovering a ScanEagle reconnaissance drone that had returned to the base moments before the 5.30am strike, and did not use the cameras available to them to investigate the unknown tracks. No warning came from radar or other systems at Tower 22 or at nearby Al-Tanf. The investigation further found that the position was not manned with the appropriate rank and experience to make the decisions the situation required, and identified insufficient leadership presence, crew exhaustion and inadequately rehearsed battle drills.[55]

That sequence says far less about proxy forces than about identification. It is the clearest documented example available of the identification problem discussed at section 12.1 producing a fatal outcome at a defended military site with sensors working. The tracks were on the screen; what failed was a tired, under-ranked crew's ability to resolve, in the time available, which of two tracks was which, and no sensor procurement addresses that.

4.3 Terrorist organisations

ISIS's campaign in and around Mosul between 2016 and 2017 is the foundational case study for terrorist use of small drones. The group began by using drones for surveillance and propaganda filming before its engineers began modifying commercially available quadcopters to drop small munitions, likely 40 mm rifle grenades, on Iraqi and coalition forces below. Captured documents examined by the Combating Terrorism Center at West Point show a

---

[54] Australian Security Intelligence Organisation, "Director-General's Annual Threat Assessment 2026," delivered 24 June 2026; the compromise of an Australian critical infrastructure provider's network and the phrase "cripple it at a time of their choosing" were reported from the address by *The Register*, 25 June 2026.

[55] Associated Press, "Confusion gripped US base defenders as a flying bomb struck a deadly blow at Tower 22, investigation says," reporting the findings of the United States military investigation into the 28 January 2024 attack.

managed program with procurement, equipment lists, mission forms and training material, well beyond improvisation by individual fighters.[56]

The tactic was crude, but it forced a dedicated coalition counter-drone response and established a pattern that has since recurred in Myanmar and Mexico: commercially available components and a willingness to modify them are enough to give a group a tactical air capability, with nothing purpose-built required.

4.4 Criminal organisations

Organised crime's adoption of drone technology has moved within a few years from novelty to routine tactic, and Mexico provides the most complete dataset. Research mapping weaponised drone attacks attributed to Mexican cartels recorded 221 incidents between 2021 and 2025, of which 27 caused fatalities, with 77 people killed in total. Attacks that began concentrated in Michoacán and Guerrero have since dispersed, including into regions bordering the United States, and the targets are predominantly civilians, community defence forces and rival groups rather than military or police.[57] In one 72-hour period in March 2024, La Nueva Familia Michoacana delivered more than twenty explosive devices by drone.[58]

Analysts tracking this trend have explicitly noted that Mexican cartels have studied and adapted tactics from Ukraine's war: innovation in this space does not stay contained to its conflict of origin, and criminal organisations are active students of it.

For Australian readers the cartel record matters as a demonstration of how quickly technique transfers, not as a direct analogue. The Australian manifestation of criminal drone use is contraband delivery into correctional facilities (section 8.5), the same underlying capability applied to a lower-severity objective. That being said, there is no reason organised crime groups in Australia couldn't adopt similar strategies, particularly against rival groups.

4.5 Lone actors

At the lower-sophistication end are individuals acting alone, motivated by grievance, ideology, curiosity or a desire for notoriety, who fly drones into restricted airspace around airports, government buildings or major events. These incidents are harder to attribute to any coherent doctrine than state, proxy or organised criminal activity, and the individuals involved are frequently never identified.

Where operators have been identified (most clearly at the Paris Games, where most of the 85 operators apprehended turned out not to be acting maliciously), the picture that emerges is dominated by curiosity and inattention rather than intent. No comparable Australian dataset has been published, so this should be read as a pattern observed in the few places that have counted, not a national statistic. On that pattern, lone and unaware operators account for a

[56] Combating Terrorism Center at West Point, "The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft."

[57] Austin C. Doctor, Suat Cubukcu, Joel Elson, George Grispos and Mackenzie Harms, "Mapping Weaponized Drone Attacks Attributed to Mexican Drug Cartels, 2021–2025," National Counterterrorism Innovation, Technology, and Education Center, University of Nebraska at Omaha, 12 February 2026.

[58] Austin C. Doctor, "Mapping Weaponized Drone Attacks Attributed to Mexican…", see reference 21.

disproportionate share of the operational workload discussed in Part IV while sitting at the lower end of the severity spectrum.

4.6 Negligent and unaware operators

Negligence and malice need separating, because they produce identical sensor returns and very different appropriate responses.

The Australian record is dominated by this category. Recreational drones grounded water-bombing aircraft at the Manypeaks fire in Western Australia in January 2025, with the Department of Fire and Emergency Services superintendent of aviation services explaining that any drone sighting over a fire means "we put all the aircraft on the ground or send them back to their base until we can clear the area," and comparing the effect to taking fire trucks off the ground.[59] Similar groundings occurred at Esperance in 2019 and repeatedly through the 2019–20 season, among other incidents.

The operational consequence of a negligent operator can be indistinguishable from that of a hostile one, though the legal, reputational and escalation consequences of getting the identification wrong are not, which is the central difficulty examined at section 12.1. Similarly, negligence can still cause significant real danger to life hence the precautions put in place by emergency services.

4.7 Insider threats

An organisation's own personnel — employees, contractors, or anyone with legitimate routine access to a site — represent a distinct and often underweighted category. Someone with genuine access and knowledge of a site's routines, blind spots and timings is positioned to enable a far more damaging drone-based attack than an outside actor working without that access.

The concern is a general one, and it predates drones. This is the same insider-risk logic that already informs conventional physical and personnel security programs, extended to a new delivery mechanism, and it is already covered by the personnel hazard requirements of a SOCI Act risk management program.[60] It is directly relevant to how Operation Spiderweb succeeded: the operation depended on human reconnaissance and pre-positioning inside Russian territory over many months.

4.8 Activist groups

Activist use of drones is generally intended to disrupt, embarrass or publicise, not to cause physical harm, but the incidents still expose real security gaps and carry risk.

In July 2018, Greenpeace France publicly claimed responsibility for flying a drone shaped as the character Superman into the no-fly zone around the Bugey nuclear power plant near Lyon, France, deliberately crashing it into the wall of the plant's spent-fuel pool building, to

[59] ABC News, "Anger after drones ground water bombers at Manypeaks…", see reference 2.

[60] Cyber and Infrastructure Security Centre, "Security of Critical Infrastructure Act 2018 —…", see reference 47.

demonstrate what the group described as the facility's vulnerability to airborne attack.[61] EDF, the plant operator, acknowledged the incident and said the drone had no effect on the facility's safety.

That claimed action sits alongside a separate and never-resolved episode. Across October and November 2014, a series of drones were reported overflying multiple French nuclear plants in a short window, prompting police complaints from EDF and a parliamentary inquiry. Greenpeace denied any involvement, and no other party was ever identified.

4.9 Commercial competitors, and your own fleet

The actors profiled so far skew heavily towards the military, criminal and ideological, but for many readers of this paper the more probable encounter is none of them.

Competitor surveillance of construction sites, manufacturing processes or research and development activity; reconnaissance ahead of planned protest action; and surveillance of executives at public events or private residences are all real and growing categories of drone misuse. They rarely make international headlines, but for an industry audience they are very often the first and most direct way this threat is actually experienced.

Closely related, and more often overlooked, is the risk carried by an organisation's own drone fleet. A modern enterprise drone is a networked system comprising sensors, controllers, applications, firmware, cloud services and sometimes remote operations centres. Analysis published by the Cyber Security Cooperative Research Centre identifies GPS spoofing, command and control interception, data breaches and signal jamming as live threat vectors against civil UAV operations, and notes that Australia has no cyber security standards for uncrewed aircraft despite CASA identifying this as an immediate priority in 2022; existing regulation covers registration and pilot licensing, not design or security.[62]

The supply chain question sits on top of that. The Australian Defence Force suspended use of its DJI fleet in 2023 pending a supply chain security audit, and the suspension was subsequently extended to other Home Affairs-aligned agencies. The Australian Strategic Policy Institute has argued that the response since has been uneven, noting that Chinese-made drones remain deeply embedded in publicly funded operations, including the New South Wales shark surveillance program's more than 160,000 predominantly DJI-based flights since 2017. Its central argument, in substance, is that Australia regulates where drones may fly but not where their data may go, and that geospatial data collected during routine operations such as bridge inspections, substation surveys and coastal monitoring aggregates into something with strategic value.[63]

None of this adjudicates the merits of any individual ban. The point is that the drones an organisation operates itself, and the data they produce, belong in the same assessment as the drones flying over its fence line.

---

[61] ABC News, "Greenpeace intentionally crashes drone into French nuclear power plant to reveal security vulnerability," July 2018.

[62] Cyber Security Cooperative Research Centre, *Flight Critical: Drones, Cyber Security and Critical…*, see reference 49.

[63] Australian Strategic Policy Institute, "Australia is flying blind on Chinese drone data," *The Strategist*.

5. Operational employment

Having established who uses this technology, this section covers how.

One distinction runs through all of them and needs to be clarified, because it explains why small incidents are able to produce large consequences. A drone's *tactical* effect is what the aircraft itself does: observe a yard, drop a package, damage a cabinet. Its *strategic* effect is what that makes possible or forecloses: a border network briefly blinded, an airport unable to certify its own airspace as clear, a prison committed to a full search. The tactical effect is usually modest and is what a risk assessment measures. The strategic effect is where the cost sits, and it is generally a function of what the target depended on, not what the drone carried, although direct damage is still a serious risk.

5.1 Intelligence collection

The most common and least escalatory use is also the simplest: real-time aerial observation. Artillery spotting, monitoring vehicle movements and building a pattern-of-life picture of a target's routines are applications of one capability — a cheap elevated camera that can loiter over an area for longer, and far more cheaply, than any alternative.

This is the baseline function from which almost everything else in this section derives. An actor rarely moves straight to payload delivery without first having used drones to see. That sequencing matters defensively: the first indication of a serious problem is usually a surveillance pattern, not an attack, and an organisation that treats repeated observation as a nuisance rather than an indicator has discarded its warning.

5.2 Electronic attack and cyber-enabled payloads

Drones are increasingly discussed, and in at least one well-documented case have been used, as a delivery platform for cyber and signals collection tools rather than physical ones.

In 2022, security researchers investigating anomalous internal network activity at a United States financial firm traced the source to the building's own roof, where they reportedly found two modified consumer drones fitted with wireless network intrusion hardware, used to intercept an employee's credentials and then attempt access to internal systems.[64] The case is notable less for its sophistication (the underlying wireless attack is nothing new) than for what it demonstrates: a drone allows a proximity-dependent attack to be launched from a position, such as a rooftop or the airspace above a fence line, that a person or a parked vehicle could not occupy unnoticed.

This paper does not go into how such tools are configured. The relevant point is that the drone threat to an organisation is not purely physical, and that facilities teams and cyber security teams who have never had reason to coordinate closely may need to.

[64] *The Register*, "Wi-Fi spy drones used to snoop on financial firm," 12 October 2022.

5.3 Battle damage assessment

Drones increasingly confirm whether a target was destroyed, damaged or missed, which historically required a separate mission or collection cycle. FPV footage from Ukraine has made near-real-time assessment routine at the tactical level, because an operator watches the strike land in the same feed used to guide it. For a civilian audience the relevance is that footage of an incident is likely to exist and to circulate, which is a communications problem discussed at section 9.6.

5.4 Delivery of payloads

Payload delivery spans a wider spectrum than the severe end most readers will picture, and the full range matters.

At the lethal end sits the pattern established by ISIS in Mosul: small munitions dropped from modified commercial quadcopters, since recurring in Myanmar's civil war and among Mexican cartels. At the other end, and considerably more common in practice, is non-lethal but seriously disruptive delivery: primarily contraband smuggling into correctional facilities, examined in detail at section 8.5, which for corrections and justice agencies is very likely to be the most frequent manifestation of this threat they face.

Between the two ends sit deliveries that are not necessarily lethal, but also not inconsequential: incendiary devices, chemical irritants, or objects intended to be ingested into machinery. An organisation assessing this risk should think in terms of what a 1.5kg payload placed accurately anywhere on its site could do, not in terms of explosives specifically.

5.5 Combined arms and coordinated operations

Drones deliver their greatest effect when integrated with other capabilities as part of a coordinated operation rather than used in isolation.

The October 7 attack, examined at section 6.4, is the clearest illustration using aircraft of the class this paper addresses. Commercial quadcopters were used to disable the sensors that would have detected a ground assault, in the minutes before the ground assault. The drones did not need to damage anything of value; they needed to blind the thing that was watching, for long enough.

Azerbaijan's 2020 campaign in Nagorno-Karabakh, summarised in section 6.4, demonstrates the same principle at state level with much larger aircraft (Bayraktar TB2 drones and Israeli-made Harop loitering munitions) used to suppress air defence and armour so that ground forces could occupy observation positions that fed further targeting data back.

The pattern to internalise is that a drone threat assessed purely on its own terms will tend to understate the actual risk, because the most damaging uses of the technology have consistently been as one component of a coordinated action. For a civilian site, the equivalent question is not "what could a drone do to us" but "what does a drone make possible that was previously impractical."

5.6 Disruption without contact

A distinct employment pattern, and the one most relevant to Australian peacetime risk, is disruption achieved without the drone doing anything at all.

Gatwick is the example: no confirmed drone was recovered, no damage was caused, and the airport closed anyway. The 2025 European wave is the same pattern at continental scale. In both cases the effect was produced by the defender's own necessary caution, not by the attacker's payload.

This category stands apart because it inverts the usual relationship between an attacker's capability and the damage they cause. It is available to an actor with no explosives, no expertise and no intention of harming anyone, and it cannot be defeated by hardening the target. It can only be managed by improving the speed and confidence of identification, which is why Part IV treats detection and identification as the foundation of everything else.

5.7 Mass and saturation attacks

Saturation, or swarm, attacks are operationally distinct from single-drone use, not simply more of the same.

Operation Spiderweb is the case that matters most here, because the aircraft involved were exactly the class this paper is about: Over 100 first-person-view drones launched almost simultaneously from concealed positions against parked aircraft at four separate airbases. Nothing in that operation required a platform an Australian hobbyist could not buy easily.

Larger examples exist, with the caveat that they describe a capability an Australian site is unlikely to face: Russia's Shahed and Geran-series waves against Ukrainian cities have on the heaviest nights involved several hundred aircraft launched together, and the 2019 Abqaiq–Khurais attack combined eighteen drones with seven cruise missiles in a single salvo by the Saudi Defence Ministry's own account.[65] They are included because they are the best-documented instances of the saturation principle, not because a comparable capability is likely to appear over an Australian facility.

What unites them is the specific effect a mass attack is engineered to produce. Saturation does more than increase the odds that any one drone gets through; it is designed to overwhelm the decision and engage stages of a defender's response process, not just the detect stage: a defender may see every drone coming and still be unable to engage all of them in time. This is why counter-swarm defence is treated as a separate response category at section 12.7.

[65] Arab News, *Saudi Arabia's Defense Ministry displays Iranian…*, see reference 14.

6. International case studies

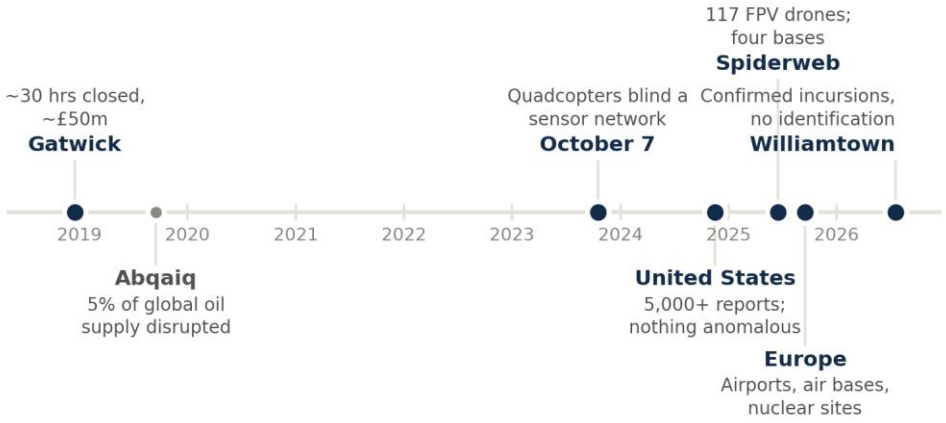

Figure 2: Selected incidents, 2018–2026. Plotted on a true time scale; the clustering from 2023 onward is the point. Navy marks incidents involving the small quadcopter and FPV class this paper addresses. Abqaiq, in grey, involved larger aircraft and is included for the infrastructure lesson only.

Selection criteria. These cases were chosen to illustrate mechanisms, not to form a statistical sample, and that distinction should be kept in view when reading the conclusions at section 6.6. Each was selected because it demonstrates something specific and documented: a delivery method, a failure mode, a consequence pathway, or a response that worked. They span the range of conditions in which small drones have been used, from a full-scale interstate war to a peacetime democracy in which nobody was ever attacked. Three of them (Gatwick, the 2024 United States sightings and the 2025 European wave) happened in countries at peace and are the closest available analogues to Australian conditions. The set is deliberately weighted toward incidents that went badly, because those are the ones that generate published investigation records; section 6.5 sets against them the clearest documented case of a response that worked, which is an equally important input to planning.

6.1 Ukraine

No conflict has driven small drone technology, or the countermeasures against it, as hard or as fast as the war in Ukraine. Since Russia's full-scale invasion in February 2022, both sides have fielded drones across the entire spectrum this paper describes, from inexpensive FPV quadcopters flown by individual soldiers to AI-guided strike systems and the fibre-optic platforms discussed at section 2.7, at a scale with no real historical precedent.

Ukraine's National Security and Defence Council states that domestic industry capacity supports more than eight million FPV drones a year across more than 160 manufacturers, and attributes around 60% of Russian losses to FPV drones.[66] Loss rates on both sides run to thousands of aircraft a month, and that rate has driven the innovation cycle described in Part I:

[66] National Security and Defence Council of Ukraine, "Results of Ukraine's Defense Industry in 2025: FPV Drones.", see reference 75.

first toward guidance that survives a severed link, then toward fibre-optic control that is all but impervious to jamming.

6.1.1 Operation Spiderweb

On 1 June 2025, Ukraine's Security Service executed an operation codenamed Pavutyna, or Spiderweb, that stands as the most significant demonstration to date of the argument this paper is making.

The operation had been in preparation for roughly eighteen months. Ukrainian intelligence smuggled approximately 150 small strike drones, modular launch systems and 300 explosive payloads into Russia, concealed in wooden modular cabins loaded onto cargo trucks. At the appointed time the cabin roofs were opened remotely and over 100 drones launched directly from the trucks. The drones flew pre-planned routes toward parked aircraft, guided by video relayed over local 4G and LTE networks. AI-assisted targeting reportedly identified structural weak points such as underwing pylons and fuel tank locations, with training data derived in part from museum aircraft.[67]

The targets were chosen deliberately: Tu-95 and Tu-22M3 strategic bombers, Tu-160s, and the rare A-50 airborne early warning aircraft of which Russia has fewer than ten, each estimated at around US$350 million. The bases struck included Olenya in Murmansk Oblast, roughly 1,900 kilometres from Ukraine; Dyagilevo in Ryazan Oblast; Ivanovo, home to the A-50 fleet; and Belaya in Irkutsk Oblast, more than 4,000 kilometres away and the first Ukrainian strike ever conducted in that region.[68] According to President Zelensky's subsequent account, the truck drivers who hauled the cabins across Russia had no idea what they were carrying.

The scale of the damage is disputed, and it is more useful to state the range than to repeat a single number. Ukraine's Security Service claimed 41 aircraft hit or destroyed, representing by its own estimate around a third of Russia's long-range bomber fleet, with damage exceeding US$7 billion.[69] CSIS assessed the operation as striking more than forty high-value aircraft and putting 34% of Russia's strategic cruise missile delivery platforms at risk.[70] Independent and United States assessments have been more conservative, with some analysts putting confirmed destroyed aircraft closer to ten to thirteen. Even at the lower bound it describes a strike deep inside Russian territory, using commercially derived drones, against some of the most valuable and hardest-to-replace (impossible, in some cases) aircraft in the Russian inventory, with no Ukrainian personnel present at the moment of attack.

Assessment. The significance for an Australian readership lies less in the damage total than in what the operation demonstrated about planning assumptions. The aircraft were parked in the open, not in hardened shelters, at bases their operators had no reason to think were within reach, because in any conventional sense they were not. Ukraine did not need to fly an aircraft

[67] Center for Strategic and International Studies, "How Ukraine's Operation 'Spider's Web' Redefines…", see reference 36.

[68] Center for Strategic and International Studies, "How Ukraine's Operation 'Spider's Web' Redefines…", see reference 36.

[69] *Kyiv Independent*, "Operation Spiderweb — everything we know about Ukraine's 'audacious' attack on Russia's heavy bombers," 2 June 2025, recording the Security Service of Ukraine's claim of 41 aircraft, around a third of Russia's cruise missile bomber fleet, and damage of approximately US$7 billion.

[70] Center for Strategic and International Studies, "How Ukraine's Operation 'Spider's Web' Redefines…", see reference 36.

over Russian airspace or fire a missile from Ukrainian soil. CSIS drew three conclusions that carry directly into this paper (the proliferation of cheap attritable technologies, advancing autonomy, and the growing vulnerability of military infrastructure to precision drone threats) and assessed that technological agility, not industrial scale, determines advantage.[71]

Australian relevance. What transfers is the proximity model and the assumption it defeated: an operation of this kind requires access near the target, not reach from the sponsor. What does not transfer is the scale. Eighteen months of clandestine pre-positioning inside a hostile state is a state intelligence operation, not a template for the actors at section 4 most likely to affect an Australian site.

6.2 Gatwick Airport, December 2018

Gatwick is particularly relevant to this topic and to Australia, because it is potentially closest to what an Australian organisation is realistically likely to face.

