

**LOWY
INSTITUTE**

The ungoverned sky: Drones and the domestic extremist threat

POLICY BRIEF



**JAMES PATERSON
LYDIA KHALIL**

March 2026

LOWY INSTITUTE



The Lowy Institute is an independent, nonpartisan international policy think tank. The Institute provides high-quality research and distinctive perspectives on the issues and trends shaping Australia's role in the world.

Cover image: Facu de Iellis/500px via Getty Images

Lowy Institute Policy Briefs are designed to address a particular, current policy issue and to suggest solutions. They are deliberately prescriptive, specifically addressing two questions: What is the problem? What should be done?

This report is part of the Lowy Institute's Changing Violent Extremism Threat Landscape Project funded by the Australian Federal Police (AFP). Responsibility for the views, information, or advice expressed in this report is that of the authors. The contents of this report do not necessarily reflect the views of the Lowy Institute, the AFP, or the Australian government. The authors wish to acknowledge editorial director Clare Caldwell, Sam Roggeveen and Mihai Sora for their editorial support, and the anonymous peer reviewers for their constructive feedback. The authors would also like to acknowledge Ian Bruce for his design contribution.

Published 23 March 2026

31 Bligh Street
Sydney NSW 2000

lowyinstitute.org
+61 2 8238 9000

Version 2026-03-19.5E17B0B

Contents

| | |
|--|----|
| Key findings | 4 |
| What is the problem? | 5 |
| What should be done? | 5 |
| Extremist non-state actors and drone use | 6 |
| The Ukraine addition | 8 |
| The domestic warning signs | 9 |
| Threat recognition and response | 11 |
| Remaining vulnerabilities | 12 |
| Policy recommendations | 15 |
| Conclusion | 18 |
| Notes | 19 |

Key findings

- Domestic extremist actors are incorporating drone technology into operational capabilities and attack plots, taking inspiration from the battlefield. The number of violent plots utilising drones has increased sharply over the past five years.
- Domestic counter-drone frameworks are mismatched to the threat. Effective protection requires layered, multi-system approaches across potential civilian targets and critical infrastructure.
- Easy-to-access technologies, such as 3D printing, open-source design files, additive hardware, and AI-assisted navigation are lowering the barriers to modifying and weaponising drones.

What is the problem?

In the past two decades, drones have transformed from niche military tools into widely available “commercial off-the-shelf” technologies. What was once the exclusive domain of state actors now rests within reach of nearly anyone with a credit card and a data signal. With uncrewed aircraft systems — or drone platforms — becoming cheaper, smaller, and easier to operate, the number of drone plots by domestic extremist groups has increased rapidly. In the last two years alone, US law enforcement personnel thwarted two extremist plots involving drones, and the Australian Federal Police arrested seven individuals in connection with a plot to use an explosive-laden drone. Remote-controlled drones are a low-cost option for intelligence gathering, surveillance, reconnaissance, transport, and attack preparation. Drones are easily modified and weaponised, enhancing and expanding their capabilities. The combination of easy accessibility and payload potential, and the limitations of domestic counter-drone systems, presents a growing challenge.

What should be done?

This Policy Brief provides three recommendations to address this vulnerability. First, countries should establish domestic counter-drone task forces to tackle domestic actor exploitation of drones. International knowledge-sharing protocols should be developed among national task forces to guide national coordination mechanisms and help coordinate domestic counter-drone responses. Second, internationally coordinated safety-by-design regulations should be implemented to make it easier to identify and respond to malicious drone use. Third, specific policy attention and response should be directed towards the threat posed by 3D printing in the additive manufacturing ecosystem.

Extremist non-state actors and drone use

To understand the evolution of the threat posed by malign actor use of drone technologies in domestic settings, it is important to consider how terrorist and insurgent organisations have used uncrewed aircraft systems (UAS) — or drones — in conflict environments.

The Lebanese paramilitary group Hezbollah, through significant Iranian support, was the first known insurgent group to establish a UAS program. Hezbollah used Iranian-produced drones to conduct surveillance missions over Israeli territory as early as 2004 and later expanded its use of drones to carry explosive payloads against Israeli targets.¹ Palestinian Islamist organisation Hamas also exhibited an early interest in drones. Hamas' program developed at a slower pace, but after eventually receiving Iranian support, and by reverse-engineering failed or shot-down Israeli drones, it too was able to conduct drone incursions into Israeli airspace.²

However, it was Islamic State that pioneered terrorist insurgent drone tactics. Its drone program demonstrated how commercially available technology could be adapted for asymmetric warfare, establishing an operational template that domestic extremists have sought to emulate.³ Islamic State transformed commercial off-the-shelf quadcopters — drones with four rotors for vertical take-off, landing, and stable hovering — into a versatile capability that provided intelligence, surveillance, and reconnaissance (ISR), strike capability, and propaganda material at minimal cost and maximum effectiveness.

Islamic State has used uncrewed aircraft systems across a range of ISR missions.⁴ In one of the earliest demonstrations of this capacity, drones were used to conduct reconnaissance prior to the movement's 2014 takeover of Tabqa Air Base, a major Syrian military facility.⁵ The group also used drones to coordinate battlefield operations by directing mortar and artillery fire and guiding vehicle-borne explosives.⁶

Islamic State weaponised consumer drones by developing release mechanisms for grenades, mortar shells, and improvised explosives. These flying artillery platforms required minimal technical expertise but generated disproportionate tactical impacts.⁷ Drone-captured imagery became a core part of Islamic State's pioneering strategic communications campaign. First-person aerial perspectives of attacks made propaganda videos more cinematic and

compelling, projecting military competence that enhanced recruitment and publicity.⁸

While Islamic State was the first terrorist insurgent organisation to employ large-scale integration of drone technology, many others have since incorporated the capability, experimenting with advanced propulsion, fabrication, and supply-chain diversification.

