



THE ASIA GROUP

COUNTER-UNCREWED AERIAL SYSTEMS (C-UAS) AND THE PROTECTION OF CRITICAL INFRASTRUCTURE

Global Strategies and Best Practices:
Implications for Australian Policy

OCTOBER 2025

A SPECIAL REPORT BY THE ASIA GROUP

Acknowledgements

The Asia Group thanks the individuals who contributed to the research and supported this report's publication.

This report draws on the foundational research of Dr Oleksandra Molloy, a recognised authority on uncrewed aerial systems. Valuable peer review and insights were provided by Mick Ryan, AM, WGCDR Keirin Joyce, CSC, and Mark Ogden. Colleagues from The Asia Group's Defense and Australia practices also provided significant input throughout the drafting process.

The Asia Group thanks DroneShield for providing support to this project.



DRONESHIELD

About this Report

The Asia Group developed this independent special report to provide strategic insight into a rapidly evolving area of national security policy. Focused on the growing challenges faced by critical infrastructure from unauthorised drones, and the importance of counter-drone systems, it aims to equip Australian decision-makers with practical recommendations grounded in international best practice and expert analysis. The report reflects The Asia Group's commitment to advancing informed, forward-looking approaches to complex policy challenges in the Indo-Pacific.

About The Asia Group

The Asia Group is a leading strategic advisory firm dedicated to helping businesses navigate the intersection of public policy, geopolitics, and commercial strategy across the Indo-Pacific. Drawing on deep expertise in regional political and regulatory environments, the firm provides tailored analysis and guidance on market access, investment risk, government engagement, and evolving strategic trends.

The Asia Group launched its Australia Practice in 2023 to deepen engagement with one of the Indo-Pacific's most dynamic markets. The practice opened regional offices in Canberra, Melbourne, and Sydney in January 2025 to support a growing demand for strategic advice.

The Australia in-country team, currently led by Greg Chaffin, provides on-the-ground support to clients navigating complex regulatory environments, fostering public-private collaboration, and advancing commercial objectives in sectors such as defence, critical minerals, clean energy, and emerging technology.

Table of Contents

Executive Summary	3
Interim Recommendations for C-UAS Capability Deployment.....	4
Longer-Term Recommendations for C-UAS Capability Deployment.....	4
Introduction	5
The Dual-Use Challenge of Uncrewed Aerial Systems.....	5
Technologies for Countering UAS Systems	7
Australia's C-UAS Policy Landscape	8
Regulatory Measures	9
Enforcement Mechanisms	10
Coordinated Drone Detection Initiative	10
Drone Rule Digitalisation Initiative	10
Other Drone Detection Initiatives.....	10
Technology Development.....	11
Aviation White Paper 2050	11
What Needs to be Achieved.....	11
Comparative Analysis of International UAS/C-UAS Policies	13
Case Studies.....	15
Case study 1: The United Kingdom	15
Case study 2: The European Union.....	18
Case study 3: The United States	21
Recommended Best Practices to Inform Australian C-UAS Policymakers	24
Interim Recommendations for C-UAS Capability Deployment.....	25
Establish a National C-UAS Strategy and Framework.....	26
Strengthen Governance and Legal Authority	26
Implement Site-Specific Risk Management and Incident Response	26
Enhance Intelligence and Threat Monitoring.....	27
Endnotes	28

Executive Summary

This report assesses Australia's policy framework for the application of Counter-Uncrewed Aerial Systems (C-UAS) technologies in the non-military sphere and benchmarks it against international best practices, including those of the United States (U.S.), the United Kingdom (UK), and the European Union (EU).

Much has been written on the fast-paced and iterative use of drone technology in civilian life and on the battlefield, but not enough deliberation has been given to the use of C-UAS systems for essential defensive missions, including the protection of critical infrastructure. This gap is manifesting as a national security risk. This report highlights best practices and policies which could enable greater effective and proportionate use of C-UAS technologies in Australia.

C-UAS technologies detect, track, identify, and, where legally permitted, intercept or neutralise drones. Drones offer significant benefits when used responsibly, and effective C-UAS policies must avoid unnecessarily restricting these advantages. At the same time, policy and frameworks for the use of C-UAS technologies must address complex challenges related to safety, security, legality, privacy, coordination, planning, and airspace integration.

“Governments cannot solely rely on the timelines for conventional consultation, legislation, and implementation processes to manage this threat.”

Policymakers, regulators, and law enforcement agencies must carefully balance a range of complex considerations as they develop and implement C-UAS policies and frameworks, ensuring that regulatory strategies keep pace with the evolving threat environment while preserving the benefits of drone innovation. They need to weigh both the risks and opportunities that these technologies present in their strategic decision-making.

This report finds that while Australia has made progress in select C-UAS initiatives and selective exemptions for law enforcement, policy, legal, and jurisdictional barriers remain. Australia lacks a unified national C-UAS framework which undermines its ability to respond effectively and proportionately to UAS threats. This report offers actionable recommendations to guide legislative reform, strengthen critical infrastructure protection, and ensure Australia can respond to emerging UAS threats.

Given the pace of innovation in the drone and counter-drone technology ecosystem outstrips traditional policy cycles, governments cannot rely on the timelines for conventional consultation, legislation, and implementation processes to manage this threat. While this report outlines a long-term path toward a coordinated national framework, it also recognises the need for interim responses for C-UAS capability deployment – guided by risk and operational urgency – while longer-term reforms are being developed.

Interim Recommendations for C-UAS Capability Deployment

- **Establish risk-based authorisations** allowing site operators at designated high-risk locations to deploy fixed-site non-kinetic C-UAS effectors, having processes to allow operation of the effectors to defeat drones if certain conditions are met.
- **Mandate strict oversight and reporting** for interim deployments to inform broader legislative development.
- **Develop legal and operational templates** for rapid authorisation (e.g. event-based risk approvals and command and control structures, potentially including for remote operations) that could serve as the basis for future legislation.
- **Develop a clear Commonwealth legislative head of power** to enable lawful drone detection activities by critical infrastructure operators for the purpose of safeguarding sensitive sites from malicious drones.
- **Enable public-private coordination pilots** at selected critical infrastructure sites to test collaborative counter-drone operations under government supervision.
- **Deploy low-cost drone detection sensors** at a representative sample of critical infrastructure sites to rapidly assess the scope of the drone threat and inform future risk-based authorisations, oversight frameworks, and legislative development.

Longer-Term Recommendations for C-UAS Capability Deployment

- **Adopt a coordinated, whole-of-government strategy and framework** informed by lessons learnt from the U.S., the UK, and the EU. This includes clearly defining legal authorities, improving interagency coordination, developing risk-based deployment strategies, and supporting the use of sovereign C-UAS capabilities.
- **Strengthen governance and legal authority** by legislating clear authorities for drone mitigation, conducting a mapping study to identify legal gaps and regulate across federal and state levels, developing technology-agnostic national regulatory guidelines, and promoting coordinated governance across all levels of government.
- **Implement site-specific risk management and incident response** through mandating vulnerability assessments for critical infrastructure sites, developing and testing C-UAS plans for high-risk sites, categorising critical sites into risk tiers, standardising national incident reporting protocols, establishing post-incident coordination guidelines, and extending C-UAS training by law enforcement operators to private security operators to ensure frontline readiness.

- **Enhance intelligence and threat monitoring** by ensuring the national incident register tracks, logs, and analyses UAS misuse, continuously assessing vulnerabilities and system capabilities to address emerging threats, and participating in international working groups on drone threat intelligence and information sharing.