Between the 19th and 21st of December 2018, reported drone sightings closed the runway at London Gatwick, Britain's second-busiest airport, across three days in the busiest travel week of the year. Sussex Police described a shutdown of around 30 hours, during which sightings occurred in twelve separate groupings lasting between seven and 45 minutes each; later accounts of the total disruption run to 33 or 36 hours depending on how the multiple attempted reopenings are counted.[72] [73] Around 1,000 flights were cancelled or diverted and roughly 140,000 passengers were affected.[74] easyJet alone reported £15 million in losses, comprising around £10 million in customer welfare costs and £5 million in cancelled bookings, having cancelled more than 400 flights affecting 82,000 passengers; Gatwick itself lost at least £15 million in revenue, and contemporaneous reporting put the combined cost to the airport and airlines at around £50 million, possibly higher.[75] [76]

The response was substantial. Ten RAF personnel from the Defence Warning and Reporting Flight deployed counter-drone systems (Falcon Shield, Metis Skyperion and DJI AeroScope) on 20 December, and the military presence was not withdrawn until after the incident had run its course. Sussex Police ran Operation Trebor at a cost of £790,208, with a further £206,708 in assistance from nine other forces, bringing total policing costs to almost £1 million. The Ministry of Defence charged a token fee of £1,161 for the ten RAF personnel deployed.[77]

What makes Gatwick important is what the investigation found, which is very little. Sussex Police recorded 129 separate reports of drone activity, of which 109 came from what it assessed as credible witnesses including pilots and airport staff. No drone was recovered. No photograph or video of a drone was provided to police, despite press photographers with

---

[71] Center for Strategic and International Studies, "How Ukraine's Operation 'Spider's Web' Redefines…", see reference 36.

[72] Sussex Police, as reported in *The Register*, "Sussex Police gives up on £790k Gatwick drone shutdown probe," 27 September 2019, recording 129 reports of drone activity of which 109 came from credible witnesses including pilots and airport staff, sightings in twelve groupings across a 30-hour shutdown, and Assistant Chief Constable Dave Miller's statement closing the investigation.

[73] Fortune, *Gatwick's December Drone Closure Cost Airlines $64.5…*, see reference 68.

[74] Fortune, *Gatwick's December Drone Closure Cost Airlines $64.5…*, see reference 68.

[75] Fortune, *Gatwick's December Drone Closure Cost Airlines $64.5…*, see reference 68.

[76] The Week, *Gatwick drone sightings 'cost airport and airlines £50m'*, see reference 104.

[77] Airprox Reality Check, "Gatwick 2018", see reference 10.

professional equipment being on site within hours. The Civil Aviation Authority and Department for Transport have both confirmed they hold no description of the aircraft. Not a single flying pilot filed a report in the vicinity of Gatwick over the period, and National Police Air Service crews sighted neither a drone nor an operator on any of the occasions they flew. After the RAF systems arrived on 20 December, visual sightings continued but were not corroborated by the counter-drone equipment, and the RAF confirmed to the airport's operating authorities the absence of any hostile or malicious drone activity.[78] Two people arrested on the 21st of December were released without charge and were later found to be innocent. The investigation closed in September 2019 with, in Assistant Chief Constable Dave Miller's words, "no further realistic lines of enquiry."[79]

Assessment. Five lessons follow, each applying to an Australian critical infrastructure operator without modification.

First, the disruption was the attack, whether or not there was an attacker. Gatwick lost no aircraft, no building and no person; what it lost was around a day and a half, and the cost of that time exceeded the cost of almost any physical damage a small drone could realistically have caused.

Second, the absence of reliable detection did not merely prevent a response, it prevented a decision. Because nobody could confirm whether a drone was present, nobody could confirm when it was safe to reopen, which is partially why the closure ran across three days instead of one evening. This is the origin of the detection-and-decision principle at section 10.2 and the exercise requirement at section 14.6.

Third, a trialled capability is not an operational one. The airport had engaged with drone detection before December 2018 and had no working network in place when it was needed.

Fourth, a capability brought in during a crisis behaves differently from one integrated beforehand. The RAF equipment that arrived on December 20th did not corroborate the sightings that continued after it was in place, and the RAF's own conclusion was that there had been no hostile or malicious drone activity. Whether that means there was never a drone, or that the equipment could not see it, is both unknown and ultimately irrelevant: by the time a specialist capability is being driven to a site, the decisions that matter have already been made without it.

Fifth, and most uncomfortably, the record does not settle whether a drone was ever there. Sussex Police maintained throughout that the incident was a genuine malicious act, and 109 credible witnesses is not a trivial evidentiary base. Against that, no airprox report was filed, NPAS crews saw nothing, no photograph was produced, and the counter-drone equipment did not corroborate the sightings that continued after it arrived; some analysts have concluded from this that at least part of the episode was misidentification amplified by reporting. This paper does not adjudicate between those readings, and neither should a planner. An airport lost around 30 hours and £50 million to sightings whose physical cause was never established,

[78] Airprox Reality Check, "Gatwick 2018", see reference 10.

[79] *The Register*, "Sussex Police gives up on £790k Gatwick drone shutdown probe," 27 September 2019.

and hardening does not address that. What does address it is the ability to resolve a sighting quickly, and to say publicly and defensibly what is and is not known while it is unresolved.

6.3 The 2025 European drone wave

If Gatwick is the clearest single-site case study, the wave of incursions that began across Europe on 22 September 2025 is the clearest demonstration of what the same phenomenon looks like at national and continental scale, against states that are demonstrably not at war on their own territory. The incidents spread across at least Denmark, Norway, Germany, Belgium, the Netherlands and France through to early December. A partial list gives the shape of it:

- **Denmark and Norway, 22–23 September.** Drone sightings halted traffic at Copenhagen Airport for close to four hours and closed Oslo Airport's airspace for three. Danish Prime Minister Mette Frederiksen called it "the most serious attack on Danish critical infrastructure to date" and said the activity appeared designed to disrupt and create unrest. Police Chief Superintendent Jens Jespersen described an operator with "the capabilities, the will, and the tools to show off in this way," and investigators did not exclude launch from a ship, the airport sitting adjacent to Baltic shipping lanes.[80]
- **Germany, 2–4 October.** Munich Airport closed twice inside 24 hours. Across the two closures, 46 flights were cancelled or delayed and around 6,500 passengers were affected. Police confirmed two simultaneous sightings by patrols near both runways, but the drones moved away before they could be identified. Interior Minister Alexander Dobrindt called the episode a wake-up call, and the German government moved to legislate to allow the military to shoot drones down.[81]
- **Belgium, October–November.** Belgium recorded seventeen unexplained drone sightings across nuclear power plants, military sites and airports, among them Kleine Brogel air base (believed to host United States nuclear weapons) and both main Brussels airports, with shutdowns on 6 and 10 November.[82] The first reports came from the Elsenborn military training area a month earlier, and a €50 million counter-drone package was approved on 8 November.[83] Defence Minister Theo Francken described the incidents as coordinated and resembling a spying operation, adding that he had ideas about who was responsible but would be careful about speculating.[84]
- **Netherlands, 22 November.** Dutch forces fired on unidentified drones over Volkel Air Base, a site where drones are prohibited under Dutch law. The drones left the area and were not found, and the Defence Ministry declined to describe the detection methods or weapons used.[85] Related sightings occurred at NATO's Brunssum command centre, Maastricht Aachen Airport, Schiphol and the port of Terneuzen.[86]

---

[80] CNN, "Denmark links drones at Copenhagen airport to hybrid…", see reference 43.

[81] Al Jazeera, "Munich airport resumes operations after more drone sightings halted flights," 4 October 2025.

[82] Arms Control Association, *Drone Incursions in Belgium Spark Probes, NATO-EU Response*, see reference 16.

[83] Egmont Institute, "Belgium's Public Confrontation with Hybrid Threats: Lessons from Drone Incursions."

[84] Arms Control Association, *Drone Incursions in Belgium Spark Probes, NATO-EU Response*, see reference 16.

[85] Netherlands Ministry of Defence, "Optreden tegen drones boven vliegbasis Volkel," 22 November 2025, confirming that air force personnel deployed ground-based weapons, after which the drones departed, and that no further information on detection or countermeasures would be released.

[86] NL Times, "Dutch military opens fire on unidentified drones over…", see reference 79.

- **France, 4 December.** Five drones overflew the Île Longue submarine base on the Crozon Peninsula, home to France's ballistic missile submarine force, at around 7.30pm. The marine rifle battalion responsible for base security carried out several counter-drone engagements using a jammer rather than a firearm. None of the drones was brought down and no operator was identified. Drones had been reported over the Crozon peninsula on the night of 17–18 November, though French reporting notes that those did not overfly military installations.[87] [88]

Documented, and separately, suspected. Precision about which is which matters here, because the two are routinely conflated in reporting on this episode. Documented: the closures, the sites, the flight reports, the engagements, the national alert postures, the €50 million Belgian package,[89] and the deployment of French, German and British counter-drone teams into Belgium with further United States assistance offered.[90] Suspected but not established: that any of it was state-directed. Belgian Defence Minister Theo Francken described the incidents as coordinated and resembling a spying operation, and said he had views on responsibility that he would be careful about airing; NATO officials expressed concern that the flights were testing allied defences.[91] Those are characterisations by officials, not findings.

Analysis by the Egmont Institute puts the position carefully: no European country possesses absolute security against such incursions even with advanced layered systems; no definitive evidence linked the incursions to any entity; and the operations were calibrated to sit below the threshold that would trigger retaliation, in the grey zone between peace and conflict.[92]

No operator was publicly identified in any of the episodes above, and none has been since. Every practical decision described here was made, and had to be made, without attribution.

Five things about this episode should concern an Australian planner.

The sites chosen were not random. Nuclear power stations, a submarine base, a nuclear weapons storage site, a naval shipbuilder, a major cargo airport and a strategic canal is a target set that reads like a deliberate survey of national dependencies.

Airports closed for hours, not days, and the cumulative effect was still severe. The lesson from Gatwick was that a single long closure is expensive; the lesson here is that many short closures across a network are expensive in a different and harder-to-model way.

Existing countermeasures failed visibly. French marines attempted to jam five drones over a ballistic missile submarine base and brought down none of them. Dutch forces fired on drones

---

[87] The War Zone, "Nuclear Submarine Base Drone Incursion Prompts French Military Response," reporting the 5 December 2025 overflight of Île Longue, the use of a jammer by the marine rifle battalion responsible for base security, and the failure to bring down any of the five drones.

[88] Opex360 (Zone Militaire), "Les fusiliers marins de la base sous-marine de l'Île Longue ont tenté d'abattre des drones inconnus," 5 December 2025, placing the overflight at about 7.30pm on 4 December and recording that drones reported over the Crozon peninsula on 17–18 November had not overflown military installations.

[89] Egmont Institute, "Belgium's Public Confrontation with Hybrid Threats…", see reference 60.

[90] Arms Control Association, *Drone Incursions in Belgium Spark Probes, NATO-EU Response*, see reference 16.

[91] Arms Control Association, *Drone Incursions in Belgium Spark Probes, NATO-EU Response*, see reference 16.

[92] Egmont Institute, "Belgium's Public Confrontation with Hybrid Threats…", see reference 60.

at Volkel and recovered nothing. These are well-resourced NATO militaries operating on their own bases under national authority, which is the most permissive legal and operational environment available anywhere, and it was still not sufficient.

The response required international assistance. That the United Kingdom, France and Germany had to send counter-drone teams into Belgium, with the United States offering further support, indicates that even advanced European states did not hold enough organic capability to cover their own critical sites. Belgium's €50 million package was announced four days into the intensified phase, which is a fast response by any government standard but still well behind the events.

And attribution never arrived. Every practical decision — closing an airport, raising alert levels, deploying a frigate — had to be made in its absence, and would have had to be made the same way whether the operator turned out to be a state, an activist or a group of enthusiasts. It should be noted though, that there were and are suspicions (Russia) but not *publicly* acknowledged.

6.4 Four further cases in brief

Four more cases are drawn on elsewhere in this paper and are set out here in short form, because each contributes one finding, not a full narrative.

The 2024 United States sightings. From mid-November 2024, drone sightings were reported in large numbers across the northeastern United States, concentrated around sensitive New Jersey sites, producing weeks of public alarm and federal flight restrictions. On 17 December the Department of Homeland Security, FBI, FAA and Department of Defense published a joint statement: more than 5,000 reported sightings had generated around 100 leads, and the agencies had "not identified anything anomalous," attributing the reports to lawful commercial, hobbyist and law enforcement drones, crewed aircraft and… stars.[93] The panic was not substantiated however the institutional problem behind it was. In February 2025, NORAD commander General Gregory Guillot testified that 350 drone detections had been reported across 100 United States military installations during 2024, sought authority extending slightly beyond the fence line, and described existing constraints as creating "significant vulnerabilities that have been exploited by known and unknown actors."[94] Uncrewed aircraft had been observed over Langley Air Force Base a year earlier, and a former NORAD commander said afterwards that an installation commander's responsibility "stopped at the fence line," leaving commanders who "didn't feel empowered" to act.[95] The institutional response arrived after a public panic rather than after the operational indicator, and the most capable military in the world could not detect, attribute, explain or communicate about activity over its own bases.

Abqaiq, September 2019. The Saudi Defence Ministry's own account put the attack on Aramco's Abqaiq processing facility at eighteen drones and three cruise missiles, plus four missiles against Khurais, launched from the north rather than from Yemen as the Houthis

[93] Department of Homeland Security, "Joint Statement on Ongoing Response to Reported Drone…", see reference 56.

[94] United States Senate Committee on Armed Services, *Stenographic Transcript: Hearing to Receive Testimony…*, see reference 105.

[95] The War Zone, "Drone Swarms Over Langley AFB Didn't Surprise General In Charge Of NORAD," reporting the December 2023 Langley incursions and retired General Glen VanHerck's assessment of detection and authority gaps.

claimed.[96] It temporarily disrupted 5.7 million barrels a day, over half of Saudi output and about five percent of global supply.[97] Air defences built around high-altitude ballistic intercept (Patriot air defence systems), with batteries oriented against a southern and eastern threat axis and not a northern one, did not engage it.[98] The aircraft were far larger than the class this paper addresses and the attack included cruise missiles, so it stands outside the question of what a commercial drone can do on its own. It earns its place as the only case here in which the target was industrial processing plant whose loss had immediate global economic consequences, and the vulnerability it exposed — that a small number of precisely placed charges can take down infrastructure that is expensive and slow to replace — belongs to concentrated industrial plant, not to any particular delivery vehicle.

October 7, 2023. Hamas' assault into southern Israel began with small commercial quadcopters flying ahead of them, dropping munitions on the generators powering communications towers and on the remotely operated weapon stations along the Gaza border, while sniper fire took out the surveillance cameras. The Middle East Institute describes the effect as leaving the soldiers monitoring the border from behind blinded by a loss of cellular signal and alarms, in the minutes before the barrier was breached at multiple points.[99] Its broader argument is that the failure was one of overreliance on technology, not of the technology itself. Substituting sensors and remote weapons for personnel created a single point of failure that a handful of cheap drones could exploit. The attack did not try to defeat the sensors' technical capability; it targeted the link between the sensors and the people monitoring them, which every detection system at section 11 also depends on.

Myanmar, 2021 onward. Since the coup, Myanmar's civil war has produced a well-documented case of drone warfare conducted almost entirely by parties with limited budgets and no state sponsor supplying purpose-built equipment. The Armed Conflict Location and Event Data Project has recorded more than 2,100 drone strike events by resistance groups across more than 600 locations, using commercial drones modified to carry small munitions. The military responded with jamming at major bases, requests to China to block dual-use component exports, and arrests of parts importers; ACLED recorded 1,134 distinct military airstrikes between January and May 2025, against 197 in 2023.[100] The lesson is tempo: a full cycle of innovation, countermeasure and counter-countermeasure that took NATO militaries years in earlier eras played out here, between poorly resourced belligerents, in two to three years.

One further conflict sits outside this paper's subject but explains why defence establishments stopped treating uncrewed aircraft as niche: Azerbaijan's 44-day campaign in Nagorno-Karabakh in 2020, in which large, state-supplied Bayraktar TB2 drones and Harop loitering munitions dismantled Armenia's largely Soviet-era air defence network and armoured

---

[96] Arab News, *Saudi Arabia's Defense Ministry displays Iranian…*, see reference 14.

[97] Congressional Research Service, "Attacks on Saudi Oil Facilities: Effects and Responses", see reference 45.

[98] Michael Knights and Conor Hiney, "Plugging the Gaps in Saudi Arabia's Air Defenses," The Washington Institute for Near East Policy, 25 September 2019, recording that Saudi batteries mostly faced east and lacked 360-degree coverage, and that legacy systems built against aircraft would struggle against smaller, slower cruise missiles and drones.

[99] Middle East Institute, "The October 7 Hamas attack: An Israeli overreliance on…", see reference 73.

[100] Armed Conflict Location & Event Data Project, "The war from the sky: How drone warfare is shaping the conflict in Myanmar," 2025.

formations in days, and which CSIS treats as a case study in the future of strike and defence.[101] Subsequent analysis cautions against reading it as a pure drone story, pointing to Armenian force structure, command failures and the absence of modern electronic warfare as equally causal.[102] That caution generalises across this chapter: in every case examined here, the drone exploited an existing weakness and did not create one.

6.5 A response that worked: Paris, 2024

The cases above are weighted toward failure, because failure generates investigation records. Planning from failure alone produces a distorted picture, so this section examines the best-documented instance of a counter-drone posture that did what it was designed to do.

Observed. For the 2024 Olympic and Paralympic Games, French authorities deployed a layered system built around PARADE, a modular French system from CS Group and Thales combining a 360-degree radar with an instrumented range of five kilometres, radio frequency detection and an electro-optical camera, feeding the Boreade command and control system. It was designed to distinguish aircraft between 100 grams and 25 kilograms from birds and other objects before jamming them onto a safe landing.[103] Around it sat Giraffe 1X air surveillance radar, handheld NEROD RF jamming rifles and AI-enabled sensor fusion. The French Ministry of Armed Forces recorded 88 aircraft interceptions and 85 drone remote pilots apprehended across the Games, and reported that most of those apprehended were not acting maliciously.[104] Testing beforehand had exposed the system's limits: in one exercise PARADE detected one of three hostile drones at 800 metres, and a defence consultant reviewing the trials identified dense urban terrain — where buildings, trees and monuments degrade radar — and swarm saturation as the unresolved problems.[105]

Assessment. The transferable lesson lies not in PARADE's performance but in the integration of four things that most sites hold separately or not at all: lawful authority to act, detection capable of producing a usable track, a decision arrangement that could resolve each track inside the time available, and trained operators empowered to make the call. Remove any one and the result changes, which is the three-factor argument at section 12.2 observed working rather than failing. Two further conditions helped and are hard to reproduce: a defined perimeter, and a defined duration. The system did not eliminate incursions but it was not designed to. It achieved its objective by enabling attribution and a significant reduction in ambiguity in the air picture.

Australian relevance. The event model transfers to Australian major events and is already in use: state police forces, working with Home Affairs and Defence, deployed comparable

---

[101] Center for Strategic and International Studies, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense."

[102] EVN Report, "Beyond the Drone Hype: Unpacking Nagorno-Karabakh's Real Lessons."

[103] Second Line of Defense, "The PARADE Anti-Drone System and the Paris Olympic Games," January 2024; and Breaking Defense, "France takes aim at unmanned systems, taking lessons from Paris Olympics," November 2024.

[104] Ministère des Armées, "JOP 24 — bilan de la sécurisation aérienne des Jeux Olympiques," 19 August 2024, and the ministry's closing statement of 11 September 2024, recording 88 aircraft interceptions and 85 drone remote pilots apprehended across the Games, most of them not acting maliciously.

[105] France 24, "Tests expose worrying flaws in France's anti-drone system for 2024 Olympics," 19 April 2024, reporting the Coubertin exercise results and the assessment of independent defence consultant Marc Chassillan on urban radar performance and swarm saturation.

detection at the 2024 Australian Open, the Australian Formula One Grand Prix, the MCG concerts, the ASEAN Summit and Land Forces 2024, and reported interdicting more drone pilots than ever before.[106] It also provides an initial blueprint from which to base further improvements on for future events such as the Brisbane 2032 Olympic Games. What does not transfer is the standing case. A permanent facility owned by a private operator has neither the jamming authority nor continuous police presence, which is why Part IV treats identification and investigation, rather than defeat, as the achievable objective for most readers.

6.6 Comparison and lessons

Table 3 sets the cases side by side before the conclusions are drawn from them.

Table 3: Case comparison and Australian transferability

Case	Environment	Drone class	Primary feature or failure	Consequence	Transfers to Australia?
Gatwick, 2018	Peacetime, commercial airport	Never established	No corroborating detection; no basis to declare the airspace clear	~30 hrs closed, ~£50m, no damage	**Directly.** The closest analogue to Australian conditions
October 7, 2023	Opening phase of an assault	Commercial quadcopter	Sensor-to-decision-maker link attacked, not the sensors	Border detection network blinded	**The mechanism does.** The setting does not
US sightings, 2024	Peacetime, nationwide	Mostly none identified	Ambiguity at national scale; authority stopping at the fence line	Political crisis, no confirmed act	**Directly**, including the communications failure
Spiderweb, 2025	Interstate war	FPV	Proximity model defeats strategic depth; assets parked in the open	Strategic aircraft struck at up to 4,000 km	**The proximity model does.** The state intelligence operation does not
European wave, 2025	Peacetime, multi-national	Never established	Countermeasures deployed by capable militaries with no result	Airports closed, alert postures raised	**Directly.** This is the peacetime scenario
Paris, 2024	Peacetime, major event	Commercial	Authority, detection, decision and response integrated	88 interceptions, 85 operators apprehended	**The event model does.** The standing case does not
Williamtown, 2026	Peacetime, Australian defence base	Never established	Authority in force, capability not brought to bear	Police referral; no identification	**It is Australia**
Myanmar, 2021–	Low-resource civil war	Modified commercial	Full innovation and counter-innovation cycle in 2–3 years	Sustained strike campaign	**The tempo does.** The conflict does not
Abqaiq, 2019	Regional confrontation	Larger, plus cruise missiles	Concentrated processing plant disabled by a few precise charges	~5% of global oil supply	**The infrastructure lesson only**

[106] Dedrone, "Australian Police protect major events from drone threats," describing deployments at the 2024 Australian Open, Australian Formula One Grand Prix, MCG concerts, the ASEAN Summit and Land Forces 2024.