For example, groups such as the Pakistan-based Islamist terrorist organisation Lashkar-e-Taiba have trialled drone use for human transport.⁹ The Chin National Army in Myanmar has a dedicated UAS unit, modifying commercial off-the-shelf drones to incorporate anti-jamming technology into its arsenal.¹⁰ Hayat Tahrir al-Sham has instituted a similar unit and even established its own drone production facilities, using 3D printing to manufacture components. Its drone program played an important role in bolstering the organisation's advance on, and eventual overthrow of, the Assad regime in December 2024.¹¹

The Houthis, a Yemen-based Islamist military organisation that has received technical and logistical support from Iran, developed a long-range drone program that surpasses Islamic State's arsenal in both range and complexity.¹² Houthi drones have been instrumental in attacks on targets in Saudi Arabia, the United Arab Emirates, and Israel.¹³ The organisation has even attempted to develop hydrogen-powered drones that could enable greater endurance and range than conventional battery configurations.¹⁴

The additive power of drones was most recently highlighted in the attacks on Israel on 7 October 2023, where more than 100 modified commercial drones played a role in Hamas' day-long assault.¹⁵ Hamas targeted Israeli surveillance infrastructure using explosive-laden commercial drones, reducing the situational awareness of the Israel Defence Forces and delaying the Israeli response to the preliminary incursion.¹⁶ Hamas also used drones to carry aerial munitions to target Israeli tanks, armoured vehicles, infantry, first responders, and civilians, not only to maximise physical destruction but also to erode the perception that Israeli defences were invulnerable.¹⁷

The Ukraine addition

The Russia–Ukraine conflict, dubbed the first large-scale “drone war”,¹⁸ has revolutionised the range, speed, scale, and autonomy of drones¹⁹ and has allowed Ukraine to surpass its conventional military capabilities.²⁰

One significant innovation has been the emergence of fibre-optic tethered drones, first deployed by Russia.²¹ This development was driven by the need to circumvent jamming capabilities. Another innovation has been in automation, with autonomous drones now better able to track and strike targets through the incorporation of artificial intelligence (AI).²² Both reflect how technological adaptation and iteration have become key measures of combat strength.²³

Insurgent and terrorist groups have consistently borrowed from and adapted battlefield innovations.²⁴ Aerial hijacking, for instance, a tactic first used by Peruvian revolutionaries in 1931, was later seized upon, refined, and expanded on by numerous non-state actors.²⁵ The Japanese kamikaze pilots of the Second World War represent one of the most organised and systematic uses of suicide tactics in modern warfare. Suicide attacks were later deployed by various other non-state militant groups, ultimately becoming a hallmark of modern terrorism. Extremist instruction material, such as Abu Bakr Naji’s seminal jihadist work *Management of Savagery*, often references military strategies, seeking to repurpose military doctrine into insurgent operations.²⁶

The conflict in Ukraine is no different.²⁷ While the hurdles for the development and deployment of drone capabilities by domestic extremist actors are of course higher, and domestic actors will not be able to replicate battlefield-grade capabilities, the Ukraine war has shown that the significant modification of commercially available drones using off-the-shelf components and open-source software is possible. Innovations such as Operation Spiderweb, a covert attack carried out by Ukrainian forces in which drones concealed in trucks were transported into and launched from deep inside Russian territory causing significant damage to military installations, offer a blueprint for attacks in both conflict and non-conflict environments.²⁸

The domestic warning signs

Although many of the most notable incidents of non-state actor drone use have been on the battlefield, the growing ease with which uncrewed aircraft systems can be accessed by domestic extremist actors outside of conflict zones has corresponded with a rise in their use over the years.²⁹ Members of Aum Shinrikyo, the doomsday cult that carried out the 1995 Tokyo subway sarin nerve agent attack, explored the use of a remotely controlled helicopter in their pursuit of a deployable chemical and biological weapons program.³⁰ In 2011, US citizen and homegrown extremist Rezwan Ferdaus was arrested for plotting in support of al-Qaeda to fly three explosive-laden drones into the Pentagon and US Capitol.³¹ In a 2018 attack linked to defectors from the Venezuelan military, two explosive-laden drones were deployed in a failed assassination attempt on Venezuelan President Nicolás Maduro.³² In 2021, Iraqi insurgents attempted to assassinate then prime minister Mustafa Al-Kadhimi using drones to target his residence with explosives, bypassing on-the-ground security.³³ Brenton Tarrant, the perpetrator of the 2019 Christchurch mosque shootings in New Zealand, used a drone to surveil the targets prior to his attack.³⁴ Since then, domestic extremist interest in drones has only accelerated.

In 2023, a PhD student in the United Kingdom was arrested for using a 3D printer to build “kamikaze” drones for Islamic State.³⁵ In November 2025, a Queensland counter-terrorism operation arrested seven individuals possessing 20 kilograms of explosive material, alongside homemade guns and one drone-mounted improvised explosive device (IED).³⁶ One month earlier, an attempted jihadist plot involving the use of a drone-powered IED against Belgian elected officials was foiled.³⁷ US authorities thwarted two separate plots by domestic extremists that involved the use of drones in 2024. In the first, an Arizona teen was arrested for planning an Islamic State-inspired assault, during which he intended to use an explosive-laden drone to attack the Phoenix Pride parade.³⁸ Another individual was arrested in Tennessee for plotting to destroy an electric power station in Nashville with a homemade drone strapped with explosives.³⁹ A drone was used for reconnaissance in one of the two assassination attempts on Donald Trump during his 2024 presidential campaign.⁴⁰