Introduction

The Dual-Use Challenge of Uncrewed Aerial Systems

Uncrewed Aerial Systems (UAS), or drones, are an evolving technology that play a beneficial role in industries including agriculture, logistics, security, and emergency response. They enhance safety, reduce costs, and improve response efforts. Across Australia, drones fight bushfires, respond to natural disasters, inspect infrastructure, deliver aid to remote areas, and transport essential goods like food and medicine.

While drones offer benefits, their misuse by criminal, state, and non-state actors presents serious security risks.¹ Recent Ukraine and Israeli operations have demonstrated how small, inexpensive drones can be deployed at scale to infiltrate targeted territory and deliver coordinated, high-impact effects – despite prior assumptions about the required logistical and operational complexity.

“As UAS technology continues to advance with longer flight times, greater ranges, and increased payload capacities, the threat to critical infrastructure grows. When combined with malicious intent, these capabilities pose risk to federal and state facilities and assets.”

The war in Ukraine has drawn attention to military application, which remains the primary use globally, but governments and critical infrastructure operators must also respond to domestic UAS security challenges. This report is focused on this civilian context, where risks to infrastructure and public safety are growing alongside increased drone accessibility and capability. As UAS technology

continues to advance with longer flight times, greater ranges, and increased payload capacities, the threat to critical infrastructure grows. When combined with malicious intent, these capabilities pose risk to federal and state facilities and assets.

Globally, there have been numerous reports of drones being used for unauthorised surveillance, interference with critical infrastructure, and even targeted attacks, underscoring the urgency for global and localised countermeasures.² National infrastructure has become a primary target for malicious actors including activist groups, industrial disruptions, and terrorist threats. The most vulnerable assets include communication towers, broadcast transmitter sites, fiber networks, data centres, power plants, water and natural gas facilities, transportation systems, manufacturing sites, and government installations.








Drone Threats to Critical Infrastructure Assets – Illustrative		
Asset Type		Key Problems Caused by Drones
Communication Towers, Broadcast Transmitter Sites & Fiber Networks		<ul style="list-style-type: none"> • Signal jamming or disruption • Physical damage • Intelligence gathering/surveillance to identify weak points for future attacks • Hacking or intrusion
Data Centres		<ul style="list-style-type: none"> • Physical damage • Intelligence gathering/surveillance • Interference with communications
Power Plants & Power Grid		<ul style="list-style-type: none"> • Physical damage causing wide-scale outages • Intelligence gathering/surveillance • Environmental hazards from physical damage
Water & Natural Gas Facilities		<ul style="list-style-type: none"> • Physical damage – water contamination • Damage to infrastructure and facilities • Environmental hazards from physical damage
Transportation Systems		<ul style="list-style-type: none"> • Disruption of traffic (air/ground) • Intelligence gathering/surveillance • Physical damage • Cyber intrusions
Manufacturing Sites		<ul style="list-style-type: none"> • Espionage • Intelligence gathering/surveillance • Physical damage and disruption – attacks on supply chain, damage to production lines • Cyber intrusions
Government Installations		<ul style="list-style-type: none"> • Espionage • Intelligence gathering/surveillance • Data collection and privacy invasion • Physical damage

Table 1. Drone threats to critical infrastructure assets – illustrative

To address these challenges, the International Organization for Standardization (ISO) is taking steps toward harmonising best practices and technical standards for drone detection, localisation, and identification. For example, the ISO is developing ISO/AWI 25461, which is intended to specify functional requirements for detection, localization, and identification systems.³ This ongoing effort aims to ensure consistency and interoperability across international jurisdictions.

Australia, Canada, New Zealand, the UK, and the U.S., collectively known as the ‘Critical 5,’ have established an international forum to collaborate on critical infrastructure protection. This forum facilitates the exchange of information, best practices, and policy approaches to meet both current and emerging threats.⁴ Beyond these actors, the EU

arguably represents global best practice in C-UAS policy. This report includes the EU in its analysis for that reason, and to offer a broader perspective on global C-UAS strategies.

While countries such as Ukraine, Israel, and Taiwan have developed advanced C-UAS capabilities, their frameworks are largely focused on active conflict zones and battlefield environments. These settings are less applicable to Australia's domestic, civilian infrastructure context and were therefore not included in this analysis.

Technologies for Countering UAS Systems

Counter-UAS, or Counter-Unmanned Aircraft Systems, refers to technologies and methods used to detect, identify, monitor, and potentially mitigate threats posed by UAS, commonly known as drones. Driven by the growing accessibility and misuse of drones, the development of C-UAS technologies has accelerated over the past decade, resulting in a range of commercial and military-grade solutions. The technologies can be categorised into detector and effector systems. The former allows the operator to detect, track and identify drones, while the latter acts to disrupt, disable or destroy the drone. Table 2 provides examples.

Detectors	Effectors
<ul style="list-style-type: none">• Radio Frequency (RF) detectors• Microwave radars• Passive (non-emitting) radars• Optical scanning (cameras)• Radio monitoring• Electro-optical sensors• Acoustic sensors• AI-enabled C2 (sensor fusion, “single pane of glass”)	<ul style="list-style-type: none">• RF jammers• Hunter/ killer drones (with net launchers)• Ground-based net launchers• GPS jammers• Directed energy (including laser) systems• Kinetics (e.g. shotguns, cannon)• Hacking (taking control of the drone)• Electromagnetic pulse• AI-enabled C2 (multi-effector tasking when faced with complex, high-velocity threats)

Table 2. C-UAS technologies

Individual C-UAS technologies cannot address every malicious or inadvertent drone threat. Each system has limitations, making it important to calibrate deployment of C-UAS technologies relative to the drone threat. A risk-based approach of selecting and deploying counter-drone technologies based on the nature of the threat and the operational environment is required. This approach ensures that response measures are effective and proportionate.

Effective C-UAS systems provide a layered defence, integrating both detection and interdiction capabilities depending on the size and capability of the target drone. Two or more capabilities can be installed and/or deployed at a site to provide multiple defeat options based on the assessment of the threat. For example, combining capabilities such as multi-modal and fused sensor capabilities to enhance detection and tracking together

with disrupt and defeat technologies including RF-jamming and high-power microwave capabilities can enable a system to address a range of threats and minimize risk to people and property.



Image 1. Examples of layered C-UAS systems. (Images: DroneShield)

International standards for categorising counter-drone systems support national regulatory efforts by defining clear operational requirements and legal constraints. This standardisation helps authorities establish baseline performance metrics and develop targeted training programs for law enforcement, the Australian Government Department of Defence (Defence) and other authorities' personnel, and ensure effective UAS threat management. It also facilitates collaboration across international security agencies and industry stakeholders, aligning efforts to address the evolving drone threat.

Australia's C-UAS Policy Landscape

In the Australian context, the primary C-UAS threats include unauthorised drone activity near airports, prisons, mass gatherings, and critical infrastructure—such as energy generation and transmission assets, telecommunications facilities, and defence establishments.

To address the risks posed by unlawful drone use, the Australian federal government has taken initial steps to enable limited counter-drone operations and clarify the legal basis

for some enforcement activities. Regulatory authorities are fragmented across multiple laws, agencies, and levels of government, with no overarching strategy or framework. Drawing on lessons from international peers outlined in the forward sections, Australia has an opportunity to build a more coordinated, risk-based policy architecture that enables effective operational use of C-UAS technologies.

Regulatory Measures

Australia has not yet established a dedicated regulatory framework for C-UAS operations. The current patchwork of responsibilities and legal restrictions suggests a need for legislative reform to clarify permissible use cases and to ensure coordinated enforcement across agencies.