Case	Environment	Drone class	Primary feature or failure	Consequence	Transfers to Australia?
Nagorno-Karabakh, 2020	Interstate war	Large, state-supplied	Air defence suppression at scale	Operational paralysis	**Context only.** Not a small-drone case

Seven conclusions carry forward from very different starting conditions: an interstate conventional war, a war of attrition, a covert special operation, a low-resource civil war, a non-state actor with no air force, a single day's opening assault, a commercial airport in a peaceful country, two waves of unexplained sightings, and one well-managed major event.

Low-cost drones can impose disproportionate costs on high-cost defensive systems. Commercial quadcopters disabled a Gaza border sensor network that had cost orders of magnitude more to build, and FPV airframes launched from trucks reached strategic aircraft four thousand kilometres from the launching country. The larger-aircraft cases make the same point at a different scale and are useful mainly for the cost arithmetic they generate.

Rear areas are not safe areas. Spiderweb, October 7 and both sighting waves demonstrate from different angles that garrison, rear-area and sensor infrastructure is exposed, and that distance from an active conflict is not, by itself, protection.

Jamming is a diminishing-returns countermeasure. Fibre-optic control and link-loss autonomy have both eroded it, and the European wave provided a public demonstration of a NATO military jamming five aircraft over a submarine base and bringing down none. Jamming is still relevant, but it is not the silver bullet that many militaries around the world currently rely on. This has direct legal implications in Australia (section 13.2), because jamming is also the capability Australian law most tightly restricts.

In many realistic peacetime scenarios, identification becomes the binding constraint once basic detection is available. Tower 22 failed at identification with sensors working. Gatwick failed at identification with no corroborating sensors at all. Paris apprehended 85 operators and found that most were not acting maliciously.

Attribution frequently does not arrive. Gatwick, the 2014 French nuclear overflights, the 2024 American wave, the 2025 European wave and the 2026 Williamtown incursions each closed without a publicly identified operator.

Ambiguity is itself the cost. Three of these cases produced severe economic, operational and political consequences without a confirmed hostile act. This is the finding that most directly transfers to Australian peacetime conditions, and it is developed at sections 9.2 and 9.6.

Where a response worked, it worked by converting ambiguity into identification. Paris did not defeat the drone problem, but it did turn 88 interceptions into 85 identified operators arrested. That is the achievable objective, and detection, evidence capture and referral are available to Australian organisations under existing law even though the jamming component that supported it is not.

Part III — Australian Risk

7. Australia's security environment

For most of its modern history, Australian defence and security planning has been able to treat geographic isolation as an asset: a wide moat that any adversary would need to cross before Australian territory, forces or infrastructure came within reach. Small drones are one of the few threat categories that meaningfully erodes the value of that moat. The point of employment does not need to be close to the sponsoring actor, only close to the target.

7.1 Strategic geography

Australia's coastline and its expanses of remote airspace remain genuinely protective against certain categories of threat. A long-range missile or crewed aircraft strike still requires an adversary with substantial reach and a willingness to be detected well before arrival.

Small drones sit outside that logic. The plausible drone-based threats to Australian assets involve local access, insider knowledge or short-range employment near the target, echoing the proximity-based model of Operation Spiderweb, not any scenario requiring a capability to be projected across thousands of kilometres of ocean.

A second-order effect runs the other way. Remoteness, which is protective against conventional threats, is actively unhelpful against this one. Writing in ASPI's *The Strategist*, DroneShield chief executive Oleg Vornik has argued that northern Australian installations are more exposed for the simple reason that remoteness means fewer people are present to spot anything.[107] The same argument applies to remote mine sites, pipeline infrastructure, pumping stations and offshore-supporting facilities.

In practical terms, Australia's geography does comparatively little to reduce the drone threat relative to the threats Australian planning has traditionally been built around. Security planning should be calibrated accordingly, and not on the assumption that distance provides a comparable layer of protection.

7.2 What counts as critical infrastructure

Australia has an authoritative framework for scoping what counts, and this paper uses it throughout. The *Security of Critical Infrastructure Act 2018* (Cth), substantially reformed in 2021 and 2022, covers eleven sectors and twenty-two asset classes[108]: energy, communications, data storage and processing, financial services and markets, water and sewerage, health care and medical, higher education and research, food and grocery, transport, space technology, and defence industry.[109]

---

[107] Oleg Vornik, chief executive of DroneShield, "Like the US, Australia remains badly unprepared for drone threats," Australian Strategic Policy Institute, *The Strategist*, 27 August 2024.

[108] Australian National Audit Office, *Administration of Critical Infrastructure Protection…*, see reference 28.

[109] Cyber and Infrastructure Security Centre, "Security of Critical Infrastructure Act 2018 —…", see reference 47.

As section 13.5 explains, the SOCI Act is the basis for legal obligations that already apply to many readers of this paper, including a risk management program requirement that expressly covers physical and personnel hazards as well as cyber ones, so a credible small-drone threat assessment fits inside an obligation most readers already carry.

7.3 The Australian incident record

Australian discussion of this topic still tends to treat it as an international problem. The domestic record no longer supports that.

Defence establishments. Between the 11th and 13th of July 2026, the Department of Defence confirmed multiple uncrewed aircraft in restricted airspace over RAAF Base Williamtown, and referred the matter to the New South Wales Police Counter-UAS Unit. Defence has not disclosed what counter-drone measures were used, or whether the aircraft were intercepted, identified or recovered.[110] The activity was reported over Newcastle Airport as well as the base. The two share an airfield, the civilian terminal operating on Defence land under a long-term lease.[111]

Minister for Defence Industry Pat Conroy confirmed the incident on August 10th, said the New South Wales Police investigation was "now complete", and declined to disclose its findings or the number of aircraft involved.[112] Ten days later police confirmed a second incursion into the restricted airspace in early August, said they were working with the ADF and partner agencies to identify the aircraft and their operators, and reported no arrests or charges in either episode.[113] The sequence matters more than either event. A confirmed incursion, an investigation described as complete, a second incursion within weeks, and no identification in either is the pattern this paper describes throughout, occurring at an Australian base hosting the F-35A fleet.

Conroy also confirmed the counter-drone investment set out at section 8.1 and the 2025 regulations permitting Defence to seize, disable or destroy a drone. Commentators including Dr Oleksandra Molloy identified the gap the episode exposed, that authority and fielded capability are not the same thing, and offered three readings of the activity, none of them established: intelligence collection, probing of Australian defences, or preparation.[114]

Aviation. In 2020 CASA publicly appealed for information after a pilot on approach reported a drone at approximately 1200 metres altitude over western Sydney, beneath the Sydney Airport approach path.[115] The Australian Federal Police and CASA have issued joint warnings about drone use around Cairns Airport.[116] Airservices Australia has gone to market for a drone

---

[110] Newcastle Herald, *RAAF Williamtown: drones reportedly breached…*, see reference 78.

[111] Royal Australian Air Force, "RAAF Base Williamtown," recording that Newcastle Airport operates from RAAF Base Williamtown under a lease with Defence, and that the base hosts the F-35A Lightning II squadrons of Air Combat Group.

[112] Newcastle Herald, *RAAF Williamtown: drones reportedly breached…*, see reference 78.

[113] ABC News, "Drones breach restricted airspace at Williamtown RAAF base," 20 August 2026, reporting the New South Wales Police confirmation of a second incursion in early August 2026, that investigations into both episodes were continuing with no arrests or charges, and Prime Minister Anthony Albanese's comment that it is "unsafe and dangerous to have drones around airspace."

[114] Australian Aviation, "Australia must learn from Williamtown drone incident…", see reference 22.

[115] Civil Aviation Safety Authority, "Help find rogue western Sydney drone," 2020, appealing for information after a pilot on approach to Sydney Airport reported a drone at approximately 1,200 metres altitude over western Sydney.

[116] Australian Federal Police, "AFP and CASA warn of drone usage around Cairns Airport."

surveillance system covering 29 controlled airports, citing increased drone activity in airport no-fly zones and particularly smaller micro-drones.[117]

Emergency services. Recreational drones grounded water-bombing aircraft at the Manypeaks fire in Western Australia in January 2025,[118] and at Esperance in 2019,[119] following a pattern that recurred through the 2019–20 fire season.

Corrections. Victoria recorded 97 drone-related security incidents between March and early November 2020, a 246% increase, following the suspension of prison visits.[120] Four Queensland high-security prisons were locked down after drones overflew all of them on a single afternoon.[121] A drone intercepted at Townsville Correctional Complex in May 2026 carried an estimated $1 million in contraband.[122]

Public events. In May 2026, 89 of the 1,000 drones in a professionally operated Vivid Sydney display fell from the sky, with 83 landing in Cockle Bay and six on boardwalks and a bridge. The operator attributed the failure to radio interference and the Australian Transport Safety Bureau opened an investigation; the following two nights' displays were grounded pending a safety assessment.[123]

> **Infrastructure analogue — not a drone incident.** Two subsea cables in the protection zone off Perth suffered faults in close succession over the weekend of 10–11 August 2026, prompting the AFP to receive a crime report and assess the matter; Australia has 16 subsea cables carrying 99% of its international communications.[124] No drone was involved and none is alleged. It is noted here only because it demonstrates the concentration and single-point-of-failure characteristics discussed at section 8.7, and because the investigative and attribution difficulties it produced are the same ones that follow an unexplained drone incursion.

None of the drone incidents above individually constitutes a national emergency. Taken together, they describe an environment in which unauthorised drone activity around sensitive Australian sites is routine, response capability is thin outside Defence and the major airports, and the operators are almost never identified.

8. Where the exposure sits

The SOCI Act covers eleven sectors and twenty-two asset classes, and every one of them has some drone exposure, although no equal. What follows sets out the six areas where the combination of what is physically exposed, what an interruption costs, and what the Australian

[117] Unmanned Airspace, "Airservices Australia publishes tender for drone…", see reference 106.
[118] ABC News, "Anger after drones ground water bombers at Manypeaks…", see reference 2.
[119] ABC News, "Drones cause waterbombing to stop at bushfire in WA's south-east," 3 March 2019.
[120] Australian Aviation, "Drone incidents at Victorian prisons rise 250%", see reference 23.
[121] Queensland Corrective Services, "High security prisons locked down after drone incursion.", see reference 85.
[122] ABC News, "Drone with $1 million worth of contraband intercepted…", see reference 3.
[123] ABC News, "Why drones fell from the sky during Sydney's Vivid…", see reference 9.
[124] ABC News, "Two subsea communication cables damaged off Perth coast in 'concerning development'," 11 August 2026.

record already shows makes the case most clearly. It is a description of where the problem is concentrated, not a rating any site should substitute for its own assessment.

8.1 The defence estate

The parallel to Operation Spiderweb applies to Australia's defence estate without requiring speculation about specific vulnerabilities. Any air force or navy that concentrates high-value assets in fixed, known locations shares something with what Russian planners assumed about their rear-area bases before June 2025.

Three current developments make this concrete. **RAAF Base Tindal** has been modernised with United States funding to support rotational bomber deployments, with expanded aircraft parking and associated infrastructure; a $355 million tranche of hangars, working accommodation and airfield pavements was reported complete in January 2026.[125] [126] **HMAS Stirling**, at Garden Island south of Perth, is the subject of an investment of up to $8 billion to prepare it to host United Kingdom and United States nuclear-powered submarines under Submarine Rotational Force–West from 2027; the Australian Submarine Agency's published description of the works includes a "base-wide uplift to physical security."[127] **RAAF Base Williamtown** hosts Australia's F-35A and E-7A Wedgetail fleets and was the site of the July 2026 incursions described above.[128]

The analytical point does not require further facility detail, and this paper deliberately does not provide any. Fixed, high-value assets, multi-year construction programs and allied activity together create a security-by-design opportunity that is available while the works are under way and gone once they are complete.

Defence's own response has accelerated considerably over the past two years. The *Defence Amendment (Counter-UxS Measures) Regulations 2025*, registered in December 2025 and announced the following month, expanded Defence's authority to detect and disable or destroy drones suspected of posing a threat to ADF assets, and established a Counter Small Uncrewed Aerial Systems industry panel of 28 companies under Project LAND 156.[129] In April 2026 it committed up to $7 billion over a decade to counter-drone capability, within up to $22 billion for drone, counter-drone and autonomous systems under the 2026 Integrated Investment Program.[130] Exercise Southern Arrow 25 demonstrated live-fire defeat of small uncrewed aircraft under an Australian systems integrator in December 2025.[131]

---

[125] The War Zone, "Australian Airbase Gets Upgrades For American Bomber Deployments," 31 October 2022, describing the United States-funded apron expansion and squadron facilities then in design.

[126] ABC News, "Albanese government turns defence sights north, completing $355m upgrade to RAAF Base Tindal," 28 January 2026.

[127] Australian Submarine Agency, "Upgrades at HMAS Stirling pave the way for Submarine Rotational Force-West."

[128] Unmanned Airspace, "Multiple unidentified drones reported over Australian F-35 base," reporting the Department of Defence statement that multiple uncrewed aircraft systems were confirmed in restricted airspace over RAAF Base Williamtown on 11–13 July 2026 and that the incidents were referred to the New South Wales Police Counter-UAS Unit.

[129] The Hon Pat Conroy MP and the Hon Peter Khalil MP, "Government boosts response to drone threats," 29 January 2026, announcing the *Defence Amendment (Counter-UxS Measures) Regulations 2025* and the LAND 156 counter-small-UAS industry panel.

[130] The Hon Pat Conroy MP, "Albanese Government to invest up to $7 billion in…", see reference 98.

[131] Department of Defence, "Army tests counter-drone technology," 24 December 2025, describing Exercise Southern Arrow at Cultana and its live-fire demonstration as the first iteration of the LAND 156 schedule.

8.2 Aviation

Gatwick is the global reference point, and the 2025 European wave demonstrated the same effect distributed across a network. Australia's capital city airports share Gatwick's essential characteristics: high traffic density, a hard safety requirement to suspend operations on a credible sighting, no lawful mitigation capability held by the operator, and a very high cost per hour of closure. Airservices Australia has gone to market for a drone surveillance capability covering 29 controlled airports, which would address the detection gap that made Gatwick's closure open-ended.[132] Detection does not shorten a closure by itself, but it is what allows an airport to declare the airspace clear, which at Gatwick took three days.

Two Australian variations deserve naming. Regional airports carry the same regulatory obligations and effectively none of the detection capability, and have fewer options for holding, diversion or parallel operations when something is reported. And the aeromedical and firefighting fleets (the Royal Flying Doctor Service, state air ambulances, water bombers) operate in remote areas and hospital helipads in exactly the low-altitude regime where small drones fly, often at night, in areas with no airspace surveillance whatsoever. Recreational drones have already grounded aerial firefighting in Australia more than once, but that precaution will not stop the fire.

8.3 Ports and maritime infrastructure

Australian export infrastructure is concentrated to a degree that has few international parallels. Pilbara Ports is the world's largest bulk export port authority; Dampier and Port Hedland together handle approximately 77% of Australia's, and 42% of the world's, iron ore trade,[133] which puts a disruption at Port Hedland well outside the category of a local commercial event.

Ports are physically large, mostly outdoors, adjacent to public water and public roads, and operate continuously. While there are undoubtedly assets that, if damaged, could have an outsized impact, the sheer size and materials at the site do offer some inherent protection against small drones.

8.4 Energy

Energy carries the widest cascading footprint of any sector here. The Cyber and Infrastructure Security Centre's own risk review notes that the sector's assets are geographically dispersed and often remote, that new renewable infrastructure is a prime target, that physical security threats have historically been uncommon in Australia but that geopolitical tensions are changing that calculus, and that significant disruption in one sector will affect others, with loss of power capable of producing loss of life through its effects on health care.[134]

---

[132] Unmanned Airspace, "Airservices Australia publishes tender for drone…", see reference 106.

[133] Ports Australia, "Pilbara Ports," describing Dampier and Port Hedland as handling approximately 77 percent of Australia's and 42 percent of the world's iron ore trade.

[134] Cyber and Infrastructure Security Centre, version 2.0, February 2026, *Critical Infrastructure Annual Risk Review — Energy Sector*.

High-voltage transmission is the classic case of a network where a small number of components carry disproportionate load. Large power transformers are individually expensive, have long lead times, are frequently not held as spares, and sit outdoors inside a fenced compound with no overhead protection. The target that matters may not be the primary plant at all but the protection and control cabinets and the communications link back to the control room: the pattern demonstrated on 7 October 2023, discussed at section 6.4.

Western Australia's North West Shelf and the Queensland LNG trains on Curtis Island are the Australian assets that most closely resemble Abqaiq in structure: concentrated processing infrastructure, individually significant to global supply, expensive and slow to replace or route around. Australian facilities do not face Saudi Arabia's 2019 threat environment and the aircraft used there were larger than anything considered here, but the vulnerability Abqaiq exposed is a property of concentrated industrial plant and not of any particular delivery vehicle, and a small explosive payload placed on the right cabinet could be enough to interrupt production.

8.5 Correctional facilities

Corrections is the Australian sector with the most extensive, best-documented and fastest-growing drone problem, and it is the one that has been forced to develop practical responses first.

Victoria recorded 97 drone-related security incidents between March and early November 2020, a 246% increase on the prior year, in freedom-of-information data obtained by *The Age* and reported by *Australian Aviation*; the spike followed the suspension of prison visits due to COVID-19, with airdrops reported to contain heroin and other street drugs.[135] In Queensland, four high-security prisons were locked down after drones overflew all four perimeters on a single Sunday afternoon.[136] At Capricornia Correctional Centre on Christmas Day 2019, two packages were dropped into an exercise yard, the prisoner who caught one reported the next day that he had swallowed an unknown substance and was hospitalised, and all non-essential movement within the centre ceased for the day.[137] In May 2026, a drone intercepted at Townsville Correctional Complex carried drugs, syringes and a mobile phone worth an estimated $1 million.[138]

Three things make this instructive for every other sector. The cost is almost entirely operational rather than physical: nothing was damaged in any of those incidents; what was consumed was lockdown time, staff hours and search effort. The response is a whole-of-facility one, because it is necessarily precautionary and does not wait for confirmation of what was delivered. Additionally, corrections is where the detection-without-mitigation asymmetry is most visible: even with detection installed, an Australian prison can watch a drone approach, watch it drop, and do nothing to it. Every other sector in this chapter will eventually find itself in that position; corrections has been there longest, which is also why it has the clearest legal

[135] Australian Aviation, "Drone incidents at Victorian prisons rise 250%", see reference 23.

[136] Queensland Corrective Services, "High security prisons locked down after drone incursion.", see reference 85.

[137] Queensland Corrective Services, "Drone incursion sends Capricornia into lockdown," December 2019.

[138] ABC News, "Drone with $1 million worth of contraband intercepted…", see reference 3.

framework. Victoria has banned flying within 120 metres of the boundary of around twenty correctional facilities since 2018, with a maximum penalty of two years' imprisonment,[139] and Queensland applies the same two-year maximum to being caught with a drone at a correctional facility, though without an equivalent exclusion zone.[140]

8.6 Population centres, stadiums and major events

Australian central business districts, stadiums and major public events present exposure at both ends of the severity spectrum: casualties on the extreme end, disruption or panic from a non-hostile incursion at the far more common end.

Australian police have built operational experience here. Dedrone, the vendor involved, reports detection systems deployed with state police forces in cooperation with Home Affairs and Defence at 2024 events including the Australian Open, the Formula One Grand Prix, the Eras Tour concerts at the MCG, the ASEAN Summit and Land Forces 2024, and that police interdicted more drone pilots than ever before.[141] This is the most capable counter-drone practice routinely deployed in Australian civilian settings, and why it works is instructive: it is deployed by police, who hold the ACMA exemption, at events with a defined perimeter and a defined duration. None of those three conditions holds for a permanent venue owned by a private operator.

Authorised drone displays are a separate and growing exposure. The Vivid Sydney failure in May 2026, in which 89 of 1,000 drones fell into Cockle Bay and onto public boardwalks and the operator attributed the failure to radio interference, is a reminder that for an event organiser the airspace problem is not confined to malicious operators.[142]

8.7 The sectors not treated here

Leaving a sector out of this chapter is a statement about where the argument is clearest, not about where risk is absent. Water utilities hold a consequence profile in which physical damage to a pump is recoverable and public confidence in a metropolitan supply is not. Communications and data have low reach and very high concentration: subsea cables are not exposed to drones, but landing stations, exchanges and the generator, fuel and cooling plant on a data centre roof all are, and a data centre's security model is built around who walks in the door. Hospitals carry a modest direct exposure at helipads and rooftop plant, and a serious indirect one through the electricity sector above.

---

[139] Department of Justice and Community Safety Victoria, "Drone ban near Victorian correctional and youth justice facilities," in force from 1 February 2018.

[140] The Hon Mark Ryan MP, Queensland Minister for Police and Corrective Services, "New regulation brings down drones," 15 February 2018, recording a maximum penalty of two years' imprisonment or a $12,615 fine for being caught with a drone at a correctional facility.

[141] Dedrone, "Australian Police protect major events from drone threats", see reference 51.

[142] ABC News, "Why drones fell from the sky during Sydney's Vivid…", see reference 9.

9. Consequence analysis

9.1 Physical damage

The physical damage a small drone can cause spans a wide range, and the appropriate response to each end of it differs. At the lower end sits a single strike on a vehicle, a piece of equipment or a section of fencing: real, but localised and usually recoverable in days. At the upper end sits Operation Spiderweb. Between them lies most of what this paper is concerned with: damage severe enough to matter to an organisation's operations and finances but well short of the extremes that dominate international reporting.

A risk assessment built only around worst-case scenarios will under-invest in the much larger number of moderate-severity incidents an organisation is more likely to experience. The answer to a moderate incident is usually detection, evidence capture and a rehearsed response, not an interceptor.