These incidents follow a 2022 warning from the FBI that it was tracking several domestic plots that sought to “weaponize drones with homemade IEDs”⁴¹ and a previous instance in 2020 involving the targeting of a power station in Pennsylvania by far-right accelerationists using drones.⁴² Extremists with military backgrounds have talked openly online of the advantages of drones, especially “cheap, 3D-printed drones with a [high-explosive] round zip tied to it” and referenced innovations in Ukraine and by drug cartels.⁴³

The vulnerability is also highlighted by several cases that do not have a clear link to an extremist agenda. Between 2015 and 2019, there were at least 57 drone incursions over two dozen US nuclear sites.⁴⁴ In 2018 and 2019, drone incursions shut down major airports in London.⁴⁵ In 2023, Sydney airport reported a significant increase in the level of drone activity in its no-fly zone. The same year, drones repeatedly breached restricted airspace above Langley Air Force Base in the United States.⁴⁶ Some 350 intrusions across 100 different US domestic military installations were reported in 2024, and despite weeks of investigation, authorities were unable to identify the operators.⁴⁷ In Europe, numerous airports had to ground flights in 2025 after repeated drone incursions.⁴⁸

Threat recognition and response

In response to these incursions, many jurisdictions and authorities are working to harden national critical infrastructure and develop domestic counter-drone strategies. The United Kingdom has arguably been the most proactive, driven by the high-profile drone disruption at Gatwick Airport in 2018, which exposed critical vulnerabilities in airport security. As a result, the United Kingdom closed a number of legal gaps and developed a coordinated Counter-Unmanned Aircraft Strategy.⁴⁹ The Unmanned Aircraft Act 2021 expanded police powers to counter drones and established drone flight restriction zones across a number of critical infrastructure and sensitive sites.

Following the initial efforts of the Biden administration, the Trump administration issued an executive order in 2025 that tasked the Federal Aviation Administration with establishing long delayed rules to restrict drone flights over critical infrastructure and mandated increased enforcement of criminal violations relating to drones. Joint Interagency Task Force 401 was also established to synchronise and coordinate efforts across agencies.⁵⁰ In December 2025, the Safer Skies Act was passed, granting new authority for state and local law enforcement agencies to protect certain sites from drones, and significantly expanding the legal authority to take down drones in the United States.

Germany has paved the way for the amendment of its Aviation Security Act to grant German armed forces the authority to neutralise drones over domestic critical infrastructure. Germany is also drafting reforms to provide police forces with counter-drone tools.⁵¹ Through Project Land 156, the Australian Defence Force will acquire a suite of counter-drone systems, some of which will be deployed for domestic site security.⁵² Australia is also seeking to develop its domestic drone security framework and coordinate drone detection efforts across jurisdictions and sectors. Like Germany, it too is considering counter-drone capabilities for domestic law enforcement.⁵³

Remaining vulnerabilities

These are important initiatives but vulnerabilities remain that these strategies and frameworks do not address.

First is the issue of target proliferation. Although the equipment needed to detect and shoot down small drones is cheap compared with high-end air defence systems, each system covers only a small area that requires constant monitoring. There is no one system that could cover multiple potential targets. Domestic terrorist attack targets could include a vast array of civilian infrastructure and mass gatherings and events, extending well beyond traditional high-value targets such as government buildings or military facilities, which the aforementioned counter-drone systems are designed to protect.⁵⁴

Second, no single counter-UAS mechanism provides comprehensive protection against the full spectrum of vulnerabilities. Radio frequency detection can struggle to identify modified or custom-built drones. Radar systems may be able to detect larger drones but may fail to detect smaller platforms. This means that robust site protection requires the integration of multiple complementary and layered systems, each with their own procurement, maintenance, and operational costs. Authorities must make difficult decisions on not only which sites to protect but which threat profile to defend against at each site.

For example, the European Drone Defence Initiative, also known as the Drone Wall, is an attempt by the European Union to establish a continent-wide defence to counter hostile drones. Not yet realised, and currently stalled due to lack of coordination and political backing, it is a planned interoperable system to detect, locate, and neutralise hostile drones. The Drone Wall is itself vulnerable to malign and extremist actor disruption, either by jamming the wall's sensor systems, interfering with command-and-control systems, or attacking the wall's hardware elements. Because it is primarily intended as a response to Russian drone incursions, it is not clear if it would function effectively against drones deployed by domestic actors internally, or by adversaries from outside Europe.⁵⁵

Third, while there have been legislative changes made to address domestic drone threats across a number of jurisdictions, challenges remain. For example, the Australian Communications and Media Authority prohibits the possession or use of jamming devices except under narrowly defined exemptions. This means that while domestic law enforcement can deploy counter-drone tools in exceptional circumstances, most electronic countermeasures remain legally constrained and subject to strict oversight. In jurisdictions where there is

expanded authority to use jamming devices, malicious actors may deliberately exploit frequencies that authorities are reluctant to jam, such as those used by emergency or cellular networks. And there remains the risk of collateral damage should a drone be brought down in a populated area or over critical infrastructure.

Fourth, governments have attempted to address drone threats through preventive regulation, requiring manufacturers to embed location-based safety features such as geofencing and remote identification into drone design. The EU's Regulation 2019/945, various UK regulations, US Remote ID requirements, and Japan's comparable regulations all mandate geofencing features to prevent unauthorised drone flights near sensitive locations. However, these systems can be disabled or circumvented by malign actors, a process known as "jailbreaking".