There are a number of regulations and exemptions currently in effect:

- In March 2023, the Australian Communications and Media Authority (ACMA) imposed the *Radiocommunications (Jamming Equipment) Permanent Ban 2023*⁵ under subsection 172(1) and section 174 of the **Radiocommunications Act 1992**,⁶ permanently restricting the use of certain jamming technologies.
- ACMA prohibits the possession, operation, supply, or offering of supply of banned equipment – including Global Positioning System (and other position, navigation and timing systems) and drone jammers – in Australia.⁷
- ACMA previously issued the *Radiocommunications (Exemption – Remotely Piloted Aircraft Disruption) Determination 2022*⁸ which grants Australian police the authority to use counter-drone equipment for public safety and security purposes. This exemption overrides certain restrictions in the *Radiocommunications Act 1992*.
- Exemptions under the *Radiocommunications Act 1992* provide certain industry actors limited access to banned equipment for research and development, and manufacturing.⁹
- Further exemptions under the *Radiocommunications Act 1992* apply to the Australian Department of Defence and its suppliers. Section 26 of the Act exempts Defence personnel and officials from certain provisions when carrying out functions related to military command, intelligence, and weapons systems. In addition, the *Radiocommunications (Exemption) Determination 2024* permits the supply and use of banned equipment by authorised Defence suppliers, subject to conditions such as record-keeping and operational restrictions.¹⁰

Enforcement Mechanisms

The Civil Aviation Safety Authority (CASA) enforces regulations governing civilian drone operations, but it does not regulate or authorise the use of C-UAS technologies. Under Section 4 of the **Civil Aviation Act 1988**,¹¹ state aircraft—including those operated by the military and police – are exempt from CASA oversight. State, territory, and local governments maintain their own supplementary regulations, including additional laws and penalties for improper drone use.

Responsibility for deploying C-UAS technologies is fragmented. The Australian Federal Police (AFP) and state police forces are currently the primary entities deploying C-UAS technologies in response to UAS threats, particularly at major public events. ACMA regulates the use of radiofrequency-based countermeasures as referenced above.

Under the **Defence Act 1903**,¹² the Australian Defence Force (ADF) must be authorised through a federal call-out order and cooperate with state governments to act against drones within Australia. Such actions must be supervised by a law enforcement officer authorised by CASA or Airservices Australia. Additionally, the federal **Aviation Act** prohibits interfering with any aircraft in flight unless it poses a direct threat to life, limiting the ADF's domestic counter-drone capabilities.¹³

Coordinated Drone Detection Initiative

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) is leading the Coordinated Drone Detection initiative to address security risks associated with drones. This program supports data sharing among stakeholders, integrates drone management systems, and prepares for a future Uncrewed Traffic Management (UTM) system, which is designed to provide a platform for safe air traffic management of commercial drones and other uncrewed aircraft. Specific evaluations of its effectiveness have not been publicly released.

Drone Rule Digitalisation Initiative

DITRDCA is also working on the Drone Rule Digitisation initiative, which focuses on managing non-safety-related security risks associated with drones. This includes developing rules for drone operations around sensitive sites, such as correctional facilities, and establishing permanent and temporary restrictions to protect critical assets, events, and activities from drone threats. The project led to the release of the Local Drones Rules Map in February 2024, showing local restrictions in place for flying drones.

Other Drone Detection Initiatives

The Australian federal and state police forces and the Department of Home Affairs are exploring nationwide drone threat detection networks to be deployed at high-profile events. The networks support the Detect, Tract, and Identify (DTI) approach to counter-

drone operations in Australia, lessons from which can contribute to a national framework for drone threat management.

Airservices Australia, Defence, and CASA have deployed drone detection systems at 29 major airports as part of a trial in 2019.¹⁴ However, broader deployment or the use of counter-drone defeat measures remains restricted to operation by the AFP and state law enforcement agencies.

Technology Development

While Australia has taken steps toward enabling operational counter-drone deployments, there is currently a lack of regulatory support for sovereign C-UAS technology in Australia. Nor is there a central body responsible for coordinating innovation or developing sovereign capabilities. Unlike peer countries, Australia lacks a public-private pipeline to trial promising technologies, set performance benchmarks, or fast-track procurement through field exercises or innovation sprints.

Aviation White Paper 2050

In 2024, the Australian Government issued the *Aviation White Paper Toward 2050*, outlining 56 policy initiatives across 10 key areas. Initiative 42 aims to reform the administration and management of Australia's airspace by 2030. This will involve a four-stage process:

- Initial consultation and stakeholder engagement.
- Development of a new Australian Airspace Policy Statement to replace the 2021 policy.
- CASA preparation of a new framework for Australian airspace in 2026, detailing how airspace classes will be implemented and managed.
- Update of relevant airspace legislation by 2030 to support safe government operations.

The Aviation White Paper commits to new legislation which will be introduced by 2030 to protect Australian communities, infrastructure, and businesses from the security risks posed by drones and Advanced Air Mobility (AAM) systems.

What Needs to be Achieved

There is a clear need for Australia to develop and enforce comprehensive processes and strategies for enabling critical infrastructure to respond to nefarious UAS. Government stakeholders and ACMA have collaborated to facilitate the interim use of counter-drone capability by law enforcement that would otherwise be prohibited under the under the

*Radiocommunications Act 1992*¹⁵, *the Civil Aviation Act 1998*¹⁶, and relevant state surveillance legislation. There is a need for robust immediate and long-term approaches to manage the risks associated with drones and counter-drone devices across the full spectrum of critical infrastructure.

DITRDCA is currently drafting policies, processes, and regulations which aim to enhance access to C-UAS technologies. These efforts focus on improving coordination between agencies and governments, aiming to ensure that users have access to drone activity data for effective security risk management, and to assist targeted use of interdiction capabilities when they need to be deployed.¹⁷

“The Aviation White Paper sets a process and a timeline for taking forward important initiatives related to the evolving UAS threat, but the deteriorating threat environment and continued iterative and creative use of relatively unsophisticated drones for maximum effect calls for more immediate action, including close collaboration with industry.”

The Aviation White Paper sets a process and a timeline for taking forward important initiatives related to the evolving UAS threat, but the deteriorating threat environment and continued iterative and creative use of relatively unsophisticated drones for maximum effect calls for more immediate action, including close collaboration with industry.

With the legal use of technologies for the detection of drones currently falling under state jurisdictions, there is ambiguity around what private operators may legally implement. In some states, legislation relating to the tracking and surveillance of airborne vehicles was not designed with modern drone threats in mind. As a result there exists a regulatory grey zone where private critical infrastructure operators may be unsure about the use of drone detection equipment, while balancing the need to protect sensitive infrastructure from potential drone incursions.

There is opportunity for the Australian Government to be a global leader on advancing the use of C-UAS, in part by allowing critical infrastructure operators to take control of their security to advance national security outcomes. The government is already on the forefront of drone technology usage for non-military and non-law enforcement purposes. In 2018, Australia authorised Wing Aviation, a subsidiary of Alphabet Inc. (Google’s parent company) to run a trial using drones to operate commercial deliveries.¹⁸ Australia was one of the first and remains the leading market for this service. Following successful trials, the delivery service was expanded to multiple locations across the country and provides coverage for hundreds of thousands of residents.