9.2 Operational disruption

Disruption frequently exceeds physical damage as the dominant cost. Gatwick involved no physical damage and still produced the costs set out at section 6.2. The Red Sea campaign did not need to destroy half the cargo to halve Suez transits; the credible threat was sufficient.[143] Four Queensland prisons locked down and searched in full, and nothing was found.[144]

In each case the disruption was the effect, not a side consequence of it, and the distinction should be built explicitly into incident and continuity planning at section 14.5.

9.3 Economic consequences

Tables 4 and 5 separate two things that are often conflated. Table 4 records what selected incidents cost. Table 5 records what governments have since committed to counter-drone capability.

Table 4: Observed consequences of selected incidents

Incident	Reported consequence	Source and notes
Gatwick (2018)	~£50 million to airport and airlines, easyJet alone ~£15 million; ~1,000 flights and ~140,000 passengers affected; ~£1 million in policing costs	Airline disclosure, police records and contemporaneous reporting. No physical damage occurred
Red Sea campaign (2023–)	Suez transits fell from more than 26,000 ships (2023) to 13,213 (2024); canal revenue fell from US$10.3bn to US$4bn, about 61%	Suez Canal Authority figures. Recurring rather than one-off; excludes freight and war-risk insurance costs borne by shippers
Abqaiq–Khurais (2019)	5.7 million barrels a day disrupted, over half of Saudi output and about 5% of global supply	Saudi official figures. Larger aircraft plus cruise missiles, not the class this paper addresses; included for the infrastructure lesson
Victorian prisons (2020)	97 drone-related security incidents in roughly eight months, a 246% increase	Freedom-of-information data; excludes lockdown, search and staff-time costs, which are not published

[143] Euronews, "Egypt's Suez Canal revenue fell sharply in 2024 on…", see reference 63.

[144] Queensland Corrective Services, "High security prisons locked down after drone incursion.", see reference 85.

Incident	Reported consequence	Source and notes
Operation Spiderweb (2025)	US$7 billion claimed by Ukraine; independent assessments materially lower, some as low as 10–13 aircraft destroyed; Significant regardless	Belligerent claim, partially corroborated by imagery analysis and contested by allied assessment. See section 6.1.1

The pattern across the first four rows is the one identified at section 3.2: the attacker's outlay is a small fraction of the resulting cost, however that cost is measured. What the table cannot show also matters. Every figure here is a reported direct cost. None captures the management time, reputational effect or forgone activity that follows an incident, and in the disruption cases those are likely to be substantial.

Table 5: Recent counter-drone investment

Programme	Commitment	Notes
Australia — counter-drone capability	Up to $7 billion over a decade	Within up to $22 billion for drone, counter-drone and autonomous systems, 2026 Integrated Investment Program
Australia — Project LAND 156	Standing offer panel of 28 companies	Counter-small-UAS capability for Defence and other Commonwealth agencies
Australia — Airservices drone surveillance	Network covering 29 controlled airports	Procured for aviation safety purposes
Belgium — counter-drone package	€50 million	Approved 8 November 2025, four days into the intensified phase of the incursions
Victoria — corrections detection	$420,000	Following the 2020 increase in prison drone incidents
Gatwick — post-incident detection	£5 million	Installed after the December 2018 closure

9.4 National security consequences

Some incidents carry a strategic consequence that outlasts the repair bill. Analysts examining Operation Spiderweb have argued that its significance lay less in the aircraft destroyed than in what it did to Russian confidence in its own strategic depth, which cannot be restored as quickly as physical damage can be repaired. Rebuilding it requires investment in detection, dispersal and hardening across an entire estate. For Ukraine, the added benefit of forcing Russian bombers to further disperse is not insignificant with further flight hours on aging airframes and complicating the maintenance and logistical footprints these platforms require.

For Australian defence planning this is the category that most repays attention in advance. A single successful incident against the Australian defence estate, even a moderate one in physical terms, would carry a deterrence and alliance-confidence cost out of proportion to the damage, and would do so at precisely the moment when bases like Tindal are hosting allied strategic assets.

9.5 Cascading effects

Second and third-order effects frequently exceed the direct consequences and are correspondingly easy to underestimate. The CISC's own risk review makes the general case: the energy sector is both an upstream provider and a downstream consumer, it has a strong nexus

with communications in both directions, and disruption in one sector will affect others, with loss of power capable of producing loss of life through effects on health care.[145]

The practical instruction for a risk assessment is to ask not only what would be damaged, but what depends on what would be damaged. In Australian conditions that second question frequently leads to a small number of remote, unstaffed assets (a substation, a pumping station, a cable landing station, a rail bridge, etc.) that no one has assessed for aerial exposure because no one previously needed to.

9.6 Public confidence and psychological consequences

The harm from small drones is not purely physical, and this section closes on that deliberately, because it is the consequence category most often left out of a conventional risk assessment.

Three of the cases in Part II produced severe political, economic and public-confidence consequences without a confirmed hostile act being established at all. A fourth, at Williamtown, produced a month of unanswered public questions from a single confirmed detection. The transferable finding is that the confidence cost of a drone incident is not proportional to the physical damage involved, and may not require any physical damage at all.

Communication is key in these situations. The ability to say quickly and credibly what is and is not known matters more, in most realistic Australian scenarios, than the ability to bring an aircraft down. And the standard to aim for is not certainty, which will rarely be available, but consistency; the 2024 United States wave did much of its damage to public confidence through shifting official explanations rather than through the sightings themselves.

[145] Cyber and Infrastructure Security Centre, *Critical Infrastructure Annual Risk Review — Energy Sector*, see reference 48.

Part IV — Protecting Against the Threat

10. Counter-drone principles

Before examining specific technologies, this section sets out the doctrine that should shape how they are combined, because no single sensor or effector reliably defeats this threat on its own. Six principles recur throughout the rest of Part IV.

10.1 Layered defence and defence in depth

Counter-drone doctrine borrows directly from integrated air and missile defence. An effective system combines multiple overlapping sensor and effector types (radar, radio frequency, electro-optical and thermal, acoustic, and whatever response options are lawfully available) and also builds redundancy into each stage of the chain that runs detect, track, identify, decide, respond and adapt, so that a failure or delay at one stage does not mean total failure.

These are distinct ideas and organisations routinely buy the first while neglecting the second. Layering is diversity of sensor and effector types; depth is redundancy along the chain connecting them. October 7 (section 6.4) is what excellent layering with no depth looks like: the sensors worked, and the link between them and the people who needed to act did not.

The Paris 2024 deployment examined at section 6.5 illustrates both principles working together: diverse sensor types feeding one command arrangement, with trained operators making the call on each track. It is also instructive for what pre-Games testing and analysis identified as unsolved (radar performance in dense urban terrain, and swarm saturation), which is a more useful disclosure than most published counter-drone material contains.[146]

10.2 Detection and decision first

Detection alone is half the principle, and the paper's own evidence shows why. Tower 22 had the tracks on screen. Williamtown produced a confirmed detection, a police referral and no interception. Detection that does not resolve into an identification, and an identification that does not resolve into an authorised decision, leaves an organisation exactly where it started, having spent money.

The principle is therefore *detection and decision*, in that order and both before response. Two supporting reasons. A response system is of limited use without reliable cueing. And, as section 13.2 explains, Australian law permits considerably more latitude for detection than for active response, which makes detection and the decision architecture around it the parts of the layered model most readers of this paper can actually build.

There is a second, less obvious half to the detection argument: you cannot declare a threat over if you never saw it begin. Without corroborating detection an airport could neither respond nor confirm when it was safe to reopen, and a single evening's sightings consumed three days.

[146] France 24, "Tests expose worrying flaws in France's anti-drone…", see reference 69.

Response latency. One variable connects the two halves. Response latency is the interval between reliable detection and the point at which a response must occur to be effective. It is set by the threat's approach speed and by the organisation's own decision chain, not by the sensor. A camera drone loitering at a fence line may allow twenty minutes. A fast FPV airframe approaching from outside the perimeter compresses the same chain into seconds: a window shorter than most civilian escalation procedures are written for, and shorter than the time it takes to reach a decision-maker by telephone. An organisation that has not calculated its own response latency for each realistic approach profile has not finished the analysis, and the number it arrives at will usually argue for pre-delegated authority.

10.3 Cost per engagement

The cost-exchange problem introduced at section 3.2 is the central constraint shaping procurement in this space.

The only reliable published figures come from a larger class of aircraft, which makes them conservative for our purposes, not directly applicable. CSIS analysis puts a Shahed-type one-way attack drone at around US$35,000 against roughly US$1 million for a NASAMS engagement and over US$3 million for a Patriot PAC-3.[147] Substituting the aircraft an Australian site would actually see (a commercial quadcopter or self-built FPV airframe costing between a few hundred and a few thousand dollars) would move the ratio further in the attacker's favour, though no equivalent published engagement-cost data exists at that end of the spectrum. Additionally, it is not realistically suggested that a Patriot or NASAMS missile be used against a small FPV drone (for which it was never designed), however this example illustrates how the defender is now bearing greater costs than attackers.

Four costs have to be separated, because conflating them is how procurement decisions go wrong. **Platform cost** is what the attacker spends on the airframe. **System cost** is what the defender spends on sensors, integration and the people who watch them, most of which is incurred whether or not an engagement ever occurs. **Cost per engagement** is the marginal cost of defeating one aircraft, which is where directed energy differs most sharply from kinetic options. **Cost of failure** is the consequence at section 9, and for the disruption scenarios that dominate Australian risk it is usually the largest of the four by a wide margin.

That arithmetic is the single fact that most explains the current wave of investment in lower cost-per-engagement alternatives: net-capture interceptors, reusable interceptors, and directed-energy systems whose marginal cost per engagement approaches the cost of electricity. It also explains why an Australian civilian operator should be sceptical of any counter-drone proposal whose economics only work against a small number of engagements.

10.4 Technology neutrality

Committing heavily to a single detection or defeat modality is a documented and recurring mistake, because the threat adapts faster than any one technology remains dominant.

[147] Center for Strategic and International Studies, "Calculating the Cost-Effectiveness of Russia's Drone…", see reference 35.

The clearest example is the jamming-to-fibre-to-microwave sequence described at section 2.7. An organisation that built its entire counter-drone posture around jamming five years ago would, without updates, now be facing a materially different threat than the one it planned for; in a European context, it would have watched a French marine unit jam five drones over a ballistic missile submarine base and bring down none of them.[148]

Technology neutrality means building a program around outcomes and layered redundancy, and not around a specific product or technique. Stated as a procurement principle: **specify the required outcome, not the preferred technology.** In practice that means writing requirements against

- probability of detection, against a stated target class and flight profile;
- classification confidence, and what the system does below the threshold;
- time from first detection to operator alert;
- coverage geometry, stated separately from performance;
- false-alarm rate at the operating threshold, and the staffing that rate implies;
- availability and uptime, accounting for the weather the site actually gets;
- whether third-party sensors can be added, and on what terms;
- graceful degradation when an input is lost.

Technology selection then follows from the requirement, and can be changed later without rewriting it.

10.5 Security by design

The strongest form of counter-drone investment is made before a facility is built. This extends the logic of crime prevention through environmental design into the airspace domain.

Sensor siting, buffer zones and standoff, overhead protection for critical outdoor plant, and the dispersal or concealment of high-value assets are all dramatically cheaper and more effective when designed in from the outset. Another benefit to considering overhead protection is the impact this would have on satellite imagery, something ubiquitous in intelligence gathering. Australia has a live example at national scale in the HMAS Stirling program, whose published scope of works includes a base-wide uplift to physical security.[149] For most readers the equivalent opportunity is smaller but just as real: any capital works program, plant replacement or site expansion currently in design is an opportunity to place critical equipment where it is not overhead-accessible, at a marginal cost close to zero.

10.6 Assume you will not know who it is

This principle rarely appears in counter-drone literature and it should. Almost every peacetime case examined in Part II closed without a publicly identified operator, and Australian defence and corrections incidents follow the same pattern. The design consequence is that every

[148] The War Zone, “Nuclear Submarine Base Drone Incursion Prompts French…”, see reference 103.

[149] Australian Submarine Agency, “Upgrades at HMAS Stirling pave the way for Submarine…”, see reference 34.

decision threshold, escalation trigger and communications position must be executable on observed behaviour alone.

11. Detection technologies

This section covers what each detection modality does well, what it does poorly, and where it fails. One factor that cannot be overstated is that detection is key – nothing can be done if nothing is detected. Figure 3 shows comparisons between commonly available detection technologies at a glance and Table 6 summarises them; the discussion that follows explains the trade-offs that matter when combining them.

Coverage is not performance. Before the detail, one distinction that procurement documents routinely collapse. *Detection coverage* is geometric: the volume of airspace a sensor is positioned to observe. *Detection performance* is probabilistic: how reliably it registers a particular target, of a particular size, on a particular flight profile, in particular conditions. A system can cover a site completely and still miss a two-kilogram airframe approaching low out of ground clutter in light rain. Vendor specifications describe coverage far more often than they describe performance, and the two are quoted in the same breath. A specification that asks for a detection radius has bought coverage; one that asks for probability of detection against a stated target class, at a stated false-alarm rate, in stated conditions, has bought performance, which is harder to write and considerably harder to evaluate and satisfy.

A survey of counter-drone systems found that 53% of commercial solutions rely on a single detection technology, which the layering principle says will not be sufficient on its own, against 23% using four or more; RF monitoring appears in 64% of systems, radar in 55%, visible-light cameras in 47%, thermal in 35%, acoustic in 10% and lidar in 4%.[150]

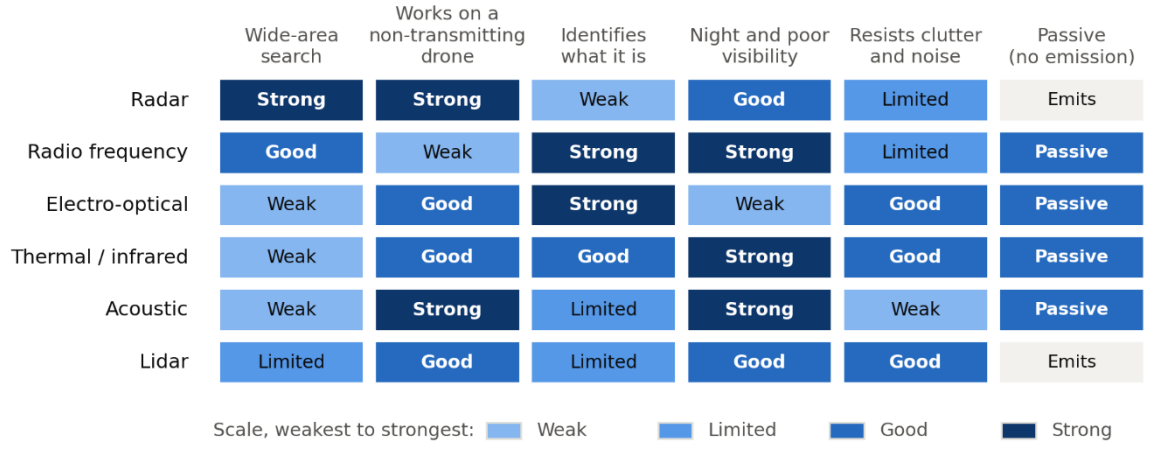

Figure 3: Detection modality comparison. No modality is strong across the row, and the weaknesses are correlated — fog degrades three at once. Every cell is labelled and the scale is defined in the legend; passivity is shown as the binary property it is.

[150] "Standardized Evaluation of Counter-Drone Systems: Methods, Technologies, and Performance Metrics," *Drones*, vol. 9, no. 5, 2025.

Table 6: Detection modality trade-offs

Modality	Principal strengths	Principal limitations	Typical role
Radar	Works day and night and in moderate weather; gives range, altitude and radial velocity; wide-area coverage; can track many targets at once	Poor against very low radar cross-section targets; degraded by heavy rain, fog and snow; struggles to separate drones from birds; clutter in urban and vegetated terrain; is an active emitter, so it can itself be detected; usually requires a transmitter licence	Primary wide-area search and cueing
Radio frequency	Passive, so no emission and no licence; can detect where visual and radar line of sight is obstructed; can often identify make, model and sometimes operator location; low cost	Blind to non-transmitting drones, including pre-programmed autonomous and fibre-optic-controlled types; high false alarm rates in RF-dense urban environments; struggles with encrypted or non-standard protocols and with modified airframes; typically short range	Primary detection and identification where the threat still uses RF
Electro-optical (visible)	High spatial resolution; imagery is directly interpretable by an operator and usable as evidence; passive; supports automated image classification	Highly dependent on ambient light; degraded by haze, fog and precipitation; narrow field of view at long range; poor as a search sensor on its own; high false alarm rate unsupported	Cued visual confirmation and evidence capture
Thermal / infrared	Works in complete darkness; less affected by smoke and camouflage; detects motor and battery heat signatures	Degraded by heavy rain, dense fog and high ambient temperature reducing contrast; lower spatial resolution than visible cameras; narrow field of view at range	Cued confirmation at night and in poor visibility
Acoustic	Fully passive; does not require a clear line of sight; works against non-transmitting drones; compact and rapidly deployable	Very short range, typically a few hundred metres and commonly cited at 300–500 m; masked by wind, traffic and industrial noise; poor in exactly the noisy environments most industrial sites present	Gap-filling, perimeter alerting, and coverage of dead zones
Lidar	High-precision three-dimensional positioning; effective in cluttered environments	Active emitter; degraded by fog, rain and snow; eye-safety constraints limit power and therefore range; rare in fielded systems	Niche, short-range precision tracking

Sources: standardised counter-drone system evaluation literature and industry technical guidance.[151] [152]

11.1 Radar

Conventional air surveillance radar was designed to track aircraft, not this class of target. A small drone's low radar cross-section, low altitude and low speed place it in almost exactly the band that legacy systems are engineered to filter out as bird and clutter noise. That has produced a distinct product category tuned to separate a drone's flight signature from a bird's, but even purpose-built radar struggles in dense urban terrain, as testing prior to the Olympic Games in France demonstrated.[153]

Three notes for an Australian buyer. Radar is an active emitter, so it can be detected and, in principle, avoided, and it usually requires an ACMA transmitter licence. Vendor performance

[151] "Standardized Evaluation of Counter-Drone Systems…", see reference 93.

[152] Robin Radar Systems, "10 Types of Counter-Drone Technology to Detect and Stop Drones Today," vendor technical guidance; the performance ranges quoted are the manufacturer's.

[153] France 24, "Tests expose worrying flaws in France's anti-drone…", see reference 69.

figures are almost always quoted for a specified target size in specified conditions, and the same system against a smaller airframe in rain will perform very differently. And radar typically reports that something is there, not what it is, beyond an estimation of size.

11.2 Radio frequency detection

Passive RF detection listens for the signals passing between a drone and its operator, allowing a system to detect, locate and sometimes also identify the aircraft's make and model, and in many cases the operator's position. That last capability is operationally significant in Australia, because locating the operator is the primary enforcement pathway available to most organisations.

Its central limitation is clear: it cannot detect an aircraft that is not transmitting. A pre-programmed autonomous flight, fibre-optic-controlled drone, or a drone operating outside standard RF frequency standards (e.g. via mobile phone towers) and as those control modes spread, RF's value as a standalone layer is dimished. Its second limitation matters more day to day. In an RF-dense environment (a city, a port, an industrial site with extensive telemetry) false alarm rates are high.[154] An organisation that installs RF detection without resourcing the resulting alert volume will train its own staff to ignore it, leaving the site worse off than if it had installed nothing.

11.3 Electro-optical and thermal systems

Camera-based detection provides what radar and RF cannot: visual confirmation that a track is a drone and not a bird, and a basis for classifying what kind and whether it is carrying anything. It is almost always cued rather than searching (a camera slews to a bearing radar or RF has already produced), and electro-optical and thermal sensors are near-universally paired in one gimbal so that the same function works at night.

The under-appreciated value of this layer is evidentiary, not operational. Where lawful mitigation is largely unavailable, the realistic outcome of an incursion is an investigation and possibly a prosecution. Imagery is what makes that possible, and it is also what allows an organisation to state publicly and defensibly what happened, which section 9.6 identifies as a primary control.

11.4 Acoustic sensors

Acoustic detection listens for the sound signature a drone's rotors generate. It is fully passive, does not depend on a clear line of sight, and (the property that matters most) works against an aircraft with no RF emissions at all, which is the specific gap that fibre-optic and autonomous control open. Its effect is directional: terrain, wind direction and background noise all shape what it will hear and from where. Its limitation is range: effective detection is a few hundred metres under ideal conditions,[155] with experimental work putting most machine-learning

[154] "Standardized Evaluation of Counter-Drone Systems…", see reference 93.

[155] "Standardized Evaluation of Counter-Drone Systems…", see reference 93.

detectors at around 300 metres and a deep-learning detector at 500,[156] and wind, traffic or machinery noise masks the signature. For a quiet rural site this is a genuinely useful layer; for a working port or processing plant it is close to useless in isolation. It appears in about 10% of fielded systems.[157] Acoustic sensors are also an illustration of how creativity and innovation from different areas can result in novel technologies. A concept to use acoustics to detect a mosquito in flight and shoot it with a laser became DroneShield, a well-known Australian counter-UAS company.[158] [159]

11.5 Sensor fusion

No single detection technology in the table above is sufficient alone. Each carries specific blind spots and a meaningful false positive and negative rate. The point that matters most for system design is that those blind spots are accounted for by a different sensor type. Fog degrades electro-optical, thermal and lidar together. An autonomous, non-transmitting drone operating at night in wind can reduce the effectiveness of RF, acoustic and electro-optical detection simultaneously.

Modern systems address this by fusing radar, RF, electro-optical, thermal and acoustic data into a single recognised air picture, cross-referencing detections across sensor types to raise confidence before an alert reaches a human operator. The technical approaches vary: AI-based fusion that dynamically weights sensor contributions by context, adaptive Kalman filtering, interacting multiple model filters, Bayesian and particle methods for handling multiple targets and ambiguous observations, and Dempster–Shafer methods that return belief intervals rather than point estimates.[160] The distinction matters less to a buyer than what it delivers, which is a reduction in false alarms to a level an operator can actually work with.