The largest commercial drone manufacturer, Chinese company DJI, which accounts for around 70 per cent of the global consumer drone market, announced in November 2025 that it would remove hard geofencing restrictions globally.⁵⁶ Instead, DJI will offer advisory warnings and rely on user compliance rather than preventing take-off and flight in restricted areas. This reveals a fundamental limitation of regulatory approaches that depend on manufacturer cooperation. In December 2025, the US Federal Communications Commission added DJI to its covered list, meaning it will ban the sale of its new products in the United States. While this will mitigate concerns around DJI in the United States, it does not extend to other jurisdictions and may have unintended consequences for US domestic law enforcement and first responders who currently depend on DJI drones for their operations.⁵⁷

Lastly, the contemporary drone threat environment is shaped by the convergence of multiple enabling technologies. Advances in AI reduce operator skill requirements through assisted navigation and object recognition.⁵⁸ Improvements in lithium-polymer and emerging solid-state batteries extend potential range and endurance.⁵⁹ Encrypted communication, such as software-defined radio, creates complications for signals-based countermeasures. This additive ecosystem undermines detection and mitigation systems that rely on predictable performance profiles of commercially standardised systems.

Of note here is 3D printing, which is especially appealing for domestic threat actors operating under resource constraints. While it does not independently transform drone capability in the way automation software or new power systems might, it nonetheless lowers the cost, time, and expertise required to modify physical components to cheaply augment capabilities. Developing AI-enabled autonomous navigation or encrypted command architectures requires advanced coding capability, testing infrastructure, and specialist knowledge. By contrast, consumer-grade 3D printers are widely available, computer-aided design software is easily accessible, and maker communities openly share

modifiable designs. Additive manufacturing is a low-barrier pathway for hardware enhancement and payload increase. While other additive technologies may offer a higher ceiling of capability, 3D printing represents a lower floor of entry.

Policy recommendations

Although the threat of drone use by domestic extremist actors is growing, countries still have an opportunity to act and minimise vulnerabilities. The key elements of that action should be to: (1) establish national counter-drone coordination units whose primary goal is the oversight of domestic counter systems; (2) harmonise and coordinate safety-by-design regulations to achieve international consistency; and (3) formulate and implement specific policies and interventions to address the threat posed by additive manufacturing. These recommendations are designed to be country agnostic while highlighting the need for international engagement and coordination among partner countries.

Counter-drone coordination and international information sharing

Current national counter-drone responses tend to fall awkwardly between multiple agencies with unclear authority hierarchies and no single point of coordination. To begin to address the challenge of domestic extremist and malign actor use of drones, jurisdictions should establish dedicated national counter-drone coordination units, operating as joint task forces, responsible for testing, standardising, and evaluating domestic counter-drone tactics within legal and ethical constraints. The task forces would comprehensively bring together law enforcement operational expertise, aviation regulatory authority, and intelligence service threat assessment capabilities.

The United States has recently established such a coordination unit, the Joint Interagency Task Force 401, which spearheads the acquisition and integration of air defence systems aimed at taking down small uncrewed aerial systems.⁶⁰ Similar coordination units could be established to ensure the efficacy of country-specific counter-drone strategies and platforms.

These units would be responsible for evaluating counter-drone technologies suitable for civilian environments. Military counter-drone systems rely heavily on kinetic interdiction or broad-spectrum jamming that create unacceptable risks in populated areas outside conflict zones. Domestic settings require different approaches. Domestic counter-drone defence requires iterative testing and regular recalibration as both commercial platforms and additive and modification techniques from areas such as 3D printing and AI evolve. The coordination unit would establish testing protocols that evaluate each technology against effectiveness in real-world conditions and work to match those capabilities against known and likely future threats.

National coordination units will be most effective when supported by broader international cooperation. Each country operates under its own distinct regulatory framework; what is legally permissible in one may violate the law in another, forcing nations to develop capabilities in isolation. However, international knowledge sharing can enable countries to identify solutions compatible with their own regulatory constraints while benefiting from collective learning without requiring regulatory harmonisation.

International coordination of safety-by-design regulation

Governments should also focus on preventive approaches that mandate embedded safety features directly into drone design and production. If geofencing and remote identification become standard across legitimate drone operations, unauthorised activity becomes more visible. By making hobbyist and commercial drones easier to identify, and barring them from sensitive areas, authorities will be able to more rapidly distinguish inadvertent disruptions from nefarious threats. Security personnel can treat unidentified drones operating near sensitive sites as potentially hostile rather than spending time sorting genuine threats from casual rule violations.

Regulatory compliance should be a condition of market access, enforced through government verification rather than manufacturer cooperation. This requires prohibiting the import and sale of drones lacking functional safety features, treating non-compliant equipment as contraband at customs, and imposing substantial penalties on distributors selling uncertified products.

Several countries have pursued such a regulatory approach. The United States now requires most registered drones to broadcast Remote ID signals that transmit identifying and location data during flight, while the European Union introduced mandatory remote identification for many drones in 2024 and enforces geofenced airspace restrictions around sensitive locations. Japan similarly mandates remote identification for drones over 100 grams.

However, this approach only succeeds through international coordination among major markets. If countries establish common technical standards and mutual recognition of certification, manufacturers face genuine pressure to comply or forfeit market access. Without coordination, manufacturers optimise for the least restrictive market and circumvent stricter jurisdictions through e-commerce. The international cooperation framework should therefore include common drone certification standards as a central pillar, transforming fragmented national regulations into unified requirements. There will be challenges including enforcement costs for customs inspection and market surveillance, and political obstacles to achieving genuine regulatory harmonisation rather than lowest-common-denominator standards.

DJI's dominance, and its recent shift from manufacturer-reliant to user-reliant safety compliance represents a substantial hurdle to an integrated and robust safety-by-design framework. However, this is precisely why an internationally coordinated regulatory approach is needed. If major markets such as the United States and the European Union, and smaller markets like Australia and Japan, adopt common certification standards, manufacturers will face strong commercial incentives to comply despite regulatory divergence in their home markets.