Comparative Analysis of International UAS/C-UAS Policies

Table 1. Comparative analysis of drone/counter drone policy approaches

Country	Australia	UK	US	EU
Drone policies	<p>National Emerging Aviation Technologies Policy Statement (2021; National Emerging Aviation Technologies)</p> <p>Emerging Aviation Technologies: National Aviation Policy Issues Paper (2020; Emerging Aviation Technologies)</p> <p>Security policy (DITRDA)</p>	<p>Cap 722 provides policy and guidance on operation of the UAS within the UK (2024; Unmanned Aircraft System Operations in UK Airspace – Guidance)</p> <p>Defence Drone Strategy (2024; The UK's Approach to Defence Uncrewed Systems)</p>	<p>14 CFR Part 107 (Federal Aviation Regulations) regulatory framework for small unmanned aircraft systems (Part 107 – Small Unmanned Aircraft Systems)</p> <p>Exception for Limited Recreational Operations of Unmanned Aircraft (Federal Aviation Administration) (2019; Notice in the Federal Register)</p>	<p>Drone Regulations. Flying and operating drones in Belgium are subject to EU Regulation 2019/947.</p> <p>The EU has issued 'Drone Strategy 2.0' (2022; A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe)</p>
Counter-drone policies	<p>Spectrum regulation (Radiocommunications Act 1992; ACMA). Exemptions under the Radiocommunication Act.</p> <p>[Detection of drones falls under individual state laws]</p>	<p>Policy Paper: UK Counter-Unmanned Aircraft Strategy (2019; UK Counter-Unmanned Aircraft Strategy – GOV.UK)</p> <p>Countering Threats from Uncrewed Aerial Systems (2023; Making your site ready by the National Protective Security Authority)</p> <p>The National Counter Terrorism Security Office's Countering threats from UAS (2022; Countering threats from Uncrewed Aerial Systems (C-UAS) ProtectUK)</p>	<p>Interagency Security Committee best practice paper (2020; Protecting Against the Threat of Unmanned Aircraft Systems: An Interagency Security Committee Best Practice– 2020 Edition).</p> <p>The DoD National Counter-Drone Strategy (2024; DoD Announces Strategy for Countering Unmanned Systems)</p> <p>The FAA Updated Information on UAS Detection and Countermeasures Technology at Airports (2019; UAS Detection, Mitigation, and Response on</p>	<p>The EU Commission Counter-drone policy (2023; Critical Infrastructure Protection & Resilience)</p>

		<p>ADS Group Policy Paper (2019; <u>Counter-Drone Technologies</u>)</p>	<p><u>Airports Federal Aviation Administration</u>).</p> <p>Legal authorities for the Departments of Justice and Homeland Security (https://www.dhs.gov/sites/default/files/publications/dhs_cuas-legal-authorities_fact-sheet_190506-508.pdf)</p> <p>Legal guidance on the use of UAS Detection and Mitigation Technologies in the US (<u>2020: Interagency Legal Advisory</u>)</p> <p>Rulemaking guidance (Federal Aviation Administration) (<u>2024: UAS Detection and Mitigation Rulemaking Committee Final Report</u>)</p>	
--	--	---	---	--

Case Studies

The following case studies highlight how countries have developed strategies, plans, and policies to protect their national infrastructure from potential UAS threats. The analysis highlights best practices for policy frameworks that enable effective and safe use of counter-drone technologies. The case studies examine the experiences of the UK, the EU, and the U.S., and extract insights useful for Australia's requirements.

Case study 1: The United Kingdom

In December 2018, suspected drone sightings at Gatwick Airport caused significant travel disruptions in the UK, costing the aviation industry an estimated AUD 91 million.¹⁹ A similar incident occurred at Heathrow Airport on January 8, 2019, leading to temporary flight groundings.



Image 2. Joel Papalini / EyeEm via Getty Images

These events underscored the vulnerability of critical infrastructure to relatively unsophisticated drone disruptions or attacks. A major contributing factor to the events was the lack of drone detection technologies to help operators detect, identify, and assess the drone threat. While the UK imposes restrictions on C-UAS usage, the need to better protect airports and other critical sites from improper drone use is widely recognised.

UK LEGISLATION

Under the **Air Navigation Order 2016**,²⁰ it is illegal in the UK to interfere with a flying aircraft, including drones. Additionally, the **Wireless Telegraphy Act**²¹ prohibits the jamming of commercial RF bands and GPS without a license. Legal restrictions also apply to interception systems that may be considered wiretapping. Currently, only the police, military, and intelligence agencies have legal authority to use jamming technology, typically in direct life-threatening situations.

As a result, while many counter-drone technologies can effectively mitigate civilian drone risks, their use in the UK remains restricted to government agencies, with specific, legally authorised circumstances.

UK RESPONSIBLE AGENCIES

The UK government assigns primary responsibility for UAS and C-UAS strategy and policy to two key departments, supported by a range of partner organisations:

- The Department for Transport – responsible for the safe and lawful use of drones within UK airspace.
- The Home Office – responsible for domestic counter-drone activities as part of its broader security mandate.

UK C-UAS STRATEGIES AND POLICY FRAMEWORKS

The UK *Counter-Unmanned Aircraft Strategy (2019)*²² outlines a unified vision for government and industry that ensures coherent, efficient, and cost-effective responses to drone-related security challenges. This strategy aims to keep the UK attractive for companies investing in drone technology while reducing the risks of illegal drone use. The strategy focuses on:

- Understanding the evolving risks posed by malicious and illegal drone use (see Figure 1).
- Adopting a "full spectrum" approach to deter, detect, and disrupt drone misuse.
- Building strong industry relationships to ensure products meet high-security standards.
- Empowering police and other responders through access to counter-drone capabilities, effective legislation, training, and guidance.

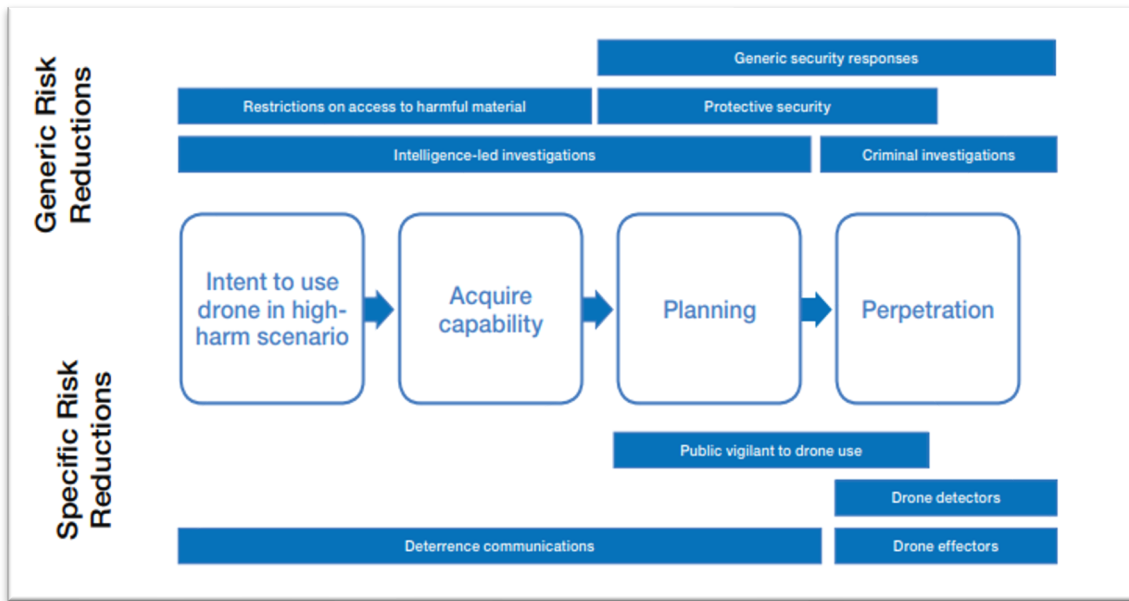


Figure 1. Examples of layered risk-reduction across a timeline of high-harm drone use²³

To support infrastructure operators in addressing drone threats, the UK National Protective Security Authority (NPSA) released *Countering Threats from Uncrewed Aerial Systems: Making your site ready (2023)*, a public document outlining how to develop site-specific C-UAS plans.²⁴ The guidance was intended for security managers and personnel responsible for the protection of national infrastructure, sensitive sites, and crowded places. The seven-step process includes (see Figure 2): conducting vulnerability assessments (VA) to inform C-UAS planning and risk assessment; identifying physical, operational, and technical mitigation measures; and addressing future strategies and policies.