Two buying implications follow, and the first matters more than the choice of algorithm. Fusion should be specified as an **integration requirement** and not as a product feature: the question to put to a supplier is not which fusion technique it uses but whether the system will accept a sensor it did not ship with, including one bought three years from now, and what happens to the recognised air picture when one input fails. Graceful degradation is part of the same requirement. And because 53%of the market is single-modality,[161] a procurement that does not specify fusion explicitly will probably not get it.

---

[156] Tejera-Berengue et al., "Analysis of Distance and Environmental Impact on UAV Acoustic Detection," *Electronics* 13, no. 3 (2024): 643, reporting effective acoustic detection to about 300 metres for most machine-learning detectors and 500 metres for a deep-learning detector, degraded by spectrally similar background noise.

[157] "Standardized Evaluation of Counter-Drone Systems…", see reference 93.

[158] *Forbes Australia*, "How DroneShield went from zapping mosquitos to dropping drones."

[159] DroneShield Limited, *Annual Report for the Year Ended 31 December 2025*, recording a Sydney registered office, distribution across more than seventy countries, the June 2016 ASX listing and Oleg Vornik's appointment as chief executive in January 2017.

[160] "Standardized Evaluation of Counter-Drone Systems…", see reference 93.

[161] "Standardized Evaluation of Counter-Drone Systems…", see reference 93.

11.6 Artificial intelligence in detection

AI's role on the detection side is automated classification: distinguishing drone from bird from aircraft, reducing operator burden and cutting false alarm rates. Classification between drones and birds is genuinely difficult, and it is where most of the practical benefit sits.

It should be read as one half of a two-sided contest, not as a solution. The same category of technique that lets a detection system classify a track more reliably is being applied, as section 2.6 described, by developers seeking to guide a drone past that classification or to complete an engagement autonomously after the operator's link is severed. Detection AI does not merely need to keep pace with the raw threat; it needs to keep pace with attacker AI, which is a harder and more open-ended problem than static pattern recognition.

There is also a governance dimension. An AI classifier that produces a confidence score is making a recommendation, not a decision, and an organisation that has not defined who owns the decision at each confidence threshold could face liability issues down the line. As with any system, nothing is perfect and given public AI mistakes over the past few years, should not be considered as such.

11.7 Remote identification

Remote ID, the broadcast of a drone's position and operator identity by the aircraft itself, is a regulatory rather than a sensor technology, and it deserves a place in this section because it will change what detection means over the next several years.

Its promise is that it converts a large share of the identification problem from a technical question into a database lookup: a compliant drone announces what it is and who is flying it. Its limitation is equally obvious. Remote ID identifies cooperative operators. It does nothing about an operator who disables it, and disabling or bypassing it is trivial. Its actual security value therefore lies in removing the enormous volume of lawful traffic from the ambiguous category, not in catching malicious operators.

11.8 What the modalities add up to

The sections above should be read together, not as a menu, because the sum is less comfortable than any of the parts.

Set the lawful Australian detection set against the threat this paper says is arriving. Radio frequency detection, the most widely deployed modality and the cheapest to install, is blind to a fibre-optic aircraft and to one flying a pre-programmed route, and both are becoming more common. Radar sees a non-transmitting drone but sits at the difficult end of its own performance envelope against a small, slow, low-flying target, degrades in weather, confuses birds, and generally requires an ACMA transmitter licence. Electro-optical and thermal are cueing sensors, not search sensors: they confirm what something else has already found. Acoustic works to a few hundred metres in quiet conditions and is close to useless at a working port or processing plant. Remote ID resolves only the operators who choose to be identified.

Against a non-transmitting or fibre-optic aircraft flown by someone who does not want to be found, the detection set an Australian civilian operator may lawfully deploy is thin, and thinner

than the vendor literature suggests. That is not an argument against investing in detection, which remains the only layer available and is the precondition for everything else. It is an argument for three things: buying against outcomes rather than product categories (section 10.4), building the decision and reporting layers that work whether or not the sensor sees anything (sections 12.2 and 14.4), and treating the regulatory reform at section 15.3 as load-bearing, not aspirational, since an operator who cannot lawfully close the technical gap has the stronger claim on the policy one.

12. Response options

Having established what can be detected, this section covers what can be done about it, and, because this is an Australian paper, which of those options are actually available. Table 7 summarises. The legal position governing each is set out at section 13.

Table 7: Response options — technical, legal and practical availability

Option	Technical availability	General legal position in Australia	Practical availability to a private operator
Observe, record, report	Mature; requires only detection and a process	No restriction beyond privacy and data handling	**Available now.** The default response, and the one most sites have not resourced
Passive protection and dispersal	Mature; works against every control mode	No restriction	**Available now.** Cheap when designed in, expensive to retrofit
Net capture, ground-launched	Short range, commonly cited at 20–300 m; single shot	The physical act is not prohibited, but aviation, work health and safety, and state law all apply	**Conditional.** Requires close approach and a lawful basis for interfering with an aircraft; unlikely to be practical at most sites
Net capture, drone-launched	Extended reach; struggles against fast or evasive targets	Operating the interceptor requires CASA approval	**Conditional and complex.** Requires a trained operator and airspace authorisation
RF jamming	Mature but declining in effectiveness against fibre-optic and autonomous types	Prohibited equipment; possession as well as use is an offence	**Not available** without a section 27 exemption
Protocol takeover (“cyber over RF”)	Precise, low collateral, recovers the aircraft; depends on a database of known protocols	Engages the same radiocommunications provisions as jamming	**Not available** without an exemption
GNSS jamming or spoofing	Denies navigation without touching the control link	Prohibited; also affects aviation, maritime, survey and timing users nearby	**Not available**, and unsafe in civil airspace regardless
High-power microwave	Defeats drones regardless of control mode; effective against multiple targets	Emission and safety regulation; no civilian pathway	**Not available.** High capital cost; downed aircraft fall uncontrolled
High-energy laser	Long range, very low cost per shot; line of sight only, weather-limited	No civilian pathway; significant collateral risk	**Not available**
Kinetic interceptors	Effective against larger and faster threats; some designs recoverable	No civilian pathway	**Not available**, and the economics do not work against cheap quadcopters

General legal position is a strategic summary.

12.1 Detect, track, identify

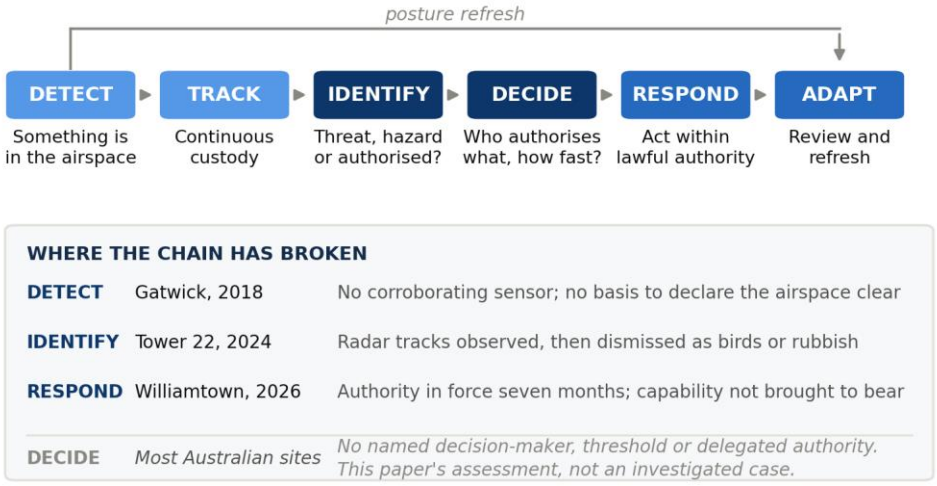

Figure 4: The counter-drone chain, and where the documented failures cluster. Detection is necessary and rarely sufficient; the binding stages sit in the middle. The three named cases are investigated incidents. The decide row beneath the rule is this paper's assessment and is not drawn from an investigation record.

This section covers the first three stages of that chain. Decision-making is at section 12.2 and the response options themselves from section 12.3; the adapt stage is the refresh discipline at section 14.8. Detect, track and identify are treated together here because organisations routinely conflate the first with the third.

Detection is the initial alert: a radar return, an RF signature, an acoustic hit. Tracking maintains continuous custody of the target as it moves, so that a decision-maker has current positional information when a decision is required. Identification is the classification of that track as hostile, unauthorised, authorised or non-threatening.

Identification is the hardest of the three and it is where systems actually fail. Of the 85 drone operators apprehended during the Paris Olympics, most were not acting maliciously: hazards rather than threats, in the terms set out at section 1.4, and indistinguishable from threats at the moment of detection.[162] At Tower 22, a defended military site with sensors working, the fatal failure occurred at identification: radar tracks were observed and dismissed as too distant, too slow, or possibly birds or rubbish, by a crew simultaneously occupied with recovering a friendly reconnaissance drone.[163] At Gatwick, Sussex Police assessed 109 of 129 reports as coming from credible witnesses, including pilots and airport staff, and no drone was ever recovered, photographed or corroborated by a sensor.[164] [165]

High false-positive rates in populated environments are an operational and legal constraint, not a technical footnote. An incorrect identification can lead to a response that is not only wasted

[162] Ministère des Armées, "JOP 24 — bilan de la sécurisation aérienne des Jeux…", see reference 74.
[163] Associated Press, "Confusion gripped US base defenders as a flying bomb…", see reference 17.
[164] Sussex Police, *Sussex Police gives up on £790k Gatwick drone shutdown…*, see reference 94.
[165] Airprox Reality Check, "Gatwick 2018", see reference 10.

but unlawful, and in Australia the legal exposure attaches to the organisation that acted, not to the drone operator who caused the confusion.

12.2 Decision-making

Three things have to hold at once for a counter-drone posture to produce an outcome, and an organisation is limited by whichever is weakest.

Detection quality determines whether a track exists and how much confidence attaches to it. **Decision quality** determines whether that track can be resolved into an authorised course of action inside the response latency available. **Lawful response authority** determines which actions are on the table at all. A site with excellent sensors, an undefined escalation path and no mitigation authority produces a well-documented incident and nothing else, which is a fair description of what happened at Williamtown, where detection worked, the regulations permitting Defence to act had been in force for seven months, and the outcome was a police referral. A site with clear authority and poor detection cannot use it. The three are multiplicative rather than additive, and most Australian civilian operators are limited by the second, which is the cheapest of the three to fix.

Once a track is identified as a credible threat, the binding constraint on everything that follows is usually authority: who may order a response, under what threshold, and by what means.

That authority varies significantly. What a defence establishment may lawfully do, examined at section 13.3, differs substantially from what an airport, a shopping centre or a critical infrastructure operator may do, examined at section 13.2. Every technology described at sections 12.3 through 12.8 is, in Australia, available to a narrower set of lawful users than a reader unfamiliar with the regulatory environment would assume.

The practical governance requirement is a documented, rehearsed decision matrix that maps observed behaviour to a defined response, with named decision-makers and defined thresholds, and that can be executed without attribution. The questions in Appendix A are designed to test whether one exists.

12.3 Soft kill

Soft kill denies a drone's ability to operate instead of destroying it, and is generally preferred where available because it avoids falling debris or an airborne detonation. In Australia, for most readers, it is not available. Table 7 sets out the position; three points follow.

Jamming is assumed to be a reliable default far more often than the record supports. It has no effect on fibre-optic-controlled aircraft, which have no radio link to attack; diminishing effect on aircraft with link-loss autonomy and terminal guidance, which continue toward the target; and an unpredictable behavioural effect, since a jammed drone may return to its launch point or may descend uncontrolled onto whatever is beneath it. The clearest recent demonstration is French: a marine rifle battalion carried out several counter-drone engagements with a jammer against five drones over the Île Longue submarine base in December 2025, and none was

brought down.[166] Furthermore, "jamming" is a blanket term but is generally only effective against targeted RF bands. Drones which operate outside these bands, or more commonly, are able to dynamically change frequencies (known as frequency hopping) remain unaffected.

Protocol takeover, sometimes marketed as cyber over RF, interacts with the drone's own communication protocol rather than blocking it, reading the exchange closely enough to take over basic functions and guide the aircraft to a safe landing. United States government guidance treats it as a distinct non-kinetic technique from radio frequency jamming,[167] and it has been integrated into Australian-developed product lines.[168] Its inherent limitation is that it depends on knowing the protocol, which makes it weakest against custom or heavily modified airframes, which is likely the category a determined actor would use.

GNSS interference is a policy question, not a technical one. Jamming or spoofing GNSS disrupts a drone's navigation, but the interference does not distinguish the drone from every other GNSS-dependent system nearby, and aviation now treats GNSS interference as a significant safety risk in its own right, with EASA and IATA having developed a coordinated mitigation plan.[169] Deliberately generating that interference in Australian civil airspace is not an option available to a private operator under any realistic reading of the law and would even be an unlikely option for military operators.

12.4 Hard kill

Hard kill covers physical destruction or capture, generally reserved for cases where soft-kill options are unavailable, ineffective or too slow.

Net capture systems physically recover the target. Ground-launched systems are cited by vendors at effective ranges of roughly 20 to 300 metres; drone-launched systems extend that reach considerably but struggle against fast or evasive targets.[170] The advantages matter in a civilian context: no falling debris beyond the target, no airborne detonation, and recovery of the aircraft intact for forensic examination, which counts for a great deal in a jurisdiction where prosecution is the primary remedy. Effectiveness is also boosted by being the inherent weakness of small drones – having something tangled in the rotor blades.

Directed energy. Two distinct technologies sit here. High-power microwave systems attack a drone's onboard electronics directly, not its communication link. Epirus states that its Leonidas system defeated a 49-drone swarm at an August 2025 live-fire demonstration in which it reports defeating 61 of 61 drones flown,[171] and that in December 2025 it defeated a fibre-optic-controlled FPV drone by inducing failure in onboard electronics through phased-array delivery

[166] Opex360 (Zone Militaire), "Les fusiliers marins de la base sous-marine de l'Île…", see reference 82.

[167] Cybersecurity and Infrastructure Security Agency, *Protecting Against the Threat of Unmanned Aircraft Systems*, November 2020, which treats protocol manipulation and control-link takeover as techniques distinct from radio frequency jamming.

[168] Unmanned Airspace, "DroneShield integrates Sentrycs cyber takeover capability to DroneSentry."

[169] European Union Aviation Safety Agency, "EASA and IATA outline comprehensive plan to mitigate GNSS interference risks."

[170] Robin Radar Systems, "10 Types of Counter-Drone Technology to Detect and…", see reference 87.

[171] Epirus, "Epirus' Leonidas High-Power Microwave Defeats 49-Drone Swarm, 100% of Drones Flown at Live-Fire Demonstration," 10 September 2025, reporting a demonstration conducted on 26 August 2025. Manufacturer-reported; no independent verification is available.

of electromagnetic energy.[172] These are the company's own accounts of its own trials and have not been independently validated in the public record. Taken cautiously, it indicates a direction of development rather than a fielded solution. High-energy lasers, including the United Kingdom's DragonFire and Israel's Iron Beam, offer a comparable low cost per shot once built, but remain constrained by line of sight, weather and thermal management in ways microwave systems generally are not.

Kinetic interceptors. Purpose-built counter-drone missiles are designed for larger and faster threats than this paper is concerned with, and are positioned as a high-value-asset protection tool rather than a wide-area civilian solution, given cost and the safety implications of falling debris. One development is built around that problem. Anduril's Roadrunner-M, ordered by the United States Department of Defense under a $250 million contract, is explicitly designed to be recoverable: the manufacturer describes a twin-jet vertical take-off and landing interceptor that returns and lands instead of being expended when it is not committed to an engagement.[173] [174] This addresses the cost-exchange problem at section 10.3 directly, by making the defender's cost contingent on engagements that actually occur, not on launches. Ukraine also has several drone interceptor manufacturers largely focused on taking out Shahed-style drones but are also used for interception of other types as well.

Australia has begun contracting in both categories, with AIM Defence's Fractl laser system (described as tracking objects the size of a ten-cent piece at speeds over 100 km/h) and SYPAQ's Corvo Strike interceptor both funded in April 2026.[175]

12.5 Passive protection and dispersal

This is the response category most available to Australian organisations and the one most often skipped.

Netting and overhead screening of critical outdoor plant. Hardened or covered shelters for high-value assets. Relocation of vulnerable equipment (control cabinets, telemetry, chemical dosing, generator sets) to positions that are not overhead-accessible. Removal of predictability in where and when high-value assets sit exposed. Standoff, through control of adjacent land or arrangements with neighbours about what is stored and parked where. As previously mentioned, this also alleviates the intelligence that can be gathered by satellite imagery.

Operation Spiderweb succeeded specifically because strategic bombers were parked in the open at fixed and predictable locations. No detection system or interceptor in this section substitutes for the protective value of not leaving a high-value asset exactly where an attacker would expect to find it. For an Australian operator with no lawful mitigation options, passive protection is the primary physical control.

---

[172] Epirus, "Epirus' Leonidas Demonstrates Successful Use of…", see reference 61.

[173] *Defense News*, "Anduril lands $250 million Pentagon contract for drone defense system," 8 October 2024.

[174] Anduril Industries, "Anduril Unveils Roadrunner and Roadrunner-M," 1 December 2023, describing a twin-jet vertical take-off and landing interceptor that returns and lands when not committed to an engagement.

[175] The Hon Pat Conroy MP, "Albanese Government to invest up to $7 billion in…", see reference 98.

12.6 Response through investigation and enforcement

For most Australian organisations the realistic response is investigative, not kinetic, and it should be planned as deliberately as any technical control. It comprises: RF-derived operator location passed to police in real time; imagery sufficient to identify the airframe and any payload; a preserved, time-stamped record of the track; established contact pathways to state police and, where relevant, the AFP and CASA; and a documented pattern-of-activity record that allows three separate sightings over three weeks to be recognised as one campaign and not as three unrelated nuisances.

12.7 Counter-swarm defence

The technologies above are, for the most part, designed to engage one aircraft at a time. A saturation attack (section 5.7) is designed to break that assumption. Single-target defeat systems do not scale against a coordinated multi-drone attack, because a defender's engagement capacity at any moment is limited while an attacker's aircraft count is not.

This is why wide-area, one-to-many effectors have attracted heavy investment: a high-power microwave system that defeats dozens of aircraft in one engagement addresses the problem in a way that missile-based interceptors structurally cannot, however cost-efficient each engagement is. Swarm saturation was identified as the principal unresolved concern going into the Paris Olympics,[176] and nothing since has changed that assessment for civil environments.

12.8 Operational limitations

Part IV closes with the caveats that should temper the preceding two sections. Identification false-positive rates remain an operational and legal problem in populated areas. Australian legal constraints (Part V) narrow the practical response set to detection, passive protection, investigation and notification for most readers regardless of what is technically possible. Weather and line of sight constrain optical and laser systems in ways microwave and kinetic options are not equally subject to. Wide-area coverage of a large industrial site is expensive and, in cluttered terrain, incomplete at any price. And the cost sustainability of kinetic options at scale remains open even accounting for reusability.

Underlying all of it is the pattern running through Part II: attacker adaptation and defender countermeasure are locked in a cycle that neither regulation nor procurement timelines have matched. Part V examines what that means for governance, given that technology alone will not resolve it.

[176] France 24, "Tests expose worrying flaws in France's anti-drone…", see reference 69.

Part V — Governance

13. The Australian regulatory environment

> **Legal information notice.** This section provides a high-level summary of Australian law based on publicly available legislation, regulations and regulatory guidance as at September 2026. Instruments in this area are under active amendment. Organisations should obtain jurisdiction-specific legal advice before acquiring, deploying or operating counter-drone equipment, or before relying on any characterisation of their obligations set out here.

This is the part of the paper that most distinguishes Australian practice from the international literature, and it is where the paper's central finding sits. The technologies described in Part IV exist, are improving, and are increasingly available commercially. What determines whether an Australian organisation can use them is a set of legislation and restrictions drafted for other purposes, mostly before small drones existed.

13.1 CASA and airspace

CASA's Part 101 framework under the Civil Aviation Safety Regulations is the starting point for understanding lawful drone operation in Australia and, by extension, for understanding what is unlawful.[177]

Part 101 classifies remotely piloted aircraft by weight: micro at 250 grams or less, very small at more than 250 grams and up to 2 kilograms, small at more than 2 kilograms and up to 25 kilograms, medium at more than 25 kilograms and up to 150 kilograms, and large above 150 kilograms. The standard operating conditions define what normal looks like: operation at or below 120 metres above ground level, by day only between morning and evening civil twilight, within continuous unaided visual line of sight, not within 30 metres of a person not directly associated with the operation, one aircraft per operator at a time, not within 5.5 kilometres of the runway measurement point of a controlled aerodrome, not within 5.5 kilometres of a non-controlled aerodrome when crewed aircraft are present, and not over an area where a fire, police or other public safety or emergency operation is under way without the approval of the person in charge.[178] Above that baseline, the certified category requires a remote pilot licence and a remote operator's certificate. CASA does not require registration or a licence for recreational flying under 250 grams; commercial use requires registration and either accreditation or a licence; and drones over 25 kilograms require specific approval.[179]

Two points of practical significance for a security audience. First, almost everything a hostile operator would do is already unlawful. Flying at night, beyond visual line of sight, over people, near an aerodrome, or over an emergency operation each breaches Part 101 independently of

[177] Civil Aviation Safety Authority, "Part 101 of CASR — Unmanned aircraft and rockets."

[178] Civil Aviation Safety Authority, *CASR Part 101 Plain English Guide — Micro and Excluded RPA Operations*, setting out the weight categories and the standard operating conditions.

[179] Civil Aviation Safety Authority, "Drone safety rules", see reference 40.

any intent. The regulatory gap in Australia is not that malicious drone use is legal; it is that detecting it, attributing it and responding to it are all difficult.

Second, CASA treats this space as unsettled and is actively reforming it, and the reform pressure runs in the opposite direction to the security interest. New beyond-visual-line-of-sight (BVLOS) pathways have opened for trial operations, and CASA has signalled further Part 101 changes under development. The regulator has to accommodate a fast-growing legitimate industry (including edge cases such as operators running remote drone operations across state boundaries) while maintaining the ability to identify and act against unauthorised flights. Those two goals pull the settings in opposite directions, and a security-driven submission to a CASA consultation that ignores the industry side of the ledger will not succeed.