Similar dynamics are already visible in other areas. Australia's recently enacted regulation of social media use places responsibility on platforms to implement age assurance measures as a condition of operating within the Australian market, regardless of where those platforms are headquartered. A comparable logic can underpin safety-by-design drone regulation. Even when major manufacturers based outside participating jurisdictions do not adopt safety-by-design features, regulatory obligations will require them to comply with certification rules if they wish to sell products in those jurisdictions.

Addressing the threat of additive technology

Even the most comprehensive safety-by-design frameworks cannot account for the growing threat posed by additive technology. While the additive ecosystem includes several threats, the ease of access to 3D printing for domestic malign actors is particularly concerning. Similar challenges have been highlighted in the space of 3D-printed firearms, where so-called "ghost guns" have provided malicious actors with untraceable weapons that circumvent black-market supply chains.⁶¹ Here, several countries, including Australia and the United Kingdom, have responded by criminalising the manufacture and possession of both the products and their digital blueprints.⁶²

However, unlike firearms, which are already heavily restricted in most countries, many 3D-printed drone components serve legitimate recreational and commercial purposes. Over-regulation risks alienating hobbyists and stifling innovation. Rather than sweeping restrictions, policymakers should pursue a more targeted response.

A database of prohibited 3D-printed drone component schematics should be established, regularly updated, and accessible to partner states through existing counter-terrorism cooperation frameworks. Establishing such a database would contribute to internationally coordinated prevention efforts focused on this narrow class of schematics. It would also avoid fragmented national efforts and mitigate the risk of over-regulation.

By establishing this shared list of prohibited blueprints, countries can work with file-sharing platforms and printer manufacturers to target restrictions. AI algorithms can now detect prohibited design files and block their production.

Multiple systems have been developed to detect 3D-printed guns. Print&Go's "3D GUN'T" uses AI-driven filters embedded in printer firmware to help prevent manufacture of restricted items.⁶³ Following US government pressure, Thingiverse, the world's largest platform for 3D printing files, implemented AI-powered detection that scans uploads to flag and remove prohibited designs.⁶⁴ These interventions occur at multiple points in the process, including on file-sharing platforms, in slicer software that prepares models for printing, and in printer firmware itself.

The effectiveness of such a framework relies on widespread industry participation. Printer manufacturers unwilling to implement detection systems or embed identifying protocols would face market access restrictions in participating countries, similar to the internationally coordinated manufacturer enforcement approaches suggested above for commercial off-the-shelf drones.

Conclusion

For a threat to pose real danger, it requires intent, capability, and opportunity. Domestic extremists have all three. They have already demonstrated the will to deploy drones as weapons, and while their attempts have so far fallen short, that record of failure should not be mistaken for the ceiling of their ambitions. The capabilities of the technology and those intent on using it for extremist ends are becoming more sophisticated. The opportunity presented by this convergence means it is not a matter of whether domestic extremists will accelerate their use of drones, but whether governments will have done enough to stop them.

Notes

- 1 Milton Hoenig, “Hezbollah and the Use of Drones as a Weapon of Terrorism”, Federation of American Scientists, 5 June 2014, <https://fas.org/publication/hezbollah-use-drones-weapon-terrorism/>.
- 2 Don Rassler and Yannick Veilleux-Lepage, “On the Horizon: The Ukraine War and the Evolving Threat of Drone Terrorism”, *CTC Sentinel*, Volume 18, Issue 3, March 2025, <https://ctc.westpoint.edu/on-the-horizon-the-ukraine-war-and-the-evolving-threat-of-drone-terrorism/>.
- 3 Daveed Gartenstein-Ross, David Jones, and Matt Shear, “Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters”, Valens Global, 20 November 2019, <http://valensglobal.com/virtual-plotters-drones-weaponized-ai-violent-non-state-actors-as-deadly-early-adopters/>.
- 4 Emil Archambault and Yannick Veilleux-Lepage, “Drone Imagery in Islamic State Propaganda: Flying Like a State”, *International Affairs*, Volume 96, Issue 4, July 2020, <https://doi.org/10.1093/ia/iiaa014>.
- 5 Emil Archambault and Yannick Veilleux-Lepage, “Drone Imagery in Islamic State Propaganda: Flying Like a State”, *International Affairs*, Volume 96, Issue 4, July 2020, <https://doi.org/10.1093/ia/iiaa014>.
- 6 Don Rassler and Yannick Veilleux-Lepage, “On the Horizon: The Ukraine War and Evolving Threat of Drone Terrorism”, *CTC Sentinel*, Volume 18, Issue 3, March 2025, <https://ctc.westpoint.edu/on-the-horizon-the-ukraine-war-and-the-evolving-threat-of-drone-terrorism/>.
- 7 Thomas Gibbons-Neff, “ISIS Drones are Attacking US Troops and Disrupting Airstrikes in Raqqa, Officials Say”, *The Washington Post*, 14 June 2017, <https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say/>.
- 8 Chelsea Daymon, Yannick Veilleux-Lepage, and Emil Archambault, “Learning from Foes: How Racially and Ethnically Motivated Violent Extremists Embrace and Mimic Islamic State’s Use of Emerging Technologies”, Global Network on Extremism and Technology, Report, 7 June 2022, <http://gnet-research.org/2022/06/07/learning-from-foes-how-rationally-and-ethnically-motivated-violent-extremists-embrace-and-mimic-islamic-states-use-of-emerging-technologies/>.
- 9 Video Shows Lashkar-e-Taiba Testing the Capability of Dropping Terrorists via Drones”, CNN-News 18, 15 September 2023, <https://www.youtube.com/watch?v=B6zbJro-GY8>.
- 10 Austin C. Doctor, “The Logic of Terrorist Use of Unmanned Aerial Systems, Enabling Factors, and Barriers to Exploitation”, Report prepared for the National Counterterrorism Innovation, Technology, and Education Center (NCITE), April 2025, <https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1129&context=ncitereportsresearch>.