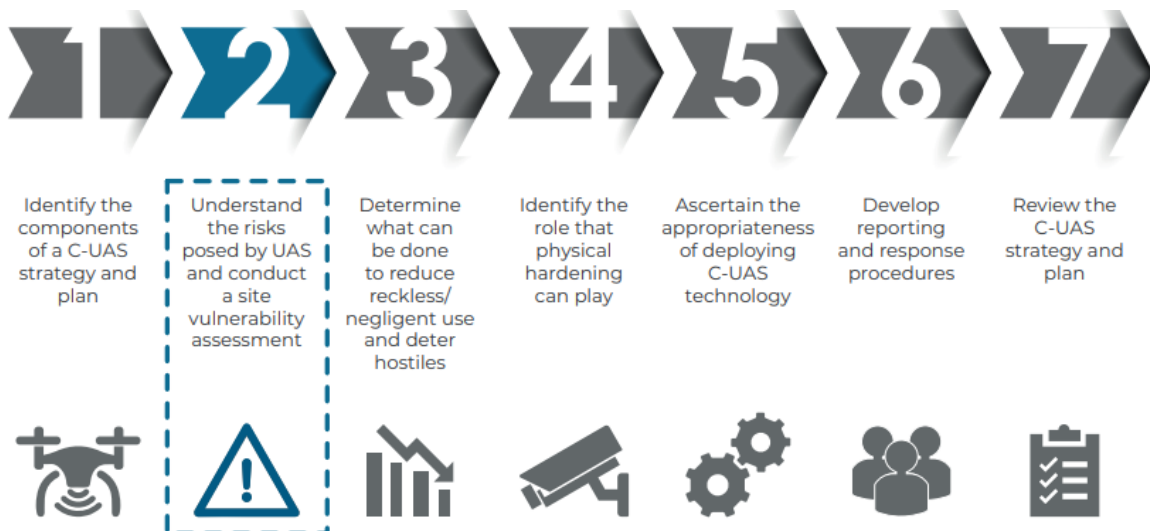


Figure 2. The NPSA seven-step C-UAS framework

The NPSA also issued guidance in 2023 outlining general principles for assessing aerial drone threats and vulnerabilities in the *Countering Threats from Uncrewed Aerial Systems – Assessing the Threat and Vulnerability*.²⁵

The VA process includes identifying key internal and external stakeholders and clearly defining their roles and responsibilities. The senior risk owner may retain overall risk ownership while coordinating with external stakeholders, including local authorities, law enforcement, neighbouring businesses, and other relevant parties.

According to the NPSA, any site assessing UAS risks should develop a comprehensive security framework, including a security strategy, risk assessment, range of mitigations, and C-UAS plans. This framework should integrate C-UAS technologies and strategies to provide a coordinated defence against drone threats.

The C-UAS Strategy provides that private sector employees responsible for safety and security in a variety of locations, including critical infrastructure operators, be designated operational responders who are vital to meeting the objectives of the Strategy.³⁷

BEST PRACTICE INSIGHTS FROM THE UK C-UAS FRAMEWORK

- A structured framework for developing national C-UAS strategies and plans for critical infrastructure protection.
- A national (centrally-driven) C-UAS framework to define processes, roles, and responsibilities for stakeholders across jurisdictions.
- Tailored assessments for each critical infrastructure site to determine the most appropriate C-UAS strategy based on site-specific risk profiles and operational environments.
- Awareness raising among site personnel about UAS threats.
- Crisis and post-incident communication plans in coordination with lead agencies.
- Robust testing and exercising plan to ensure site readiness.
- Regular vulnerabilities and system capabilities review against evolving threats.

Case study 2: The European Union

In recent years, Europe has reported numerous safety and security incidents involving drones, many of which have been linked to criminal, illegal, or terrorist activities. Common examples include smuggling contraband into prisons, crossing national borders with illegal goods, monitoring police operations, launching cyberattacks, invading privacy, and disrupting air traffic.²⁶ Given the wide range of operational scenarios and environments, as well as the complexity of aligning national and multilateral approaches, a one-size-fits-all approach to C-UAS implementation is impractical in the EU context.

Authorities responsible for internal security choose different counter-drone tactics and responses depending on the situation. For instance, when facing an imminent attack on people or critical infrastructure, physically destroying the drone may be the only viable option. In other cases, such as criminal surveillance or hostile intelligence gathering, authorities may prioritise securing control over the drone, often via radio frequency jamming, to land it intact, allowing for forensic investigation. Law enforcement can gather critical physical and digital evidence once the drone is in their possession.

The EU has through its Joint Research Centre Drone Project in Belgium ongoing research focusing on countering the civil threats of drones.²⁷ The site currently operates as a living laboratory for testing and evaluating C-UAS technologies, including detection, tracking, identification, and mitigation systems. The initiative is intended to support coordination among member states by facilitating the development of technical standards and regulatory alignment. The Centre also focuses on the integration of artificial intelligence and machine learning into C-UAS capabilities. In parallel, the EU has established a C-UAS Information Hub with more than 300 members to support information-sharing among operational stakeholders.

EU LEGISLATION

While the EU has established regulations for the legitimate use of drones, it has not yet adopted a unified counter-drone regulatory framework for member state authorities, operators, and manufacturers. Although the European Union Aviation Safety Agency (EASA) has issued guidelines for addressing drone incidents at airports, their advisory nature and limited scope have proven insufficient for managing the complex threat posed by non-cooperative drones.

EU STRATEGIES AND POLICY FRAMEWORKS

In 2023, the EU introduced a counter-drone policy to address the risks posed by illegal, irregular, or malicious drones.²⁸ This policy was part of a broader C-UAS package that included two handbooks providing practical guidance on key technical aspects of counter-drone operations.

The EU developed this counter-drone policy through six key activities:

- Community-building and information sharing.
- Testing counter-drone systems to identify and validate effective solutions.
- Providing practical guidance and operational support.
- Supporting research and innovation.
- Offering funding support.
- Exploring potential regulatory measures.

The EU Commission in 2023 recommended a five-step C-UAS development approach for securing critical infrastructure and public space against drone threats, and provided evidence-based scientific support to the EU policy-making process.²⁹

The five-step process entails:

- Getting started: Setting the principles, goals and requirements for the counter-UAS solution (identifying roles and responsibilities of the key stakeholders).
- Risk analysis: Investigating, analysing and documenting the site's UAS-driven threats and establishing a response plan.
- Solution design: Matching business needs with potential solution architectures.
- Solution implementation: Installation and testing considerations of the solution.
- Solution operation: Operating, maintaining and updating the solution.