13.2 ACMA and the Radiocommunications Act

This is arguably the single most consequential legal fact in this paper for the readership it is written for. Mobile phone jammers, GPS jammers, Wi-Fi jammers and drone jammers are prohibited in Australia under a permanent ban issued under subsection 172(3) of the *Radiocommunications Act 1992* (Cth). It is an offence to operate, supply, offer to supply, or have such a device. The penalties are up to $330,000 and/or two years' imprisonment, rising to $1.65 million or five years where the conduct causes significant interference.[180]

Exemptions exist, and they are drawn narrowly (for good reason). Section 27 exemptions are available only to a narrow range of professions with functions or duties relating to defence, national security, law enforcement or emergency services, and an applicant must demonstrate that the intended use serves an operational objective with minimal adverse impact on licensed radiocommunications. The instrument that permits Australian police to use counter-drone equipment is the *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022*. Other current exemptions cover mobile phone jamming in New South Wales correctional facilities, electronic countermeasures for bomb disposal and dignitary protection, and GPS jamming for defence entities.[181] The Australian Government's own drone security policy describes that determination as the mechanism enabling police access to counter-drone equipment that would otherwise contravene the Act.[182]

Detection technologies are generally more accessible under Australian law than active countermeasures, but their deployment is conditional: it remains subject to equipment licensing (radar will usually require an ACMA transmitter licence) and to privacy, aviation and site-specific requirements discussed at sections 13.6 and 13.7. Active electronic defeat is a different matter. Jamming is prohibited, and the prohibition attaches to possession as well as use. Protocol takeover and GNSS interference sit in the same regulatory space and are not available without an exemption that a commercial operator is unlikely to obtain.

For most readers of this paper, therefore, the layered defence model at section 10.1 currently stops at detection, identification, passive protection, investigation and notification. That is a

[180] Australian Communications and Media Authority, "Jammers are illegal in Australia", see reference 25.

[181] Australian Communications and Media Authority, "Exemptions for banned equipment", see reference 24.

[182] Australian Government, Drones.gov.au, "Security policy," describing the *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022*, work on agency access to counter-drone capability, and the Drone Rule Digitisation project.

policy setting, not a technology gap: one adopted for sound spectrum-management and traditional safety reasons, but one that has not been revisited against the current threat picture.

13.3 Defence

The Australian Defence Force's authority to respond to a drone incursion over or near a defence establishment was, until recently, quite constrained, and the reason is instructive. The *Defence Act 1903* was built to prevent unauthorised military intervention on domestic soil, requiring ministerial approval and operating within narrow limits in proclaimed circumstances. Those are sensible constraints on the domestic use of military force in general, drafted a century before anyone anticipated small commercial drones.

Analysis published by the Australian Strategic Policy Institute argued that this left the ADF in an anomalous position: civilian agencies including the AFP held statutory authority to deploy countermeasures while the ADF did not, and the counter-drone framework was spread across eight separate pieces of legislation covering everything from airspace safety to electronic countermeasures. The same analysis argued that the technology to detect a Spiderweb-style attack existed and had been proven in active military environments, and called for review of the Defence Act to allow reasonable and proportionate action around Defence facilities.[183]

That gap has now substantially closed. The *Defence Amendment (Counter-UxS Measures) Regulations 2025* were registered in December 2025 and announced the following January. They authorise Defence to detect and disable or destroy drones suspected of posing a threat to ADF assets and establishments, support law enforcement agencies in responding to drone threats, and employ Defence capabilities within Australia where safe and reasonable to do so.[184] [185]

Three observations for a civilian reader:

- The regulations resolve the ADF's problem and no one else's: a critical infrastructure operator adjacent to a defence establishment gains nothing from them.
- They are recent enough that their practical effect is not yet established, including how they interact in a real incident with state police primacy and with CASA's airspace responsibilities.
- They demonstrate that the Australian system can move on this when it decides to. The regulations, the LAND 156 industry panel and the $7 billion commitment all landed within fifteen months of Operation Spiderweb. That is the relevant precedent for the argument at section 15.3.

[183] Australian Strategic Policy Institute, "Legislation, not technology, is the biggest problem for ADF drone defence," *The Strategist*.

[184] The Hon Pat Conroy MP and the Hon Peter Khalil MP, "Government boosts response to drone threats", see reference 97.

[185] *Defence Amendment (Counter-UxS Measures) Regulations 2025* (Cth), F2025L01553, registered 12 December 2025.

13.4 Police and state authority

	Detect and track	Record evidence	Passive protection	Jam the control link	Jam GNSS	Protocol takeover	Physical capture	Destroy	Investigate and refer
Private operator (incl. critical infrastructure)	Cond.	Yes	Yes	No	No	No	Cond.	No	Yes
Airport operator	Cond.	Yes	Yes	No	No	No	Cond.	No	Yes
Corrections agency	Cond.	Yes	Yes	No	No	No	Cond.	No	Yes
State / territory police	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Australian Defence Force	Yes	Yes	Yes	Yes	Cond.	Yes	Yes	Yes	Cond.
CASA / Airservices	Yes	Yes	n/a	No	No	No	No	No	Yes

Figure 5: Australian counter-drone authority, indicative position at September 2026. Cond. = Conditional; available subject to licensing, approval or a specific authorisation.

Police are among the principal civilian authorities able to deploy active counter-drone capabilities under existing Australian arrangements, and the arrangement determines what an organisation should actually be planning for.

State and territory police hold the ACMA exemption under the 2022 Determination, which exempts members of the Australian Federal Police and of each state and territory police force.[186] They have deployed detection capability at major events across all states in cooperation with Home Affairs and Defence.[187] Their capability is, naturally, oriented toward events and operations, not toward standing protection of private infrastructure.

The consequence for an infrastructure operator is that the response plan is a *notification* plan. The relevant preparation is procedural, and none of it can usefully be worked out while an incident is running: who is called, on what number, what information they need in what format, what response time is realistic, and what the organisation does in the interim all have to be settled beforehand.

13.5 Critical infrastructure obligations

Building on section 7.2, the *Security of Critical Infrastructure Act 2018* (Cth), as reformed in 2021 and 2022, imposes Positive Security Obligations on responsible entities. Five apply here.[188]

Register reporting, with asset information registered with the Cyber and Infrastructure Security Centre and updated within 30 days of a material change. A critical infrastructure risk management program, addressing material risks from *any* hazard including cyber, personnel, natural disaster and supply chain, with an annual attestation report due 90 days after the end of the financial year. Cyber incident reporting, with significant incidents notifiable within 12

[186] *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022* (Cth), F2022L01255, registered 26 September 2022, section 8 of which exempts a member of a police force, defined to include the Australian Federal Police and the police force of each state and territory.

[187] Dedrone, "Australian Police protect major events from drone threats", see reference 51.

[188] Cyber and Infrastructure Security Centre, "Security of Critical Infrastructure Act 2018 —…", see reference 47.

hours and relevant-impact incidents within 72 hours. Enhanced cybersecurity obligations are applied to assets declared Systems of National Significance.

While not every entity has equal legal responsibilities, the risk management program obligation is all-hazards and expressly covers physical and personnel risks. Whether a particular unauthorised aircraft over a particular asset is a material risk is a judgement for the responsible entity, informed by its own circumstances and its own advice. The argument being made here is that the judgement should be made deliberately and recorded, not left unconsidered, and that for an entity already maintaining a risk management program, folding the assessment into that existing process is more efficient and more durable than running it as a standalone security initiative. It is also something for insurers to consider when underwriting assets of these entities.

13.6 Privacy

Privacy operates in both directions in this space. Drones operated by threat actors raise the surveillance concerns examined throughout Part II. Detection systems deployed in response themselves collect data (e.g. RF signatures, in some cases estimated operator locations, and inevitably imagery of members of the public in adjacent areas) and must be operated consistently with the *Privacy Act 1988* (Cth).

That Act was substantially amended by the *Privacy and Other Legislation Amendment Act 2024*, which introduced a statutory tort for serious invasions of privacy. The tort commenced in June 2025 and covers both intrusion upon seclusion, including physical intrusion into a person's private space, and misuse of personal information. A plaintiff must establish a reasonable expectation of privacy in all the circumstances and that the public interest in privacy outweighs countervailing public interests. Courts may grant damages, injunctions or orders requiring an apology, and defences include consent and lawful authority, with exemptions for intelligence agencies, law enforcement and journalists in certain circumstances.[189]

Organisations deploying sensor-heavy detection should treat their own data handling as a compliance question, not an afterthought to the security problem it is solving, and should be able to state what is recorded, how long it is retained, who can access it, and on what basis.

13.7 State and territory legislation

Beyond the Commonwealth framework, a patchwork of state and territory law intersects with drone operation and, therefore, with counter-drone activity.

Surveillance devices legislation differs between jurisdictions in what it prohibits and what it permits, as do trespass, nuisance and property law, and the extent to which the airspace above a property is treated as within the occupier's control. Corrections law provides the clearest example of state-level intervention specific to drones: Victoria has prohibited flying a drone within 120 metres of the boundary of around twenty correctional facilities and three youth justice centres since 1 February 2018, with a maximum penalty of two years' imprisonment

[189] Office of the Australian Information Commissioner, "Statutory tort for serious invasions of privacy," commenced 10 June 2025.

and exemptions for police, emergency services and departmental staff,[190] and Queensland applies a comparable two-year maximum for being caught with a drone at a correctional facility.[191]

For a national organisation attempting to apply one consistent security posture across sites in multiple states, this variation adds compliance complexity on top of Commonwealth requirements, and warrants jurisdiction-specific legal advice rather than an assumption that Commonwealth compliance is sufficient. It is also, as section 15.3 argues, an avoidable inefficiency that a harmonisation process could reduce.

13.8 Where the regulation is heading

Several developments are already underway.

Uncrewed traffic management. Airservices Australia has been building a national drone traffic management capability, including a Flight Information Management System, in partnership with Frequentis, and has separately gone to market for a drone surveillance system covering 29 controlled airports specifically to give a clear picture of uncrewed aircraft operating around them.[192] [193] This is the single most significant piece of Australian detection infrastructure being built.

Remote identification. Remote ID is under active consideration, following United States and European practice. Its promise and its limits are discussed at section 11.7.

Drone rule digitisation and site restrictions. The Government's drone security policy describes work on improving agency access to counter-drone capability, enhancing coordination and data sharing on drone activity across agencies and jurisdictions, and a Drone Rule Digitisation project addressing restrictions around correctional facilities and other sensitive sites.[194]

Counter-drone capability and industry. The LAND 156 industry panel, Mission Syracuse under the Advanced Strategic Capabilities Accelerator, and the $7 billion counter-drone commitment within the 2026 Integrated Investment Program together represent a substantial sovereign capability build.[195] [196]

What is conspicuously absent from that list is any reform of the jamming prohibition at section 13.2 as it applies to non-government critical infrastructure operators. Everything above expands government capability, government coordination and government access. None of it changes what an LNG operator, a port, a hospital or a data centre may lawfully do about a drone over its own site. The uncrewed traffic management rollout, the Remote ID work and the broader security policy development are all live, which means the framework that will govern

[190] Department of Justice and Community Safety Victoria, "Drone ban near Victorian correctional and youth…", see reference 57.

[191] The Hon Mark Ryan MP, "New regulation brings down drones", see reference 96.

[192] Airservices Australia, "Drones and Uncrewed Aircraft Systems Traffic Management."

[193] Unmanned Airspace, "Airservices Australia publishes tender for drone…", see reference 106.

[194] Australian Government, "Security policy", see reference 27.

[195] The Hon Pat Conroy MP and the Hon Peter Khalil MP, "Government boosts response to drone threats", see reference 97.

[196] The Hon Pat Conroy MP, "Albanese Government to invest up to $7 billion in…", see reference 98.

this for the next decade is being written now, and should be considered, and debated, across industries and government.

14. Governance and preparedness

14.1 Executive ownership

The argument for board-level ownership of drone risk follows the same legal logic that has already shaped how Australian boards treat cyber security. Australian directors owe duties of care and diligence under the *Corporations Act 2001* (Cth) that ASIC has increasingly interpreted to require active oversight of foreseeable risks rather than passive delegation to management. In *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496, the Federal Court found that an Australian financial services licensee had breached its licence obligations by failing to have adequate cyber security risk management in place, establishing that cyber risk management for licensees is a matter of legal obligation, not just best practice.[197] A decade before that judgment, the same risk sat almost entirely with IT departments. It moved because it became too foreseeable, too material and too well documented in the public record for a board to credibly claim it was not reasonably aware.

The evidence base assembled in this paper (Operation Spiderweb, Abqaiq, Gatwick, October 7, the American and European sighting waves, and the confirmed incursions over RAAF Base Williamtown) exists precisely to make the small-drone threat similarly difficult to characterise as unforeseeable.

For organisations already captured by the SOCI Act there is also a procedural mechanism forcing the question upward. The risk management program obligation requires an annual attestation report, due 90 days after the end of the financial year, covering material risks from all hazards.[198] That means a credible drone threat assessment, once it exists, does not stay in a facilities team's risk register; it is structurally required to be declared.

The organisations that come through a drone-related incident well will, in all likelihood, be the ones where a named executive already owned this risk before the incident, rather than the ones assembling a response team for the first time afterward.

14.2 Enterprise risk

Drone risk should be integrated into an organisation's existing enterprise risk management framework (ISO 31000 remains the most widely used reference standard in Australia) alongside physical, cyber and operational risk categories, instead of being tracked as a siloed concern with its own separate governance process.

This is partly efficiency and mostly accuracy. Section 9.5 described how a drone incident's cascading effects extend well beyond the immediate physical or operational impact, into exactly the kind of interdependent, cross-category risk that an integrated framework is

[197] Australian Securities and Investments Commission, media release 22-104MR, "Court finds RI Advice failed to adequately manage cybersecurity risks," 5 May 2022. The judgment in *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496 is also available.

[198] Cyber and Infrastructure Security Centre, "Security of Critical Infrastructure Act 2018 —…", see reference 47.

designed to surface and a siloed one is not. A drone risk owned solely by physical security will not connect to the cyber exposure at section 5.2, the supply chain exposure at section 4.9, or the aviation safety exposure at section 8.2.

The supply chain and data sovereignty questions raised at section 4.9 belong in this framework as well, and they belong there as an operational and procurement risk rather than as a geopolitical talking point. The specific question a risk committee should be able to answer is: what drones does this organisation operate, what data do they collect, where does that data go, and who else can reach it.

14.3 Security planning

The practical starting point is a site-specific vulnerability and risk assessment that asks a direct question drawn from Parts II and III: which of this organisation's sites most resemble the vulnerable, high-value, poorly dispersed targets examined at sections 6.1.1 and 8.4 — concentrated, predictable, and undefended against this specific threat?

A workable assessment covers, at minimum: the site's critical assets and which of them are overhead-accessible; the approach geometry, including where an operator could stand or park with line of sight (although that in itself is of decreasing relevance with drone ranges); the site's existing detection and camera coverage and whether any of it looks up; the baseline of legitimate drone activity, including the organisation's own; the neighbouring land uses that would constrain any response; and the notification pathways at section 13.4.

The output should feed directly into the layered defence and security-by-design principles at sections 10.1 and 10.5 and, for SOCI-captured entities, into the physical security component of the risk management program already required.

14.4 Incident management

Response protocols need to establish decision authority in advance, tying back to section 12.2, given how significantly that authority varies by location and technology. Four elements are the ones most often missing.

A behaviour-based escalation matrix that does not require attribution, consistent with the principle at section 10.6. Defined thresholds separating monitor, notify police and activate crisis response, with named decision-makers reachable outside business hours and, where response latency is measured in seconds, not minutes, authority delegated in advance to whoever is actually present. Coordination arrangements with state police, the ADF where relevant, and CASA, established and tested before an incident. And, for SOCI-captured entities, reporting pathways built into the plan from the outset, noting that the Act's 12 and 72-hour windows apply to cyber incident reporting, so whether a given drone incident triggers a notification obligation is a question to settle in advance rather than during one.[199]

[199] Cyber and Infrastructure Security Centre, "Security of Critical Infrastructure Act 2018 —…", see reference 47.

A fifth element is a communications position drafted in advance. The organisations that handled the 2024 and 2025 sighting waves worst were those that offered shifting explanations under pressure.

14.5 Business continuity

Continuity planning for this risk needs to incorporate a pure-disruption scenario: no damage, no casualties, no attribution, and an extended shutdown driven by an unresolved presence. It cannot assume it only has to cover damage-causing events (although that must be considered as well). Section 6.2 sets out what that costs at scale, and the Australian corrections record at section 8.5 shows the same pattern occurring routinely at smaller scale.

14.6 Exercises

A capability that has been trialled is still some distance from one that can be used under pressure. Exercises should simulate the identification and decision bottlenecks at sections 12.1 and 12.2 rather than testing whether the technology functions. The realistic exercise goes beyond “a drone is detected, what does the system do.” It is the sequence set out as a decision exercise in Appendix A: conflicting reports, a detection system showing nothing, an aircraft on approach, a journalist calling, and the accountable executive on leave.

14.7 Insurance and liability

Insurance belongs on the list as a distinct governance workstream, because it is where several of this paper’s threads converge.

A number of questions regarding an organisation’s insurance coverage could be asked:

- Does the organisation’s property and business interruption cover respond to a pure-disruption event with no physical damage?
- How would an incident be characterised if attribution never arrives, given that terrorism, malicious damage and accidental-cause treatments differ and that Australian terrorism cover operates through a specific statutory scheme?
- What liability attaches if the organisation’s own counter-drone measures cause harm (a downed drone injuring someone, or interference affecting a third party)?
- What liability attaches to the organisation’s own drone operations, including the privacy exposure created by the statutory tort at section 13.6?

The insurance market’s treatment of the Red Sea corridor, where war-risk premiums repriced an entire trade route, is a reminder that insurers respond to this class of risk faster than regulators do, and that an organisation which cannot describe its drone risk posture may find the question asked of it at renewal.

14.8 Continuous improvement

The pace of adaptation on both sides of this threat means a security posture that is not actively revisited is likely to be materially out of date within one to two years rather than five or ten.

Three practices follow. Structured after-action review following any incident or near-miss, including the ones where nothing happened, because the near-misses are where the pattern at section 12.6 becomes visible. Ongoing monitoring of the kind of international developments this paper has drawn on, assigned to a named person, not left to chance. And a technology refresh cycle built into procurement and budgeting from the outset rather than treated as an exceptional expense, with contracts written to allow sensor substitution instead of locking the organisation to one vendor's roadmap.

Part VI — Conclusion and Recommendations

15. Conclusion and recommendations

15.1 Conclusions

The evidence assembled in Parts II and III supports four key conclusions.

Australia's principal near-term problem is not the absence of counter-drone technology, but the integration of technology with authority, governance and operational preparedness. The sensors, classifiers and effectors described in Part IV exist and are improving, and Part IV is equally clear that they have real limits: identification remains hard, coverage is not performance, and no modality is strong across the row. The claim here concerns integration, not solved technology. Williamtown is the clearest domestic illustration where detection worked, the regulations permitting Defence to act had been in force for seven months, and the outcome was only a referral to police.

For many organisations, ambiguity and disruption are among the most plausible near-term scenarios, and more plausible than a catastrophic attack. Almost every case study in this paper that occurred in a country at peace took that form: an unresolved presence that could not be identified, could not be attributed, and could not be lawfully removed, forcing expensive precautionary decisions in the meantime.

The immediately available controls are detection, decision-making, passive protection, reporting and continuity. They are lawful today. None of them requires a regulatory change, and most require governance rather than capital; nothing external has prevented the organisations that have not made these investments from doing so.

Government must close the remaining authority and coordination gap. The Defence Amendment (Counter-UxS Measures) Regulations 2025 resolved the position for Defence. Nothing equivalent exists for the civilian operators of the assets at section 8, and the exemption framework that governs their options turns on profession, not on the criticality of what is being protected.

15.2 Recommendations for industry and critical infrastructure operators

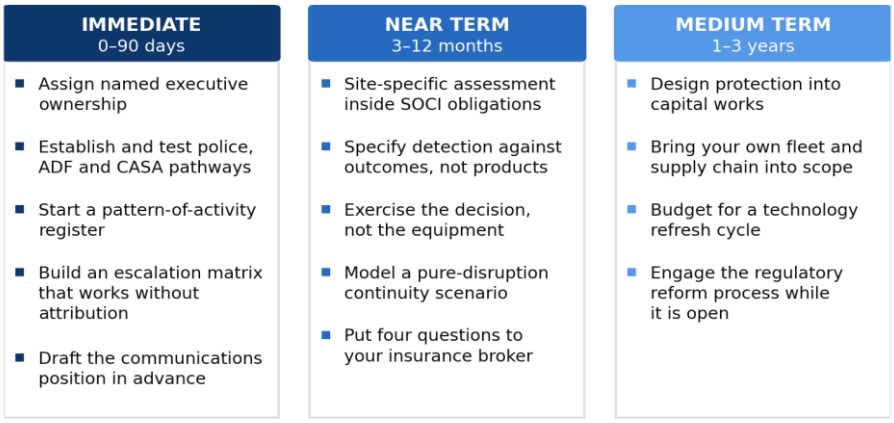

Figure 6: Recommended posture by time horizon. Generated from the recommendations at section 15.2. Nothing in the immediate column requires capital expenditure or a regulatory change.

Grouped by time horizon. Importantly, nothing in the immediate group requires capital expenditure or a regulatory change.

Immediate — 0 to 90 days

Assign named executive ownership. The legal parallel to cyber security governance reflects a real expectation of foreseeable-risk oversight under directors' duties, and for SOCI-captured entities the annual attestation will surface the question regardless. This costs nothing, and of the controls in this list it is the one most consistently associated with a well-handled incident.

Establish and test notification pathways with state police, the ADF where relevant, and CASA. Because police hold the mitigation authority most operators lack, an infrastructure operator's response plan is fundamentally a notification plan, and the contact details, information formats and expected response times it depends on need to be settled before an incident, not during one.

Start a pattern-of-activity register. Three sightings over three weeks are a campaign, but logged by three different shift supervisors they are three unrelated nuisances. The difference is only visible if one person owns the record, and assigning that costs nothing.