- 11 Broderick McDonald, “The Drones of Hayat Tahrir al-Sham: The Development and Use of UAS in Syria”, Global Network on Extremism and Technology, *GNET Insights*, 20 December 2024, <https://gnet-research.org/2024/12/20/the-drones-of-hayat-tahrir-al-sham-the-development-and-use-of-uas-in-syria/>.
- 12 Defense Intelligence Agency, “Iran: Enabling Houthi Attacks across the Middle East”, Defense Intelligence Agency, Report, February 2024, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Iran_Houthi_Final2.pdf.
- 13 Don Rassler, “Going the Distance: The Emergence of Long-Range Stand-Off Terrorism”, *CTC Sentinel*, Volume 17, Issue 2, February 2024, <https://ctc.westpoint.edu/going-the-distance-the-emergence-of-long-range-stand-off-terrorism/>.
- 14 “Hydrogen-Powered Houthi Drones”, Conflict Armament Research, Yemeni Dispatch, March 2025, <https://storymaps.arcgis.com/stories/c4eae92382c7456cae8c607af9d03794>.
- 15 Shira Rubin and Loveday Morris, “How Hamas Broke through Israel’s Border Defenses during Oct. 7 Attack”, *The Washington Post*, 27 October 2023, <https://www.washingtonpost.com/world/2023/10/27/hamas-attack-israel-october-7-hostages/>.
- 16 Elisabeth Gosselin-Malo, “Hamas Drones Helped Catch Israel off Guard, Experts Say”, *C4ISRNet*, 19 October 2023, <https://www.c4isrnet.com/global/mideast-africa/2023/10/18/hamas-drones-helped-catch-israel-off-guard-experts-say/>.
- 17 Don Rassler and Yannick Veilleux-Lepage, “On the Horizon: The Ukraine War and Evolving Threat of Drone Terrorism”, *CTC Sentinel*, Volume 18, Issue 3, March 2025, <https://ctc.westpoint.edu/on-the-horizon-the-ukraine-war-and-the-evolving-threat-of-drone-terrorism/>.
- 18 Isabelle Khurshudyan, Mary Ilyushina, and Kostiantyn Khudov, “Russia and Ukraine are Fighting the First Full-Scale Drone War”, *The Washington Post*, 2 December 2022, <https://www.washingtonpost.com/world/2022/12/02/drones-russia-ukraine-air-war/>.
- 19 Brad Lendon, “Drones have Already Revolutionized Warfare. They’re about to Do it Again”, CNN, 27 November 2025, <https://edition.cnn.com/2025/11/27/world/history-future-of-drones-intl-hnk-ml-dst>; Eric Schmidt and Greg Grant, “The Dawn of Automated Warfare”, *Foreign Affairs*, 12 August 2025, <https://www.foreignaffairs.com/russia/dawn-automated-warfare>; Kristen D. Thompson, “How the Drone War in Ukraine is Transforming Conflict”, Council on Foreign Relations, 16 January 2024, <https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict>.
- 20 Eric Schmidt and Greg Grant, “The Dawn of Automated Warfare”, *Foreign Affairs*, 12 August 2025, <https://www.foreignaffairs.com/russia/dawn-automated-warfare>.
- 21 David Kirichenko, “Fibre-Optic Drones Reshape Ukraine’s Technological War”, *The Interpreter*, 6 August 2025, <https://www.lowyinstitute.org/the-interpreter/fibre-optic-drones-reshape-ukraine-s-technological-war>; Vikram Mittal, “New Russian Fiber-Optic Drones will Expand Depth of their Kill Zones”, *Forbes*, 25 September 2025, <https://www.forbes.com/sites/vikrammittal/2025/09/25/russia-introduces-fiber-optic-repeater-drones-to-increase-strike-range/>.
- 22 Eric Schmidt and Greg Grant, “The Dawn of Automated Warfare”, *Foreign Affairs*, 12 August 2025, <https://www.foreignaffairs.com/russia/dawn-automated-warfare>.