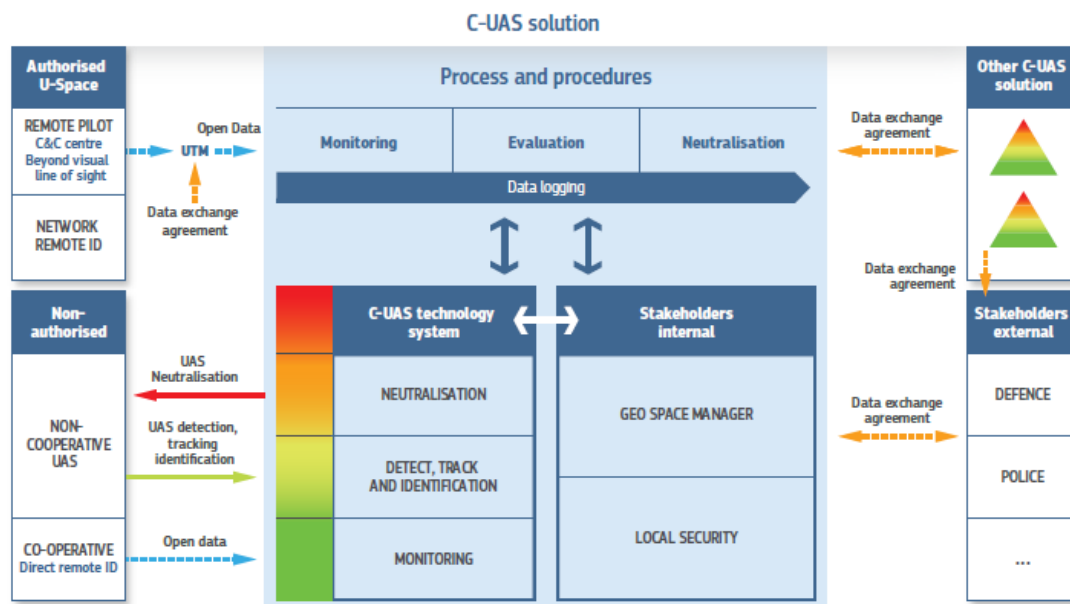


Figure 3. Example of an EU C-UAS solution architecture.

The report states that no solution can be considered static, and it should evolve with changes to needs, sites, threats and stakeholders. As changes can be temporary or permanent and occur at any time, the solutions must be closely monitored, and each step repeated when needed.

BEST PRACTICE INSIGHTS FROM THE EU C-UAS FRAMEWORK

- C-UAS Joint Research Centre DRONE project, expert groups on counter-drone activities, and investment in research and development, and innovations.

- A flexible, scenario-based approach to counter-drone operations, allowing authorities to adapt their response depending on the threat environment.
- Use of advanced cyber tools to take control of hostile drones, enabling law enforcement to secure digital and physical evidence for investigative purposes.
- A structured five-step framework for developing, implementing, and maintaining C-UAS solutions at the site level, including stakeholder coordination, risk assessment, solution design, and regular updates.
- Development of technical handbooks to provide evidence-based guidance for policymakers and operators involved in C-UAS planning and implementation.
- A comprehensive and layered policy approach that integrates technical system testing, operational guidance, stakeholder coordination, and regulatory development—ensuring that counter-drone measures are supported by sustained innovation, funding, and institutional collaboration.

Case study 3: The United States

U.S. C-UAS LANDSCAPE

In October 2024, multiple suspected and unidentified UAS were detected over some of the U.S.' most significant military sites in Virginia and Nevada, continuing a troubling pattern observed over the previous year.³⁰ Around the same time, Fengyun Shi, a Chinese national and graduate student, pleaded guilty to unauthorised drone photography for flying his UAV over the Newport News Shipbuilding facility in Norfolk, Virginia.³¹

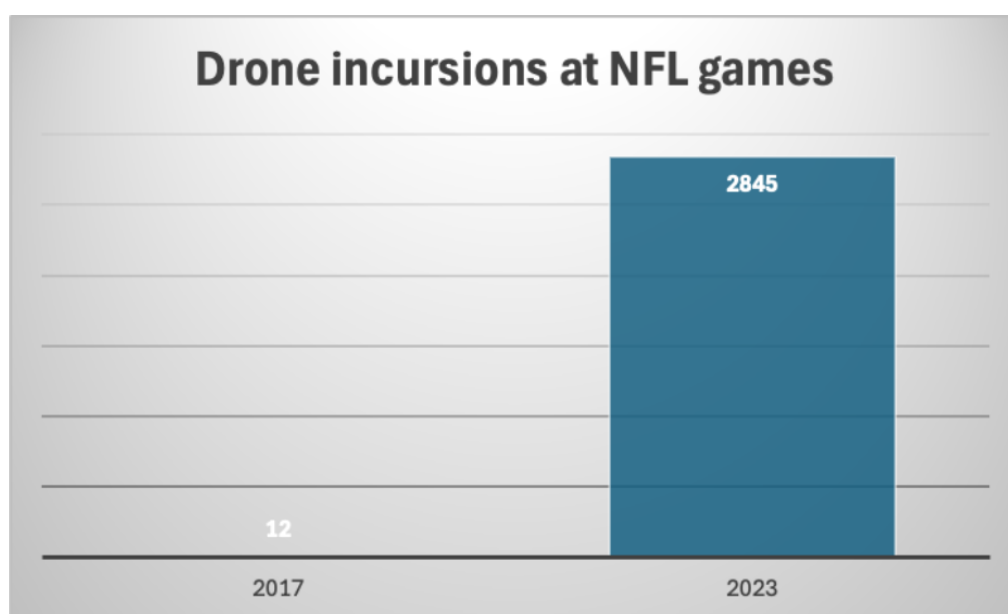


Figure 4. NFL 2017–2023 drone incursion data. (Graph: The Asia Group)

In November 2024, federal agents arrested a Tennessee man for planning to use a drone armed with explosives to attack an electrical substation. During a recent Congressional hearing, the National Football League's (NFL) chief of security reported a 20,000 percent increase in unauthorised drone incursions at NFL games between 2017 and 2023.³²

These and similar incidents, including suspected drone sightings in the Northeastern U.S., have prompted a national reassessment of federal counter-drone laws, with a focus on protecting critical infrastructure and other sensitive sites. Department of Justice (DOJ) and Department of Homeland Security (DHS) authorities, first lapsed in 2022 and extended on a temporary basis, are set to expire again on September 30, 2025. Congress is considering longer-term legislation, while the Trump Administration has sought to strengthen federal counter-UAS authorities through executive orders, including the June 2025 *Restoring American Airspace Sovereignty* order.³³

Currently, counter-drone measures in the U.S. fall into two broad categories: detection and mitigation. Few federal agencies have Congressional authorisation to employ mitigation techniques, while public and all private entities are limited to using detection methods to address potential drone threats.

U.S. LEGISLATION

Effective policy remains the most critical element of C-UAS operations in the U.S. today. Despite the availability of advanced counter-drone technologies, most law enforcement agencies lack the legal authority to act against drone threats, and no standardised process exists for responding to threats.

Although C-UAS technologies exist to detect, track, and mitigate drone threats, legal authority to act remains highly restricted:

- Under current U.S. law, only select federal agencies – Department of Defense (DoD), Department of Energy (DoE), DOJ, and select agencies within DHS – can legally disrupt or intercept drones, and only under specific, narrowly-defined conditions.
- However, in June 2025 amid rising concern over unauthorised drone activity, the U.S. state of Louisiana became the first state to grant its law enforcement agencies direct drone mitigation authority. The law empowers specifically trained officers to deploy kinetic and non-kinetic technologies to neutralise unmanned aerial systems operating unlawfully near high-risk areas and critical infrastructure.³⁴ Although the Governor of Louisiana granted this authority, state law does not supersede federal laws that prohibit the sale and use of these technologies, causing confusion in industry where some companies may be selling technology to Louisiana law enforcement agencies that is illegal under federal law.
- Public safety agencies and private operators, including those at critical infrastructure sites like airports and power plants, lack legal authority to disable threatening drones.

- Federal Communications Commission (FCC) regulations prohibit the use or sale of many C-UAS tools, such as signal jammers, due to their potential to interfere with communication and navigation systems.
- The Federal Aviation Administration (FAA) governs safe drone operations nationwide and can pursue civil penalties for reckless or unauthorised UAS use.
- DoD Authorities: The DoD receives its authority from 10 U.S.C. § 130i, which permits the Department to detect, monitor, and, if necessary, disrupt or disable unmanned aircraft posing a threat to designated defense facilities and assets.³⁵
- In 2020, the FAA, DHS, DoJ, and FCC issued joint guidance to clarify the legal use of detection and mitigation tools by non-federal entities.
- In June 2025, the White House issued an executive order titled "Unleashing American Drone Dominance," which established a federal task force on UAS threats, directed agencies to develop national C-UAS enforcement and airspace protection protocols, and called for the creation of a national counter-UAS training center.³⁶ The order also proposed legislative updates to expand enforcement powers and safeguard critical infrastructure from drone incursions.