Build a behaviour-based escalation matrix that does not depend on attribution, with named decision-makers reachable outside business hours and defined thresholds separating monitor, notify and activate.

Draft the communications position in advance. The organisations that handled the 2024 and 2025 sighting waves worst were those that offered shifting explanations under pressure.

Near term — 3 to 12 months

Commission a site-specific vulnerability assessment, framed inside existing SOCI risk management program obligations instead of as a separate initiative. For captured entities this

work is likely required regardless, and folding it into an existing process puts the finding in front of the board through a channel that already exists.

Specify and procure detection against outcomes, not products (see the procurement principle at section 10.4). Specify sensor fusion and open integration explicitly, because most of the market does not offer them by default.

Exercise the decision, not the equipment. The realistic scenario goes beyond "the system alerts": a staff report the system cannot corroborate, an aircraft on approach, a journalist calling, and the accountable executive on leave.

Model a pure-disruption continuity scenario with an explicit decision rule for resuming operations. Gatwick's second day happened because no one could say when it was safe to reopen.

Put four questions to your insurance broker: pure-disruption cover, characterisation in the absence of attribution, liability arising from any countermeasure, and liability arising from your own drone operations including the statutory privacy tort.

Medium term — 1 to 3 years

Design protection into capital works. Overhead screening, relocation of control and telemetry equipment out of overhead-accessible positions, and reduced predictability in where high-value assets sit exposed are cheap at design stage and expensive afterwards. Any project currently in design is an opportunity.

Bring your own fleet and supply chain inside the risk framework. What drones does the organisation operate, what data do they collect, where does it go, and who else can reach it. An organisation that flies its own drones routinely has also trained its staff not to report drone sightings.

Build a technology refresh assumption into budgeting instead of treating it as an exceptional expense, and write contracts that permit sensor substitution, so the organisation is not locked to one vendor's roadmap.

Engage the regulatory reform process while it is open. Section 13.8 describes a window: the uncrewed traffic management rollout, the Remote ID work and the broader drone security policy are all live, which means the framework that will govern this for the next decade is being written now. The submissions that carry weight in that process come from operators who can describe a specific site, a specific gap and a specific consequence. Section 15.3 sets out what such a submission should ask for.

15.3 Recommendations for government and policymakers

Each recommendation names the agency best placed to own it and the obstacle that has kept it from happening.

1. Reform the counter-drone exemption pathway so that eligibility turns on asset criticality, not profession

Owner: The Australian Communications and Media Authority, with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.
Obstacle: Spectrum management risk is real and the current settings exist for sound reasons; any widening creates interference and misuse exposure that ACMA would carry.

What is needed is a tightly conditioned exemption class limited to designated critical assets, requiring demonstrated technical competence, defined geographic and power constraints, mandatory ACMA coordination, incident reporting and periodic review.

The permanent ban on jamming equipment should not be repealed. What should change is the section 27 framework, under which an operator of a SOCI-designated critical asset currently has no pathway regardless of the consequence of an incident at its site. The precedent already exists in the exemptions granted for correctional facilities, bomb disposal and dignitary protection. The exceptions granted to these operators could (and should) be limited in scope to prevent any accidental misuse.

2. Extend the regulatory momentum from Defence to the civilian side

Owner: The Department of Home Affairs.
Obstacle: The civilian case is more diffuse than the Defence case and has no single agency champion.

The pace demonstrated by the *Defence Amendment (Counter-UxS Measures) Regulations 2025*, the LAND 156 panel and the $7 billion commitment should be applied to the operators of the assets at section 8. A published civilian policy position with a stated timetable would be a better use of the next year than a further round of consultation.

3. Make uncrewed traffic management data usable for security, not only for safety

Owner: Airservices Australia, with CASA.
Obstacle: The network is being built to an aviation safety specification, and retrofitting security access later is expensive.

Structured access for security and law enforcement functions, with appropriate privacy controls, should be designed in during the current rollout instead of retrofitted. Three things need to be kept distinct in the design: access to the data, legal authority to act on it, and the operational capacity to respond.

4. Harmonise state and territory law where it intersects with drone operation

Owner: State and territory attorneys-general, through a national law reform process.
Obstacle: Surveillance devices and privacy law differ for reasons unrelated to drones, and harmonisation is slow.

A model provision approach would reduce compliance cost for national operators without reducing protection. The correctional facility restrictions already legislated in Victoria and Queensland show jurisdictions moving independently. It should be acknowledged that much of

the variation here arises from broader privacy, surveillance and criminal-law policy rather than from drone regulation, which is why harmonisation is slow and why a model provision confined to drone operation is more achievable than a general alignment.

5. Address drone cyber security and data standards

Owner: The Cyber and Infrastructure Security Centre, with CASA.
Obstacle: The legitimate industry is fast-growing and cost-sensitive, and CASA's remit is aviation safety rather than data security.

What is needed is published guidance and, over time, design and data-handling expectations that a procuring agency can cite in a tender. CASA identified this as an immediate priority in 2022 and Australian regulation still covers registration and pilot licensing, not design or security.[200]

6. Set expectations for Remote ID honestly

Owner: CASA.
Obstacle: Remote ID will be presented publicly as a solution to malicious drone use, which it is not.

Remote ID should be positioned publicly as a filtering mechanism that clears cooperative traffic out of the ambiguous category so that finite response capacity can be directed at what remains.

15.4 Closing remarks

One observation remains that the preceding sections do not make.

In every case examined here, the target's planners had reasons (often good ones) for believing they were not at risk, and in every case those reasons were about the adversary rather than about themselves. Russian base commanders reasoned about Ukrainian reach. Israeli border planners reasoned about what Hamas could field. The 2024 and 2025 sighting waves were argued about almost entirely in terms of who was flying. That framing is ineffective, because it makes preparedness contingent on a judgement about intent that, on this record, is usually never resolved. The organisations that came out of these events best were not the ones that guessed the adversary correctly; they were the ones whose plans did not require them to.

This paper should be read as a snapshot of a fast-moving field, not a final word on it, and it is deliberately dated on the cover for that reason. Even during writing, multiple sections needed to be updated with new information. Its specific content will date faster than the questions in Appendix A, which are the part intended to stay useful.

[200] Cyber Security Cooperative Research Centre, *Flight Critical: Drones, Cyber Security and Critical…*, see reference 49.

Appendix A — Scenario planning and self-assessment

The scenarios below are fictional and illustrative. Their purpose is to give readers a concrete example against which to test their own organisation's preparedness. The self-assessment questions that follow are the actual deliverable of this appendix.

The facility

Simpson Regional Airport, a fictional composite, serves a mid-sized Australian coastal city. It handles approximately 2.2 million passengers annually with scheduled domestic jet services, and includes a general aviation precinct, an air freight and logistics zone adjacent to the main runway, and a co-located Australian Defence Force flying training squadron sharing the airfield under a joint-use agreement. The airport sits within controlled airspace, has invested in a basic RF detection system over the past two years, and, like the great majority of Australian facilities of its size, has no jamming or active mitigation capability, consistent with the restrictions described at section 13.2.

Scenario 1: The unaware operator

On a clear Saturday afternoon, a member of the public flying a consumer drone from a nearby park to photograph a local landmark drifts, without realising it, inside the airport's controlled zone. The RF detection system picks up the controller signal, and a controller separately receives a visual report from an inbound regional aircraft on approach. The drone is at low altitude, moving slowly, and circling a single point in a manner consistent with framing a photograph rather than surveying the airfield.

Plausible consequences. One or two inbound flights are placed in a short hold while air traffic control assesses the risk. In most cases no go-around is required, but a low-probability, high-consequence near-miss cannot be excluded until the drone is confirmed clear of the approach path. The incident is over within thirty to sixty minutes. Direct costs are modest (fuel burn from holding, staff time, a report to CASA), but the incident consumes real security and air traffic control attention.

Scenario 2: The reconnaissance pattern

Over three consecutive nights, a drone is detected at dusk making slow, repeated passes along the perimeter fence adjacent to the freight and logistics zone, and separately along the boundary of the co-located ADF squadron's apron. The behaviour is inconsistent with recreational flying and consistent with deliberate observation. On each occasion the operator cannot be located, the drone departs before security personnel can respond, and no payload is confirmed. Nothing is damaged and no one is harmed.

Plausible consequences. The direct physical impact is zero, which is what makes this harder to manage than Scenario 1, not easier. The airport is left with an unresolved attribution question (activist, competitor of a freight tenant, someone probing for a future smuggling opportunity, or something more serious) and no reliable way to answer it. Whether this pattern meets the threshold for a reportable incident under the SOCI Act is a question for the airport's legal and compliance function, and the scenario is designed to surface that it is a

question, not to answer it. The defence squadron's presence adds a further complication: a surveillance pattern against a military asset sits in a different legal and intelligence-referral category than the same pattern against a civilian freight tenant, and the airport's security team may have no pre-agreed view of which agency to notify, or when.

Note also the failure mode this scenario is designed to expose. If the three nights are logged by three different shift supervisors as three separate minor incidents, the pattern may not be recognised at all.

Scenario 3: The fast approach

During a period of high passenger movement, an FPV-style drone carrying a small payload approaches the airport at low altitude and high speed from outside the perimeter, consistent in general profile with tactics documented in this paper's international case studies. This paper does not speculate on the construction, guidance or launch method involved.

What matters here is response latency. Detection-to-impact for a fast-moving FPV airframe is measured in seconds rather than the minutes available in Scenarios 1 and 2. The entire chain has to complete inside a window shorter than most civilian escalation procedures are written for, and shorter than the time it takes to reach a named decision-maker by telephone. Even at a site holding full mitigation authority, which this one does not, the window would be inadequate unless the decision had been delegated in advance.

That is the useful conclusion from this scenario, and it is a governance one, not a technical one: where response latency is measured in seconds, the response is limited to whatever has already been decided and delegated in advance.

Plausible consequences. Depending on the target and timing, physical consequences could range from equipment damage through to a mass casualty incident. Regardless of the physical outcome the operational consequence is immediate and severe: airspace closure, a multi-week investigation involving state and federal police, a SOCI Act notification, national media coverage, and, echoing section 9.4, a national consequence extending well beyond just the airport, as every comparable Australian facility is forced to reassess its exposure to the same tactic.

Scenario 4: The ambiguous week

Over eight days, staff at Simpson Airport report eleven drone sightings. The RF detection system corroborates three of them. Two reports come from pilots on approach, one from a member of the public, and the remainder from airport staff. No drone is ever photographed. Local media picks the story up on day four. On day six a state MP calls for the airport to be closed until the matter is resolved.

Plausible consequences. This is Gatwick and the 2024 United States sightings combined, and it is the scenario Australian facilities are most likely to face. The airport cannot prove a drone is present and cannot prove one is not. Every operational decision must be made on incomplete information, under public and political pressure, with a media narrative running ahead of the facts. The costs are entirely disruption and reputation. The controls that matter are the ability

to state clearly and consistently what is and is not known, an agreed threshold for suspending and resuming operations, and a single spokesperson who has been briefed in advance.

Self-assessment questions

The value of the scenarios above lies in the questions they should prompt a reader to ask of their own organisation. There are twelve questions below that are likely to expose a gap, and they can be worked through in a meeting rather than a project.

- If a drone were reported over our site in the next hour, who would be told, and how long would that take?
- Would we detect it at all, or would our first indication be a phone call from a member of the public, a pilot or a staff member?
- If we have detection, has its real-world coverage been independently tested, or only demonstrated by the vendor under controlled conditions — and would it see a drone that is not transmitting on RF?
- Can we distinguish our own authorised drone from someone else's within one minute?
- Who holds the decision to stop operations, and can that person be reached at 2am on a public holiday?
- Do we have a written threshold separating monitor, notify police and activate crisis response — or would that judgement be made from scratch, under pressure, by whoever is on shift?
- Does our escalation plan still work if we never find out who was flying it?
- What is our response latency for a fast approach, and does our escalation path fit inside it?
- Do we know specifically which response options we are permitted to use, by whom and under what authorisation — or are we assuming a capability is lawfully available because it is commercially available?
- Who maintains the record that would let us recognise three sightings over three weeks as one pattern rather than three nuisances?
- What is our rule for declaring an unresolved incident over and resuming operations?
- Who speaks publicly, and what would they say on the information we would actually have?

An organisation that can answer all twelve is meaningfully ahead of where most comparable Australian facilities sit. An organisation that cannot has, at minimum, a specific starting point for the security planning process.

Appendix B — Glossary

The terms below are used throughout this paper in their conventional sense. The threat and hazard distinction, which is not conventional and carries an argument, is set out at section 1.4.

- **ACMA** — Australia Communications and Media Authority; Government agency regulating broadcasting, telecommunications, radiocommunications and online content in Australia (section 13.2)
- **BVLOS / VLOS** — beyond visual line of sight and within visual line of sight: the regulatory distinction between operations the remote pilot can and cannot see directly (section 13.1).
- **C-UAS** — counter-UAS: the detection and response technologies and doctrine covered in Part IV.
- **FPV** — first-person view: a drone flown by a pilot watching a live video feed through goggles rather than by direct line of sight. Fast, agile and cheap, and the platform in most of the attack cases in Part II.
- **GNSS** — global navigation satellite system, of which GPS is the best known. Most commercial drones depend on it for navigation and position-holding.
- **Hard kill** — physical destruction or capture of a drone, using interceptors, directed energy or kinetic effectors (section 12.4).
- **Kill chain** — the sequence of detect, track, identify, decide, respond and adapt that structures Part IV.
- **Loitering munition** — an uncrewed aircraft that circles a target area before being directed onto a target, or in more autonomous systems selecting one itself.
- **One-way attack drone** — a drone destroyed on impact, differing from a loitering munition in endurance and guidance rather than in principle.
- **RF** — radio frequency: the link between a drone and its operator, and a primary detection vector (section 11.2).
- **Soft kill** — non-destructive mitigation, such as jamming or protocol takeover (section 12.3).
- **SOCI Act** — the *Security of Critical Infrastructure Act 2018* (Cth), as amended in 2021 and 2022, which imposes the obligations described at section 13.5.
- **sUAS** — small UAS: the category of aircraft this paper concerns.
- **Swarm** — multiple drones operating together, usually to overwhelm a defender's capacity to engage them individually (sections 5.7 and 12.7).
- **UAS / UAV / RPAS** — uncrewed aircraft system, uncrewed aerial vehicle and remotely piloted aircraft system. Used interchangeably across the sources cited here.

References

Sources are listed alphabetically and numbered. In the footnotes the article title carries the link; here the full address is printed in each entry. Repeat citations in the footnotes are given in short form and cross-reference the numbered entry below.

1. ABC News, “Albanese government turns defence sights north, completing $355m upgrade to RAAF Base Tindal,” 28 January 2026. https://www.abc.net.au/news/2026-01-28/government-completes-upgrade-raaf-base-tindal/106275670

2. ABC News, “Anger after drones ground water bombers at Manypeaks bushfire in WA,” 15 January 2025. https://www.abc.net.au/news/2025-01-15/recreational-drones-ground-water-bombers-battling-fire-wa/104815554

3. ABC News, “Drone with $1 million worth of contraband intercepted at Townsville prison,” 28 May 2026. https://www.abc.net.au/news/2026-05-28/million-dollars-of-drone-contraband-at-townsville-prison/106732504

4. ABC News, “Drones breach restricted airspace at Williamtown RAAF base,” 20 August 2026, reporting the New South Wales Police confirmation of a second incursion in early August 2026, that investigations into both episodes were continuing with no arrests or charges, and Prime Minister Anthony Albanese’s comment that it is “unsafe and dangerous to have drones around airspace.” https://www.abc.net.au/news/2026-08-20/drones-breach-restricted-airspace-at-williamtown-raaf-base/107056708

5. ABC News, “Drones cause waterbombing to stop at bushfire in WA’s south-east,” 3 March 2019. https://www.abc.net.au/news/2019-03-03/drones-stop-waterbombing-at-esperance-fire/10865864

6. ABC News, “From food to medical supplies — what could the future of drone delivery look like in Australia?”, 23 February 2024, recording Wing’s world-first Canberra service established in 2019 and its subsequent concentration on Logan, and Zipline’s medical delivery network. https://www.abc.net.au/news/2024-02-23/the-future-of-medical-and-food-drone-delivery-in-australia/103499576

7. ABC News, “Greenpeace intentionally crashes drone into French nuclear power plant to reveal security vulnerability,” July 2018. https://abcnews.go.com/International/greenpeace-intentionally-crashes-drone-french-nuclear-power-plant/story?id=56343027

8. ABC News, “Two subsea communication cables damaged off Perth coast in ‘concerning development’,” 11 August 2026. https://www.abc.net.au/news/2026-08-11/subsea-cable-damaged-off-perth-coast-in-protection-zone/107021436

9. ABC News, “Why drones fell from the sky during Sydney’s Vivid light show,” 27 May 2026; and “Vivid Sydney drone shows cancelled for now after malfunction saw 89 drones fall into the harbour,” 26 May 2026. https://www.abc.net.au/news/2026-05-27/sydney-vivid-festival-drone-failure-explainer/106724050

10. Airprox Reality Check, “Gatwick 2018,” a documentary review assembled from UK Airprox Board records, National Police Air Service flight records, Ministry of Defence and Sussex Police freedom-of-information responses, and Civil Aviation Authority and Department for Transport correspondence. https://www.airproxrealitycheck.org/gatwick2018/

11. Airservices Australia, “Drones and Uncrewed Aircraft Systems Traffic Management.” https://www.airservicesaustralia.com/about-us/innovation-and-technology/drones-and-uncrewed-aircraft-systems-traffic-management/

12. Al Jazeera, “Munich airport resumes operations after more drone sightings halted flights,” 4 October 2025. https://www.aljazeera.com/news/2025/10/4/munich-airport-resumes-operations-after-more-drone-sightings-halted-flights

13. Anduril Industries, “Anduril Unveils Roadrunner and Roadrunner-M,” 1 December 2023, describing a twin-jet vertical take-off and landing interceptor that returns and lands when not committed to an engagement. https://www.anduril.com/article/anduril-unveils-roadrunner-and-roadrunner-m/

14. *Arab News*, “Saudi Arabia’s Defense Ministry displays Iranian drones, cruise missiles used in Aramco attacks,” reporting Col. Turki Al-Maliki’s press conference account of eighteen drones and three cruise missiles against Abqaiq and four missiles against Khurais. https://www.arabnews.com/node/1556271/saudi-arabia

15. Armed Conflict Location & Event Data Project, “The war from the sky: How drone warfare is shaping the conflict in Myanmar,” 2025. https://acleddata.com/report/war-sky-how-drone-warfare-shaping-conflict-myanmar

16. Arms Control Association, *Arms Control Today*, “Drone Incursions in Belgium Spark Probes, NATO-EU Response,” December 2025. https://www.armscontrol.org/act/2025-12/news/drone-incursions-belgium-spark-probes-nato-eu-response

17. Associated Press, “Confusion gripped US base defenders as a flying bomb struck a deadly blow at Tower 22, investigation says,” reporting the findings of the United States military investigation into the 28 January 2024 attack. https://apnews.com/article/tower-22-drone-attack-investigation-jordan-8ba39d09b6ea5d7cbaebaa9a4a1e0a2e

18. Associated Press, “Drone with explosives found at German airport, official sees ‘new quality’ of threat,” 6 August 2026, reporting the discovery of the device at Leipzig/Halle Airport and Interior Minister Alexander Dobrindt’s initial response. The Federal Prosecutor dates the incident itself to the evening of 4 August 2026. https://www.npr.org/2026/08/06/g-s1-137571/germany-drone-explosives-airport

19. Associated Press, “Germany blames Russia for attempted drone attack at Leipzig airport,” 1 September 2026, reporting the joint statement of Interior Minister Alexander Dobrindt and Foreign Minister Johann Wadephul, the characterisation of the perpetrators as lower-level operatives acting on behalf of Russian state entities, the

closure of the Russian Consulate General in Bonn and the Russian House in Berlin, and Russia's rejection of the finding. https://www.pbs.org/newshour/world/germany-blames-russia-for-attempted-drone-attack-at-leipzig-airport

20. Atlantic Council, "Fiber-optic drones have emerged as critical kit for both Russia and Ukraine," UkraineAlert. https://www.atlanticcouncil.org/blogs/ukrainealert/fiber-optics-drones-have-emerged-as-critical-kit-for-both-russia-and-ukraine/

21. Austin C. Doctor, Suat Cubukcu, Joel Elson, George Grispos and Mackenzie Harms, "Mapping Weaponized Drone Attacks Attributed to Mexican Drug Cartels, 2021–2025," National Counterterrorism Innovation, Technology, and Education Center, University of Nebraska at Omaha, 12 February 2026. https://digitalcommons.unomaha.edu/nctereportsresearch/150/

22. Australian Aviation, "Australia must learn from Williamtown drone incident, experts say," 11 August 2026, reporting Defence Minister Pat Conroy's confirmation of the incident on ABC Newcastle on 10 August 2026 and expert commentary from Dr Oleksandra Molloy, Robert Potter and Jennifer Parker. https://australianaviation.com.au/2026/08/australia-must-learn-from-williamtown-drone-incident-experts-say/

23. Australian Aviation, "Drone incidents at Victorian prisons rise 250%," November 2020, reporting freedom-of-information data obtained by *The Age*. https://australianaviation.com.au/2020/11/drone-incidents-at-victorian-prisons-rise-250/

24. Australian Communications and Media Authority, "Exemptions for banned equipment," describing the section 27 exemption pathway and current determinations including the *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022*. https://www.acma.gov.au/exemptions-banned-equipment

25. Australian Communications and Media Authority, "Jammers are illegal in Australia," setting out the permanent ban under subsection 172(3) of the *Radiocommunications Act 1992* and the applicable penalties. https://www.acma.gov.au/jammers-are-illegal-australia

26. Australian Federal Police, "AFP and CASA warn of drone usage around Cairns Airport." https://www.afp.gov.au/news-centre/media-release/afp-and-casa-warn-drone-usage-around-cairns-airport

27. Australian Government, Drones.gov.au, "Security policy," describing the *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022*, work on agency access to counter-drone capability, and the Drone Rule Digitisation project. https://www.drones.gov.au/policies-and-programs/policies/security-policy