- 23 Eric Schmidt and Greg Grant, “The Dawn of Automated Warfare”, *Foreign Affairs*, 12 August 2025, <https://www.foreignaffairs.com/russia/dawn-automated-warfare>.
- 24 Don Rassler and Yannick Veilleux-Lepage, “On the Horizon: The Ukraine War and Evolving Threat of Drone Terrorism”, *CTC Sentinel*, Volume 18, Issue 3, March 2025, <https://ctc.westpoint.edu/on-the-horizon-the-ukraine-war-and-the-evolving-threat-of-drone-terrorism/>.
- 25 Yannick Veilleux-Lepage, *How Terror Evolves: The Emergence and Spread of Terrorist Techniques* (London, England: Rowman & Littlefield International, 2020).
- 26 David Martin Jones and M.L.R. Smith, “The Strategy of Savagery: Explaining the Islamic State”, *War on the Rocks*, 24 February 2015, <https://warontherocks.com/2015/02/the-strategy-of-savagery-explaining-the-islamic-state/>.
- 27 David Hambling, “Moving Targets: Implications of the Russo-Ukrainian War for Drone Terrorism”, *CTC Sentinel*, Volume 18, Issue 7, July 2025, <https://ctc.westpoint.edu/moving-targets-implications-of-the-russo-ukrainian-war-for-drone-terrorism/>.
- 28 Laura Gozzi and BBC Verify, “How Ukraine Carried Out Daring ‘Spider Web’ Attack on Russian Bombers”, BBC, 3 June 2025, <https://www.bbc.com/news/articles/cq69qnvj6nlo>.
- 29 Don Rassler, “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology”, Combating Terrorism Centre at West Point, Report, October 2016, <https://ctc.westpoint.edu/wp-content/uploads/2016/10/Drones-Report.pdf>.
- 30 Daveed Gartenstein-Ross, Colin P. Clarke, and Matt Shear, “Terrorists and Technological Innovation”, *Lawfare*, 2 February 2020, <https://www.lawfaremedia.org/article/terrorists-and-technological-innovation>.
- 31 Don Rassler, “Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology”, Combating Terrorism Centre at West Point, Report, October 2016, <https://ctc.westpoint.edu/wp-content/uploads/2016/10/Drones-Report.pdf>.
- 32 Nick Paton Walsh, et al., “Inside the August Plot to Kill Maduro with Drones”, CNN, 21 June 2019, <https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl>.
- 33 John Davison and Ahmed Rasheed, “Iraqi PM Decries ‘Cowardly’ Attack on his Home by Drones Carrying Explosives”, Reuters, 8 November 2021, <https://www.reuters.com/world/middle-east/iraqi-pm-chairs-security-meeting-after-drone-attack-residence-2021-11-07/>.
- 34 Håvard Haugstvedt, “The Right’s Time to Fly?”, *RUSI Journal*, Volume 166, Issue 1, 26 April 2021, <https://doi.org/10.1080/03071847.2021.1906161>.
- 35 Jessica Murray, “Birmingham PhD Student Guilty of Using 3D Printer to Build ‘Kamikaze’ Drone”, *The Guardian*, 29 September 2023, <https://www.theguardian.com/uk-news/2023/sep/28/birmingham-phd-student-mohamad-al-bared-guilty-using-3d-printer-to-build-kamikaze-drone>.
- 36 Georgia Loney, “Seven People Arrested in Counter-Terrorism Sting in Regional Queensland”, ABC, 5 November 2025, <https://www.abc.net.au/news/2025-11-05/police-arrest-seven-people-in-qld-counter-terrorism-operation/105974254>.

- 37 Jessica Rawnsley, “Suspected Jihadist Drone Plot against Belgian PM Foiled”, BBC, 10 October 2025, <https://www.bbc.com/news/articles/cd721zd4xo>.
- 38 Antonio Planas and Minyvonne Burke, “Arizona Teen Planned Attack on Phoenix Pride Festival, Prosecutors Say”, NBC, 24 October 2024, <https://www.nbcnews.com/news/us-news/arizona-teen-planned-attack-phoenix-pride-festival-prosecutors-say-rcna176958>.
- 39 Austin C. Doctor, “The Logic of Terrorist Use of Unmanned Aerial Systems, Enabling Factors, and Barriers to Exploitation”, Report prepared for the National Counterterrorism Innovation, Technology, and Education Center (NCITE), April 2025, <https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1129&context=ncitereportsresearch>.
- 40 Michael Kosnar and Ken Dilanian, “Trump Shooter Flew Drone over Venue Hours before Attempted Assassination, Source Says”, NBC, 20 July 2024, <https://www.nbcnews.com/news/us-news/trump-shooter-flew-drone-venue-hours-attempted-assassination-source-sa-rcna162817>.
- 41 Austin C. Doctor, “The Logic of Terrorist Use of Unmanned Aerial Systems, Enabling Factors, and Barriers to Exploitation”, Report prepared for the National Counterterrorism Innovation, Technology, and Education Center (NCITE), April 2025, <https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1129&context=ncitereportsresearch>.
- 42 Jonathan Lewis and Luke Baumgartner, “Droning On: The Response to Use of Drones by Domestic Violent Extremists”, *GNET Insights*, 27 January 2025, <https://gnet-research.org/2025/01/27/droning-on-the-response-to-use-of-drones-by-domestic-violent-extremists/>.
- 43 Ben Makuch, “Alarm as US Far-Right Extremists Eye Drones for Use in Domestic Attacks”, *The Guardian*, 30 August 2025, <https://www.theguardian.com/us-news/2025/aug/30/us-far-right-extremists-drones>.
- 44 David Hambling, “Dozens More Mystery Drone Incursions over US Nuclear Power Plants Revealed”, *Forbes*, 7 September 2020, <https://www.forbes.com/sites/davidhambling/2020/09/07/dozens-more-drone-incursions-over-us-nuclear-power-plants-revealed/>.
- 45 Samira Shackle, “The Mystery of the Gatwick Drone”, *The Guardian*, updated 1 December 2020, <https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone>; Alice Evans, “Heathrow Airport: Drone Sighting Halts Departures”, BBC, 19 January 2019, <https://www.bbc.com/news/uk-46803713>.
- 46 Gordon Lubold, Lara Seligman, and Aruna Viswanatha, “Mystery Drones Swarmed a US Military Base for 17 Days. The Pentagon is Stumped”, *The Wall Street Journal*, 12 October 2024, <https://www.wsj.com/politics/national-security/drones-military-pentagon-defense-331871f4>.
- 47 Jon Harper, “NORAD Commander Says Hundreds of Drone Incursions were Detected at US Military Installations”, *Defense Scoop*, 13 February 2025, <https://defensescoop.com/2025/02/13/drone-incursions-us-military-bases-norad-northcom-counter-small-uas/>.
- 48 David Crowe, “How a Single Night of Mayhem Exposed Dangerous Gap in Europe’s Defences”, *The Age*, 23 October 2025, <https://www.theage.com.au/world/europe/how-a-single-night-of-mayhem-exposed-dangerous-gap-in-europe-s-defences-20251023-p5n4n9>.