Several bills, including the **Safeguarding the Homeland from UAS Threats Act (2023)**³⁷ and the **American Security Drone Act 2023**³⁸ have been introduced in Congress to strengthen drone security. Lawmakers are also weighing C-UAS authorities for state and local entities and reauthorising broader C-UAS measures.

Separately, in June 2023, the U.S. Senate began considering legislation to ban the purchase or use of drones manufactured in countries identified as national security threats, including China, Russia, Iran, North Korea, Venezuela, and Cuba.³⁹

U.S. C-UAS STRATEGIES AND FRAMEWORKS

The U.S. has developed several C-UAS strategies and frameworks to guide counter-drone operations, including:

- Interagency Security Committee (ISC) Best Practice: Published by the DHS and the Cybersecurity and Infrastructure Security Agency (CISA) in 2020, this guidance helps security professionals protect federal facilities against UAS threats. It includes frameworks for vulnerability assessments, protective measures, response planning, and community engagement.⁴⁰
- FAA Best Practices for UAS Detection and Mitigation at Airports: The FAA requires all airports certified under Part 139 to include UAS response plans in their Airport Certification Manuals (ACMs). These plans provide specific guidance for responding to unauthorised UAS activity and coordinating recovery with Air Traffic Control (ATC), airport operations, the Transportation Security Administration (TSA), and law enforcement.⁴¹

BEST PRACTICE INSIGHTS FROM THE U.S. C-UAS FRAMEWORK

- Clear legal authorities for certain agencies to defend against and neutralise UAS threats to military or critical infrastructure.
- Joint interagency guidance to clarify how detection and mitigation tools can be used legally by state and local law enforcement entities.
- Security planning framework to provide federal facility operators with structured processes for threat assessment, protective measures, response planning, and coordination.
- Requirement for certified airports to incorporate UAS response plans into their certification manuals, with protocols for coordination in the event of an incident.
- Consideration of legislative proposals to expand C-UAS authorities to state, local, and infrastructure entities, highlighting ongoing policy development in response to growing threat activity.

Recommended Best Practices to Inform Australian C-UAS Policymakers

Australia has made progress in counter-drone policy through initiatives like the Coordinated Drone Detection Network and selective exemptions for law enforcement to use jamming technologies. However, these efforts remain limited and constrained by policy, legal, and jurisdictional barriers.

When considering our examples of global best practice, Australia lacks a unified national strategy or clear guidance for responding to nefarious UAS at the national, state, and local levels for critical infrastructure operators. Unlike the UK, U.S., and EU, which have developed frameworks with clearly defined roles, threat assessments, and layered mitigation plans, Australia lacks the integrated policy approach needed to respond effectively to the evolving UAS threat landscape. This gap, including the absence of legislative clarity, national performance standards, and a coordinated operational model, undermines Australia's ability to respond effectively and proportionately to UAS threats. Without a clear directive from Government, critical infrastructure operators remain unable to act decisively despite the growing threat.

“Australia should consider developing a coordinated, evidence-based national C-UAS policy. There is also an urgent need for immediate interim measures to mitigate existing security risks.”

To address these challenges, Australia should consider developing a coordinated, evidence-based process that requires a national framework and for critical infrastructure to consider UAS threats and develop plans of action. Drawing on best practices from the

EU, UK, and U.S., it can move towards a comprehensive approach that could strengthen existing C-UAS employment and remain adaptive to evolving technology advances.

While Australia moves toward a nationally coordinated C-UAS framework, there is an urgent need for immediate interim measures to mitigate existing security risks. A short-term, delegated authority model would allow relevant agencies and infrastructure operators to act within clear parameters, support operational testing, and generate the practical insights needed to shape longer-term reforms.

Interim Recommendations for C-UAS Capability Deployment

- Establish risk-based authorisations allowing site operators at designated high-risk locations to deploy fixed-site non-kinetic C-UAS effectors, including RF drone disruptors, that may be operated under strict governance and reporting frameworks, especially where immediate threats to life or critical infrastructure are present.
- Mandate strict oversight and reporting for interim deployments, including central logging of incidents, performance metrics, and risk assessments to inform broader legislative development.
- Develop legal and operational templates for rapid authorisation (e.g. event-based risk approvals) that could serve as the basis for future legislation.
- Provide a clear Commonwealth legislative head of power to enable lawful drone detection activities by critical infrastructure operators, for the purposes of the protection of sensitive sites from nefarious drones.
- Enable public-private coordination pilots at selected critical infrastructure sites to test collaborative counter-drone operations under government supervision.
- Deploy low-cost drone detection sensors at a representative sample of critical infrastructure sites to rapidly assess the scope of the drone threat and inform future risk-based authorisations, oversight frameworks, and legislative development.

Long-Term Recommendations for C-UAS Capability Deployment

Establish a National C-UAS Strategy and Framework

- Develop a national C-UAS strategy that clearly defines processes, roles, responsibilities, and legal authorities for all stakeholders, ensuring alignment across federal, state, and local levels.
- Establish a centralised, whole-of-government approach similar to the UK's seven-step framework and the U.S. Interagency Security Committee guidance, integrating detection, mitigation, and critical infrastructure protection.
- Apply EU principles on solution architecture, mitigation tiers, and UAS category adaptation to enhance resilience against a wide range of drone threats.
- Create a National Coordination Body, such as a C-UAS Coordination Centre, to oversee policy implementation, ensure harmonisation across jurisdictions, and coordinate civil-military collaboration.

Strengthen Governance and Legal Authority

- Legislate clear authorities for drone mitigation by reassessing the Radiocommunications Act, Civil Aviation Act, and Defence Act, allowing authorised non-federal actors to engage in lawful drone mitigation, similar to the legal exemptions in the U.S. and UK.
- Conduct a comprehensive mapping study to identify legal gaps and harmonise regulations across federal, state, and local levels.
- Develop technology-agnostic national regulatory guidelines that can adapt to rapid advancements in C-UAS technology.
- Promote coordinated governance across all levels of government to ensure unified and consistent responses to UAS threats.

Implement Site-Specific Risk Management and Incident Response

- Adopt a risk-based, site-specific approach to threat assessment and mitigation, drawing from the UK's NPSA framework.

- Mandate vulnerability assessments for critical infrastructure sites, integrating C-UAS planning into broader security strategies. This should parallel legislation for cyber security incident management and reporting for critical infrastructure.
- Develop and test tailored C-UAS plans for high-risk critical infrastructure sites, supported by regular training exercises and operational drills.
- Categorise critical sites into risk tiers, prescribing scalable C-UAS technology deployments based on threat likelihood and impact.
- Standardise national incident reporting protocols, including priority data fields and thresholds for UAS incidents.
- Establish clear post-incident coordination guidelines, developed in collaboration with lead agencies like the AFP, Home Affairs, and CASA.
- Extend C-UAS training by law enforcement operators to private security operators to ensure frontline readiness.

Enhance Intelligence and Threat Monitoring

- Ensure CASA's national incident register tracks, logs, and analyses UAS misuse, supporting data-driven policy decisions.
- Continuously assess vulnerabilities and system capabilities to address emerging threats, including autonomous drones, swarms, and drone-mounted countermeasures.
- Participate in international working groups on drone threat intelligence and information sharing, including the "Five Eyes" alliance and ICAO working groups.