28. Australian National Audit Office, *Administration of Critical Infrastructure Protection Policy*, recording that amendments to the *Security of Critical Infrastructure Act 2018* expanded the asset classes covered from four to twenty-two across eleven sectors.

https://www.anao.gov.au/work/performance-audit/administration-critical-infrastructure-protection-policy

29. Australian Securities and Investments Commission, media release 22-104MR, "Court finds RI Advice failed to adequately manage cybersecurity risks," 5 May 2022. The judgment in *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496 is also available. https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-104mr-court-finds-ri-advice-failed-to-adequately-manage-cybersecurity-risks

30. Australian Security Intelligence Organisation, "Director-General's Annual Threat Assessment 2025," delivered 19 February 2025. https://www.asio.gov.au/director-generals-annual-threat-assessment-2025

31. Australian Security Intelligence Organisation, "Director-General's Annual Threat Assessment 2026," delivered 24 June 2026; the compromise of an Australian critical infrastructure provider's network and the phrase "cripple it at a time of their choosing" were reported from the address by *The Register*, 25 June 2026. https://www.asio.gov.au/resources/speeches-and-statements/director-generals-annual-threat-assessment-2026

32. Australian Strategic Policy Institute, "Australia is flying blind on Chinese drone data," *The Strategist*. https://www.aspistrategist.org.au/australia-is-flying-blind-on-chinese-drone-data/

33. Australian Strategic Policy Institute, "Legislation, not technology, is the biggest problem for ADF drone defence," *The Strategist*. https://www.aspistrategist.org.au/legislation-not-technology-is-the-biggest-problem-for-adf-drone-defence/

34. Australian Submarine Agency, "Upgrades at HMAS Stirling pave the way for Submarine Rotational Force-West." https://www.asa.gov.au/news/upgrades-hmas-stirling-pave-way-submarine-rotational-force-west

35. Center for Strategic and International Studies, "Calculating the Cost-Effectiveness of Russia's Drone Strikes." https://www.csis.org/analysis/calculating-cost-effectiveness-russias-drone-strikes

36. Center for Strategic and International Studies, "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare," 2025. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

37. Center for Strategic and International Studies, "Russia's Shadow War Against the West," 18 March 2025, recording three attributed attacks in Europe in 2022, twelve in 2023 and thirty-four in 2024 against a three-source evidentiary standard. https://www.csis.org/analysis/russias-shadow-war-against-west

38. Center for Strategic and International Studies, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense." https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense

39. Civil Aviation Safety Authority, *CASR Part 101 Plain English Guide — Micro and Excluded RPA Operations*, setting out the weight categories and the standard operating conditions. https://www.casa.gov.au/sites/default/files/2021-08/part-101-micro-excluded-rpa-operations-plain-english-guide.pdf

40. Civil Aviation Safety Authority, "Drone safety rules," covering registration, accreditation, weight thresholds and operating requirements. https://www.casa.gov.au/drones/drone-rules/drone-safety-rules

41. Civil Aviation Safety Authority, "Help find rogue western Sydney drone," 2020, appealing for information after a pilot on approach to Sydney Airport reported a drone at approximately 1,200 metres altitude over western Sydney. https://www.casa.gov.au/about-us/news-media-releases-and-speeches/help-find-rogue-western-sydney-drone

42. Civil Aviation Safety Authority, "Part 101 of CASR — Unmanned aircraft and rockets." https://www.casa.gov.au/rules/regulatory-framework/casr/part-101-casr-unmanned-aircraft-and-rockets

43. CNN, "Denmark links drones at Copenhagen airport to hybrid attacks across Europe," 23 September 2025, reporting the Copenhagen and Oslo closures, Prime Minister Mette Frederiksen's statement and the Danish police assessment. https://edition.cnn.com/2025/09/23/europe/denmark-drones-hybrid-attacks-intl

44. Combating Terrorism Center at West Point, "The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft." https://ctc.westpoint.edu/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft/

45. Congressional Research Service, "Attacks on Saudi Oil Facilities: Effects and Responses," In Focus IN11173, 2019. https://www.everycrsreport.com/reports/IN11173.html

46. Crown Prosecution Service, "How the CPS used new National Security Act legislation to prosecute the plot to sabotage Ukrainian aid warehouses on UK soil," updated with sentencing, 24 October 2025. https://www.cps.gov.uk/cps/news/updated-sentence-how-cps-used-new-national-security-act-legislation-prosecute-plot

47. Cyber and Infrastructure Security Centre, "Security of Critical Infrastructure Act 2018 — obligations factsheet," setting out the sectors, asset classes and Positive Security Obligations including risk management program and reporting requirements. https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-soci-obligations.pdf

48. Cyber and Infrastructure Security Centre, version 2.0, February 2026, *Critical Infrastructure Annual Risk Review — Energy Sector*. https://www.cisc.gov.au/resources-subsite/Documents/raa-energy.pdf

49. Cyber Security Cooperative Research Centre, *Flight Critical: Drones, Cyber Security and Critical Infrastructure*, 2024. https://cybersecuritycrc.org.au/remote-assets/sites/default/files/2024-05/Flight%20Critical.pdf

50. Cybersecurity and Infrastructure Security Agency, *Protecting Against the Threat of Unmanned Aircraft Systems*, November 2020, which treats protocol manipulation and control-link takeover as techniques distinct from radio frequency jamming. https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf

51. Dedrone, "Australian Police protect major events from drone threats," describing deployments at the 2024 Australian Open, Australian Formula One Grand Prix, MCG concerts, the ASEAN Summit and Land Forces 2024. https://www.dedrone.com/customers/australian-police

52. *Defence Amendment (Counter-UxS Measures) Regulations 2025* (Cth), F2025L01553, registered 12 December 2025. https://www.legislation.gov.au/F2025L01553/asmade

53. *Defense News*, "Anduril lands $250 million Pentagon contract for drone defense system," 8 October 2024. https://www.defensenews.com/unmanned/2024/10/08/anduril-lands-250-million-pentagon-contract-for-drone-defense-system/

54. Deloitte Access Economics, *Economic Benefit Analysis of Drones in Australia*, report for the Department of Infrastructure, Transport, Regional Development and Communications, 23 October 2020, projecting a $14.5 billion expansion in Australian real GDP to 2040 under a medium uptake scenario, $9.3 billion in direct cost savings in present-value terms at a 7 percent real discount rate, and 5,500 full-time-equivalent jobs a year on average. https://www.infrastructure.gov.au/sites/default/files/documents/economic-benefit-analysis-of-drones-to-australia-final-report.pdf

55. Department of Defence, "Army tests counter-drone technology," 24 December 2025, describing Exercise Southern Arrow at Cultana and its live-fire demonstration as the first iteration of the LAND 156 schedule. https://www.defence.gov.au/news-events/news/2025-12-24/army-tests-counter-drone-technology

56. Department of Homeland Security, Federal Bureau of Investigation, Federal Aviation Administration and Department of Defense, "Joint Statement on Ongoing Response to Reported Drone Sightings," 16 December 2024. https://www.faa.gov/newsroom/dhs-fbi-faa-dod-joint-statement-ongoing-response-reported-drone-sightings

57. Department of Justice and Community Safety Victoria, "Drone ban near Victorian correctional and youth justice facilities," in force from 1 February 2018. https://www.justice.vic.gov.au/drone-ban-near-victorian-correctional-and-youth-justice-facilities

58. Der Generalbundesanwalt beim Bundesgerichtshof, "Übernahme der Ermittlungen nach Drohnenfund am Flughafen Leipzig/Halle," 6 August 2026, recording the assumption of jurisdiction on grounds of the case's particular significance, investigation for attempted causing of an explosion and dangerous interference with air traffic, and a drone carrying professional explosive and a detonator. No suspect or foreign state is named in

the release.
https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2026/Pressemitteilung-vom-06-08-2026.html

59. DroneShield Limited, *Annual Report for the Year Ended 31 December 2025* (ASX: DRO), recording a Sydney registered office, distribution across more than seventy countries, the June 2016 ASX listing and Oleg Vornik's appointment as chief executive in January 2017. https://www.droneshield.com/investors

60. Egmont Institute, "Belgium's Public Confrontation with Hybrid Threats: Lessons from Drone Incursions." https://egmontinstitute.be/belgiums-public-confrontation-with-hybrid-threats-lessons-from-drone-incursions/

61. Epirus, "Epirus' Leonidas Demonstrates Successful Use of High-Power Microwave to Defeat Fiber-Optic Controlled UAS," describing a December 2025 demonstration. https://www.epirusinc.com/press-releases/epirus-leonidas-demonstrates-successful-use-of-high-power-microwave-to-defeat-fiber-optic-controlled-uas

62. Epirus, "Epirus' Leonidas High-Power Microwave Defeats 49-Drone Swarm, 100% of Drones Flown at Live-Fire Demonstration," 10 September 2025, reporting a demonstration conducted on 26 August 2025. Manufacturer-reported; no independent verification is available. https://www.epirusinc.com/press-releases/epirus-leonidas-high-power-microwave-defeats-49-drone-swarm-100-of-drones-flown-at-live-fire-demonstration

63. Euronews, "Egypt's Suez Canal revenue fell sharply in 2024 on regional tensions," 17 April 2025, reporting Suez Canal Authority figures. https://www.euronews.com/business/2025/04/17/egypts-suez-canal-revenue-fell-sharply-in-2024-on-regional-tensions

64. European Union Aviation Safety Agency, "EASA and IATA outline comprehensive plan to mitigate GNSS interference risks." https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-and-iata-outline-comprehensive-plan-mitigate-gnss

65. EVN Report, "Beyond the Drone Hype: Unpacking Nagorno-Karabakh's Real Lessons." https://evnreport.com/opinion/beyond-the-drone-hype-unpacking-nagorno-karabakhs-real-lessons/

66. *Forbes Australia*, "How DroneShield went from zapping mosquitos to dropping drones." https://www.forbes.com.au/news/innovation/how-droneshield-went-from-zapping-mosquitos-to-dropping-drones/

67. *Forbes*, David Hambling, "Ukraine's AI Drones Seek And Attack Russian Forces Without Human Oversight," 17 October 2023. https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/

68. *Fortune*, "Gatwick's December Drone Closure Cost Airlines $64.5 Million," 22 January 2019, recording around £50 million in airline costs, easyJet's £15 million, more than

1,000 cancellations, approximately 140,000 passengers affected and a 33-hour closure. https://fortune.com/2019/01/22/gatwick-drone-closure-cost/

69. France 24, "Tests expose worrying flaws in France's anti-drone system for 2024 Olympics," 19 April 2024, reporting the Coubertin exercise results and the assessment of independent defence consultant Marc Chassillan on urban radar performance and swarm saturation. https://www.france24.com/en/sport/20240419-tests-expose-worrying-flaws-in-france-s-anti-drone-system-for-2024-olympics

70. House of Commons Defence Committee, *Defence in the Grey Zone*, Fifth Report of Session 2024–25, 9 July 2025. https://publications.parliament.uk/pa/cm5901/cmselect/cmdfence/405/report.html

71. *Kyiv Independent*, "Operation Spiderweb — everything we know about Ukraine's 'audacious' attack on Russia's heavy bombers," 2 June 2025, recording the Security Service of Ukraine's claim of 41 aircraft, around a third of Russia's cruise missile bomber fleet, and damage of approximately US$7 billion. https://kyivindependent.com/operation-spiderweb-everything-we-know-about-ukraines-audacious-attack-on-russias-heavy-bombers/

72. Michael Knights and Conor Hiney, "Plugging the Gaps in Saudi Arabia's Air Defenses," The Washington Institute for Near East Policy, 25 September 2019, recording that Saudi batteries mostly faced east and lacked 360-degree coverage, and that legacy systems built against aircraft would struggle against smaller, slower cruise missiles and drones. https://www.washingtoninstitute.org/policy-analysis/plugging-gaps-saudi-arabias-air-defenses

73. Middle East Institute, "The October 7 Hamas attack: An Israeli overreliance on technology?" https://mei.edu/publication/october-7-hamas-attack-israeli-overreliance-technology/

74. Ministère des Armées, "JOP 24 — bilan de la sécurisation aérienne des Jeux Olympiques," 19 August 2024, and the ministry's closing statement of 11 September 2024, recording 88 aircraft interceptions and 85 drone remote pilots apprehended across the Games, most of them not acting maliciously. https://www.defense.gouv.fr/operations/actualites/jop-24-bilan-securisation-aerienne-jeux-olympiques

75. National Security and Defence Council of Ukraine, "Results of Ukraine's Defense Industry in 2025: FPV Drones." https://www.rnbo.gov.ua/en/Diialnist/7370.html

76. Netherlands Ministry of Defence, "Optreden tegen drones boven vliegbasis Volkel," 22 November 2025, confirming that air force personnel deployed ground-based weapons, after which the drones departed, and that no further information on detection or countermeasures would be released. https://www.defensie.nl/actueel/nieuws/2025/11/22/optreden-tegen-drones-boven-vliegbasis-volkel

77. New South Wales Government, “Major boost to shark-spotting drones to improve beach safety with $120 million shark program,” 28 June 2026, recording the $34 million drone allocation within a $120 million program. https://www.nsw.gov.au/ministerial-releases/major-boost-to-shark-spotting-drones-to-improve-beach-safety-120-million-shark-program

78. *Newcastle Herald*, “RAAF Williamtown: drones reportedly breached restricted airspace,” 10 August 2026, carrying the Department of Defence statement on uncrewed aircraft near Newcastle Airport and RAAF Base Williamtown between 11 and 13 July 2026, the referral to the New South Wales Police Counter-UAS Unit, and Defence Minister Pat Conroy’s refusal to detail the response. https://www.newcastleherald.com.au/story/9327002/raaf-williamtown-drones-reportedly-breached-restricted-airspace/

79. NL Times, “Dutch military opens fire on unidentified drones over Volkel air base,” 22 November 2025. https://nltimes.nl/2025/11/22/dutch-military-opens-fire-unidentified-drones-volkel-air-base

80. Office of the Australian Information Commissioner, “Statutory tort for serious invasions of privacy,” commenced 10 June 2025. https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/statutory-tort-for-serious-invasions-of-privacy

81. Oleg Vornik, chief executive of DroneShield, “Like the US, Australia remains badly unprepared for drone threats,” Australian Strategic Policy Institute, *The Strategist*, 27 August 2024. https://www.aspistrategist.org.au/like-the-us-australia-remains-badly-unprepared-for-drone-threats/

82. Opex360 (Zone Militaire), “Les fusiliers marins de la base sous-marine de l’Île Longue ont tenté d’abattre des drones inconnus,” 5 December 2025, placing the overflight at about 7.30pm on 4 December and recording that drones reported over the Crozon peninsula on 17–18 November had not overflown military installations. https://www.opex360.com/2025/12/05/les-fusiliers-marins-de-la-base-sous-marine-de-lile-longue-ont-tente-dabattre-des-drones-inconnus/

83. Ports Australia, “Pilbara Ports,” describing Dampier and Port Hedland as handling approximately 77 percent of Australia’s and 42 percent of the world’s iron ore trade. https://www.portsaustralia.com.au/members/pilbara-ports

84. Queensland Corrective Services, “Drone incursion sends Capricornia into lockdown,” December 2019. https://corrections.qld.gov.au/drone-incursion-sends-capricornia-into-lockdown/

85. Queensland Corrective Services, undated statement, “High security prisons locked down after drone incursion.” https://corrections.qld.gov.au/high-security-prisons-locked-down-after-drone-incursion/

86. *Radiocommunications (Exemption — Remotely Piloted Aircraft Disruption) Determination 2022* (Cth), F2022L01255, registered 26 September 2022, section 8 of which exempts a member of a police force, defined to include the Australian Federal

Police and the police force of each state and territory. https://www.legislation.gov.au/F2022L01255/asmade/text

87. Robin Radar Systems, "10 Types of Counter-Drone Technology to Detect and Stop Drones Today," vendor technical guidance; the performance ranges quoted are the manufacturer's. https://www.robinradar.com/resources/10-counter-drone-technologies-to-detect-and-stop-drones-today

88. Rory Cormac and Richard J. Aldrich, "Grey is the new black: covert action and implausible deniability," *International Affairs* 94, no. 3 (May 2018): 477–494. https://academic.oup.com/ia/article/94/3/477/4992414

89. Royal Australian Air Force, "RAAF Base Williamtown," recording that Newcastle Airport operates from RAAF Base Williamtown under a lease with Defence, and that the base hosts the F-35A Lightning II squadrons of Air Combat Group. https://www.airforce.gov.au/about-us/bases/raaf-base-williamtown

90. Royal United Services Institute, "Responding to Russian Sabotage Financing," 14 January 2026. https://www.rusi.org/explore-our-research/publications/insights-papers/responding-russian-sabotage-financing

91. Second Line of Defense, "The PARADE Anti-Drone System and the Paris Olympic Games," January 2024; and Breaking Defense, "France takes aim at unmanned systems, taking lessons from Paris Olympics," November 2024. https://sldinfo.com/2024/01/the-parade-anti-drone-system-and-the-paris-olympic-games/

92. Security Service (MI5), "Director General Sir Ken McCallum gives threat update," 16 October 2025. https://www.mi5.gov.uk/director-general-sir-ken-mccallum-gives-threat-update

93. "Standardized Evaluation of Counter-Drone Systems: Methods, Technologies, and Performance Metrics," *Drones*, vol. 9, no. 5, 2025. https://www.mdpi.com/2504-446X/9/5/354

94. Sussex Police, as reported in *The Register*, "Sussex Police gives up on £790k Gatwick drone shutdown probe," 27 September 2019, recording 129 reports of drone activity of which 109 came from credible witnesses including pilots and airport staff, sightings in twelve groupings across a 30-hour shutdown, and Assistant Chief Constable Dave Miller's statement closing the investigation. https://www.theregister.com/2019/09/27/gatwick_drone_probe_closed_sussex_police/

95. Tejera-Berengue et al., "Analysis of Distance and Environmental Impact on UAV Acoustic Detection," *Electronics* 13, no. 3 (2024): 643, reporting effective acoustic detection to about 300 metres for most machine-learning detectors and 500 metres for a deep-learning detector, degraded by spectrally similar background noise. https://www.mdpi.com/2079-9292/13/3/643

96. The Hon Mark Ryan MP, Queensland Minister for Police and Corrective Services, "New regulation brings down drones," 15 February 2018, recording a maximum penalty of two years' imprisonment or a $12,615 fine for being caught with a drone at a correctional facility. https://statements.qld.gov.au/statements/83735

97. The Hon Pat Conroy MP and the Hon Peter Khalil MP, "Government boosts response to drone threats," 29 January 2026, announcing the *Defence Amendment (Counter-UxS Measures) Regulations 2025* and the LAND 156 counter-small-UAS industry panel. https://www.minister.defence.gov.au/media-releases/2026-01-29/government-boosts-response-drone-threats

98. The Hon Pat Conroy MP, Minister for Defence Industry, "Albanese Government to invest up to $7 billion in counter drone defence," 21 April 2026. https://www.minister.defence.gov.au/media-releases/2026-04-21/albanese-government-invest-up-7-billion-counter-drone-defence

99. *The Register*, "Sussex Police gives up on £790k Gatwick drone shutdown probe," 27 September 2019. https://www.theregister.com/2019/09/27/gatwick_drone_probe_closed_sussex_police/

100. *The Register*, "Wi-Fi spy drones used to snoop on financial firm," 12 October 2022. https://www.theregister.com/2022/10/12/drone-roof-attack/

101. The War Zone, "Australian Airbase Gets Upgrades For American Bomber Deployments," 31 October 2022, describing the United States-funded apron expansion and squadron facilities then in design. https://www.twz.com/australian-airbase-gets-upgrades-for-american-bomber-deployments

102. The War Zone, "Drone Swarms Over Langley AFB Didn't Surprise General In Charge Of NORAD," reporting the December 2023 Langley incursions and retired General Glen VanHerck's assessment of detection and authority gaps. https://www.twz.com/news-features/former-norad-boss-wasnt-surprised-by-langley-afb-drone-incursions

103. The War Zone, "Nuclear Submarine Base Drone Incursion Prompts French Military Response," reporting the 5 December 2025 overflight of Île Longue, the use of a jammer by the marine rifle battalion responsible for base security, and the failure to bring down any of the five drones. https://www.twz.com/news-features/nuclear-submarine-base-drone-incursion-prompts-french-military-response

104. *The Week*, "Gatwick drone sightings 'cost airport and airlines £50m'," recording more than 1,000 flights affected across a 33-hour closure. https://theweek.com/99127/gatwick-drone-sightings-cost-airport-and-airlines-50m

105. United States Senate Committee on Armed Services, *Stenographic Transcript: Hearing to Receive Testimony on the Posture of United States Northern Command and United States Southern Command*, 13 February 2025, recording General Gregory Guillot's evidence on 350 drone detections across 100 military installations in 2024 and his request for

authority extending beyond the installation boundary. https://www.armed-services.senate.gov/imo/media/doc/02-13-2025-full-transcript.pdf

106. Unmanned Airspace, “Airservices Australia publishes tender for drone surveillance network covering 29 airports,” 22 September 2023, reporting the Airservices approach to market and quoting the *Australian Aviation Network Overview* on detections in airport no-fly zones. https://www.unmannedairspace.info/counter-uas-systems-tenders/airservices-australia-publishes-tender-for-drone-surveillance-network-covering-29-airports/

107. Unmanned Airspace, “DroneShield integrates Sentrycs cyber takeover capability to DroneSentry.” https://www.unmannedairspace.info/counter-uas-systems-and-policies/droneshield-integrates-sentrycs-cyber-takeover-capability-to-dronesentry/

108. Unmanned Airspace, “Multiple unidentified drones reported over Australian F-35 base,” reporting the Department of Defence statement that multiple uncrewed aircraft systems were confirmed in restricted airspace over RAAF Base Williamtown on 11–13 July 2026 and that the incidents were referred to the New South Wales Police Counter-UAS Unit. https://www.unmannedairspace.info/latest-news-and-information/multiple-unidentified-drones-reported-over-australian-f-35-base/