- html; Robyn Ironside, “100 Drones a Day in Sydney Airport No Fly Zone”, *The Australian*, 8 August 2023, <https://www.theaustralian.com.au/business/aviation/100-drones-a-day-detected-in-sydney-airport-no-fly-zone/news-story/34e1773b6aefa5ea88d85fb0e704fc13>.
- 49 UK Government, Home Office, “UK Counter-Unmanned Aircraft Strategy”, 21 October 2019, <https://www.gov.uk/government/publications/uk-counter-unmanned-aircraft-strategy>.
- 50 US Department of War, “JIATF-401 Announces Updated Guidance to Counter Drone Threats in the Homeland”, 26 January 2026, <https://www.war.gov/News/Releases/Release/Article/4389392/jiatf-401-announces-updated-guidance-to-counter-drone-threats-in-the-homeland/>.
- 51 Hila Kochavi, “Navigating the European Skies: Pushing for a Unified Counter-Drone Regulatory Framework”, *Sentrycs*, 22 April 2025, <https://sentrycs.com/the-counter-drone-blog/navigating-the-european-skies-the-push-for-a-unified-counter-drone-regulatory-framework/>.
- 52 Australian Government, “Albanese Government Ramps Up Investment in Counter-Drone Capabilities for ADF”, 27 August 2025, <https://www.minister.defence.gov.au/media-releases/2025-08-27/albanese-government-ramps-up-investment-counter-drone-capabilities-adf>; Australian Government, “Government Boosts Response to Drone Threats”, Defence Ministers, 29 January 2026, <https://www.minister.defence.gov.au/media-releases/2026-01-29/government-boosts-response-drone-threats>.
- 53 Australian Government, “Security Policy”, Drones.gov, <https://www.drones.gov.au/policies-and-programs/policies/security-policy>.
- 54 The Asia Group, “Counter-Uncrewed Aerial Systems (C-UAS) and the Protection of Critical Infrastructure”, October 2025, <https://theasiagroup.com/wp-content/uploads/2025/11/Counter-Uncrewed-Aerial-Systems-Report-.pdf>.
- 55 Nina Kurt, “Testing Resilience: Can the Proposed EU Drone Wall Defend against Extremist Actors?”, *GNET Insights*, 16 January 2026, <https://gnet-research.org/2026/01/16/testing-resilience-can-the-proposed-eu-drone-wall-defend-against-extremist-actors/>.
- 56 “DJI Expands GEO System Update to Remaining International Markets Worldwide”, DJI Media Center, 17 November 2025, <https://www.dji.com/media-center/announcements/dji-expands-geo-system-update-to-remaining>.
- 57 Jack Daleo, “Drone Pilots Fear Worst after Foreign Equipment Ban”, *Flying Magazine*, 27 December 2025, <https://www.flyingmag.com/drone-pilots-fear-worst-china-dji-ban/#:~:text=The%20U.S.%20Federal%20Communications%20Commission,due%20to%20national%20security%20concerns>.
- 58 David Hambling, “Ukraine’s Killer AI Drones are Back with a Vengeance”, *Forbes*, 2 January 2026, <http://forbes.com/sites/davidhambling/2026/01/02/ukraines-killer-ai-drones-are-back-with-a-vengeance/>.
- 59 “Advancements in Drone Battery Technology and Performance”, *Leher*, 3 September 2025, <https://www.leher.ag/blog/drone-battery-technology-advancements-performance>.
- 60 Meghann Myers, “Pentagon Stands Up New Task Force to Coordinate Anti-Drone Efforts”, *Defense One*, 28 August 2025, <https://www.defenseone.com/defense-systems/2025/08/>

[pentagon-stands-new-group-coordinate-anti-drone-efforts/407778/](https://doi.org/10.1080/1057610X.2025.2477849).

- 61 Rueben Dass, “3D Printed Firearms: Global Proliferation Trends and Analyses”, *Studies in Conflict and Terrorism*, Volume 1, No. 35, 20 May 2025, <https://doi.org/10.1080/1057610X.2025.2477849>.
- 62 Rueben Dass, “3D Printed Firearms: Global Proliferation Trends and Analyses”, *Studies in Conflict and Terrorism*, Volume 1, No. 35, 20 May 2025, <https://doi.org/10.1080/1057610X.2025.2477849>.
- 63 “3D GUN’T: Print&Go’s Solution to Prevent 3D Printed ‘Ghost Guns’”, *Print&Go*, 4 November 2024, <https://printandgo.tech/blog/3d-gunt-solution-to-prevent-3d-printed-ghost-guns>.
- 64 Denise Bertacchi, “We Spoke with Thingiverse about its New AI-Driven Ghost Gun Detection that Eliminates Designs for 3D Printing — Companies Turn to AI to Block Production of Ghost Guns”, *Tom’s Hardware*, 26 July 2025, <https://www.tomshardware.com/3d-printing/3d-printing-companies-turn-to-ai-to-block-production-of-ghost-guns-we-spoke-with-thingiverse-about-its-new-ai-driven-ghost-gun-detection-strategy>.

About the authors



Dr James Paterson is the Research Associate for the Transnational Challenges Program at the Lowy Institute. He holds a PhD from Monash University where his research focuses on insurgent dynamics and legitimacy.



Lydia Khalil is Program Director of the Transnational Challenges Program at the Lowy Institute. She is also a Senior Research Fellow at Deakin University's Alfred Deakin Institute. She serves as an editorial board member of the academic journal *Studies in Conflict & Terrorism* and is former convener of the Addressing Violent Extremism and Radicalisation to Terrorism (AVERT) Research Network.

She has previously served as a senior policy adviser with various US government agencies such as the US Department of Defense, Boston Police Department, and New York Police Department. Her research interests include new forms of violent extremism, counter-terrorism and countering violent extremism, the intersection of technology and social harms, threats to democracy, and democratic resilience.

Lydia is a frequent media commentator and has published widely in both popular and academic publications on her areas of expertise. She is the author of *Rise of the Extreme Right: The New Global Extremism and the Threat to Democracy* (Penguin, 2022).

LOWY INSTITUTE