Endnotes

¹ Dr Oleksandra Molloy, "Drones in Modern Warfare: Lessons Learnt from the War in Ukraine," Australian Army Research Centre (2024).

² Vince Bernard B Austria, "Assessing the Threat: Autonomous Commercial Drones and its Potential for Mass Civilian Casualty Attacks," *IEEE Access: Practical Innovations, Open Solutions* (2024).

³ *Uncrewed aircraft systems – Counter UAS – Functional requirements for detection, localization, and identification*. International Organization for Standards (ISO), 2025.

⁴ Adapting to Evolving Threats: A Summary of Critical 5 Approaches to Critical Infrastructure Security and Resilience, (2024).

⁵ Australian Government. *Radiocommunications Act 1992 – Sect 172 Permanent ban on equipment*. Federal Register of Legislation, 1992.

⁶ Australian Government. *Radiocommunications Act 1992*. Federal Register of Legislation, 1992.

⁷ Australian Communications and Media Authority. *Radiocommunications (Jamming Equipment) Permanent Ban 2023*. Canberra: ACMA, 2023.

⁸ The Australian Communications and Media Authority. "Radiocommunications (Exemption – Remotely Piloted Aircraft Disruption) Determination 2022." Federal Register of Legislation, 2022. <https://www.legislation.gov.au/F2022L01255/asmade/text>.

⁹ Australian Government. *Radiocommunications Act 1992*. Federal Register of Legislation, 1992.

¹⁰ Australian Communications and Media Authority. *Radiocommunications (Exemption) Determination 2024*. F2024L00924. Registered July 26, 2024. Federal Register of Legislation.

¹¹ Australian Government. *Civil Aviation Act*. Federal Register of Legislation, 1988

¹² Australian Government. *Defence Act 1903*. Federal Register of Legislation, 1903.

¹³ Australian Government, *Civil Aviation Act 1988*.

¹⁴ Australian Government Department of Infrastructure, Transport, Regional Development and Communications. *FOI 21-005: Documents Released under Freedom of Information – Drone Detection Systems*. 2020. <https://www.infrastructure.gov.au/sites/default/files/migrated/department/ips/files/log/foi-21-005-documents-redacted.pdf>.

¹⁵ Australian Government, *Radiocommunications Act 1992*.

¹⁶ Australian Government, *Civil Aviation Act 1988*.

¹⁷ Australian Government. Security Policy. Drones.gov.au. <https://www.drones.gov.au/policies-and-programs/policies/security-policy>.

¹⁸ Civil Aviation Safety Authority. *Drone Delivery Services*. 2024. <https://www.casa.gov.au/drones/industry-initiatives/drone-delivery-services>.

-
- ¹⁹ H. Detrick. "Gatwick's December Drone Closure Cost Airlines \$64.5 Million." *Fortune*, 2019.
- ²⁰ UK Civil Aviation Authority, "Air Navigation Order " (2016). <https://www.caa.co.uk/general-aviation/the-ga-unit/air-navigation-order-2016/>.
- ²¹ UK Parliament. *Wireless Telegraphy Act*. London, 2006.
- ²² UK Government. *UK Counter-Unmanned Aircraft Strategy*. APS Group on behalf of the Controller of Her Majesty's Stationery Office, 2019.
- ²³ UK Government, *UK Counter-Unmanned Aircraft Strategy*.
- ²⁴ National Protective Security Authority. *Countering Threats from Uncrewed Aerial Systems: Making Your Site Ready*. 2023. <https://www.npsa.gov.uk/system/files/documents/cuas-making-your-site-ready.pdf>.
- ²⁵ National Protective Security Authority. *Countering Threats from Uncrewed Aerial Systems: Assessing the Threat and Vulnerability*. 2023. <https://www.npsa.gov.uk/system/files/documents/npsa-uas-vulnerability-assessment-official.pdf>.
- ²⁶ European Commission Joint Research Centre. *Countering the Threat of Civil Drones: Commission Presents New Measures*. October 19, 2023. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/countering-threat-civil-drones-commission-presents-new-measures-2023-10-19_en.
- ²⁷ European Commission Joint Research Centre. "Drones, Counter Drones and Autonomous Systems." Last modified October 19, 2023. https://joint-research-centre.ec.europa.eu/projects-and-activities/drones-counter-drones-and-autonomous-systems_en.
- ²⁸ European Commission. *Communication from the Commission to the Council and European Parliament*. 2023.
- ²⁹ Paul Hansen and R. Pinto Faria. *Protection Against Unmanned Aircraft Systems: Handbook on UAS Protection of Critical Infrastructure and Public Space: A Five Phase Approach for C-UAS Stakeholders*. Publications Office of the European Union, 2023.
- ³⁰ Lara Seligman, Gordon Lubold, and Aruna Viswanatha. "Mystery Drones Swarmed a U.S. Military Base for 17 Days. The Pentagon Is Stumped." *Wall Street Journal*, 2024. <https://www.wsj.com/politics/national-security/drones-military-pentagon-defense-331871f4>.
- ³¹ George Allison. "Chinese Student Charged for Drone Shots of U.S. Shipyard." *UK Defence Journal*, 2024. <https://ukdefencejournal.org.uk/chinese-student-charged-for-drone-shots-of-u-s-shipyard/>.
- ³² Lanier, Cathy. Written testimony to the Joint Hearing of the House Homeland Security Subcommittee on Counterterrorism, Law Enforcement, and Intelligence and the Subcommittee on Transportation and Maritime Security, December 10, 2024. <https://www.congress.gov/118/meeting/house/117754/witnesses/HHRG-118-HM05-Wstate-LanierC-20241210.pdf>.
- ³³ The White House. *Restoring American Airspace Sovereignty*, June 6, 2025, <https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/>.

³⁴ Office of the Governor, “Louisiana Becomes First State to Authorize Local Law Enforcement to Neutralize Dangerous Drones.” 2025. <https://gov.louisiana.gov/news/4865>.

³⁵ U.S. Code. Protection of certain facilities and assets from unmanned aircraft. 10 U.S.C. § 130i. 2016, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section130i&num=0&edition=prelim>.

³⁶ The White House, *Unleashing American Drone Dominance*, June 6, 2025, <https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/>.

³⁷ U.S. Congress. *Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2023*. S.1631, 118th Cong., 1st sess. Introduced in Senate May 16, 2023. <https://www.congress.gov/bill/118th-congress/senate-bill/1631>.

³⁸ U.S. Congress. *American Security Drone Act of 2023*. S.473, 118th Cong., 1st sess. Introduced in Senate February 16, 2023. <https://www.congress.gov/bill/118th-congress/senate-bill/473>.

³⁹ U.S. Senate. *Stemming The Operation of Pernicious and Illicit (STOP Illicit) Drones Act*. Introduced June 2023. <https://www.blackburn.senate.gov/2023/10/issues/national-security/blackburn-measure-to-stop-taxpayer-funding-of-illicit-drones-passes-u-s-senate>.

⁴⁰ Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, Interagency Security Committee. *Protecting Against the Threat of Unmanned Aircraft Systems (UAS): Interagency Security Committee Best Practice*. 2020. https://www.cisa.gov/sites/default/files/publications/Protecting%20Against%20the%20Threat%20of%20Unmanned%20Aircraft%20Systems%20November%202020_508c.pdf.

⁴¹ Federal Aviation Administration. Best Practices for the Submission of On-Airport UAS Detection and Mitigation System(s) into OE/AAA. Washington, DC: U.S. Department of Transportation, May 2023. https://www.faa.gov/airports/new_entrants/uas_detection_mitigation_response/best_practices_OEAAA_submissions.