



The UAS Governance Gap

Securing European Airspace Before the Next Crisis

CHALLENGER RESEARCH STRATEGIC BRIEFING: CR/DEF/UAS/2026/01

Executive Briefing

Challenger Research and TWA present findings from The UAS Governance Gap — an independent strategic intelligence briefing examining UAS risk, regulatory misalignment, and counter-UAS governance across the UK and European Union.

Research Partners

- **Challenger Research:** Regulatory, policy, and geopolitical analysis.
- **TWA:** UK parliamentary/policy dynamics

Briefing reference: **CR/DEF/UAS/2026/01**

Webinar Content

- Part 1: **Overview**
- Part 2: **Regulatory & Enforcement Constraints**
- Part 3: **Public Attitudes (TWA)**
- Part 4: **Findings & Discussion**
- Part 5: **Implications for Industry**
- Part 6: **Conclusion**
- Part 7: **Q&A**

PART 1

Overview

"It is not only about a state launching attacks, we must be ready for any kind of strike, including from non-state actors, criminal networks, terrorist groups and even lone attackers who can gain access to such technologies" **Volodymyr Zelenskyy, March 2026**

A Critical Inflection Point

Active Threat Vector

Unmanned aerial systems (including FPV systems and loitering drones) are an active and clear threat (Russia & Iran).

Outpaced Governance

The threat environment is evolving faster than governance and procurement systems designed to manage it.

Awareness Asymmetry

Those closest to the issue express deep concern while those with the power to enact change have the least awareness of the issue.



Methods

Structured, multi-layer analytical design combining four workstreams.

1

Regulatory, Policy & Legal Review

I.e. Civil Aviation Act; ANO 2016; Wireless Telegraphy Act; EU Regs 2019/947-945; ATMUA 2021.

2

Stakeholder Interviews

Interviews (23) across defence, policy, and CNI stakeholders.

3

Gap Identification

Analysis of systemic misalignments across civil–military sectors.

4

Risk Evaluation

Risk severity and 24-month operational outlook. Industry & policy recommendations.

Governance Barriers



Autonomy is reshaping the threat

"Electronic Warfare and protocol attacks will define the next phase." — **Defence Prime Executive** regarding Counter-UAS



Grey-zone dynamics

Drone incursions are ambiguous, deniable, and rarely trigger unified political action.



Reactive Policy

Crisis-driven reform remains the most probable inflection point.



PART 2

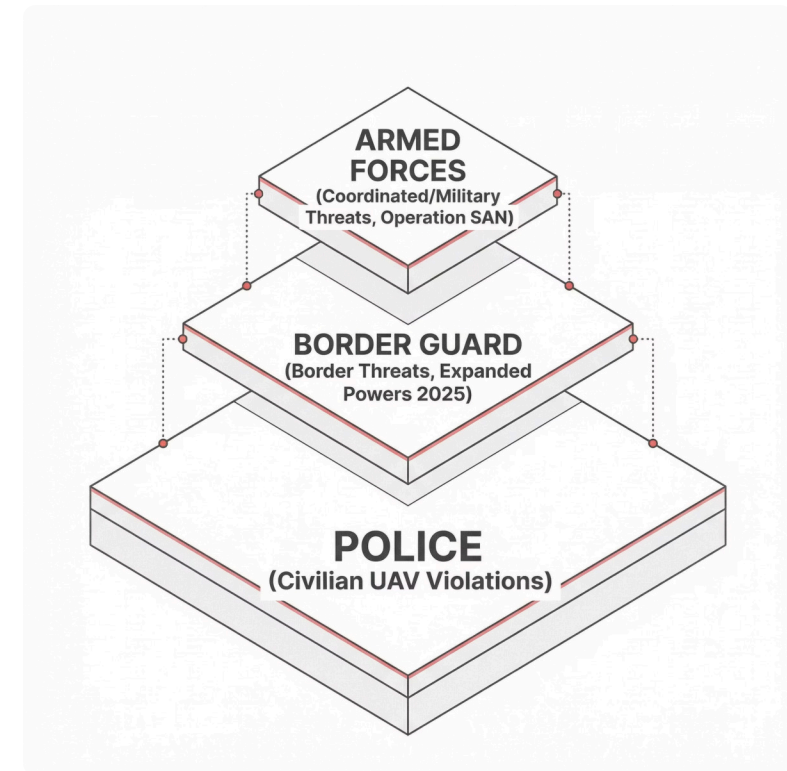
Regulatory and Enforcement Constraints

A structured audit of UK and EU counter-UAS authority finds that capability is constrained more by legal, jurisdictional, and political misalignment, than lacking technology.

Early Escalation and Legal Redundancy

Poland's Approach

Poland treats hostile drone activity as a core hybrid-warfare threat. Jurisdiction is **effects-based** — if a drone threatens borders or critical infrastructure, military authority activates even below armed-conflict thresholds.



Eastern Shield / Operation SAN

Multilayered air defence combining kinetic and electronic warfare means under Armed Forces command

Legal Redundancy

Police, Border Guard, and Armed Forces all empowered simultaneously — ambiguity treated as threat, not anomaly

Attribution Before Neutralisation

United Kingdom

Police lead detection and disruption. Military role is limited and exceptional — even on military bases, Armed Forces operate under police authority.

- Intelligence fusion prioritised over rapid neutralisation.
- Escalation carefully managed; attribution assessed first.
- **Armed Forces Bill (2026)** proposes limited site-specific powers (as of Feb 2026).

Germany

Aviation-security framing; constitutional limits on Bundeswehr. Joint Drone Defence Centre (GDAZ) opened Dec 2025 for coordination, but command remains civilian.

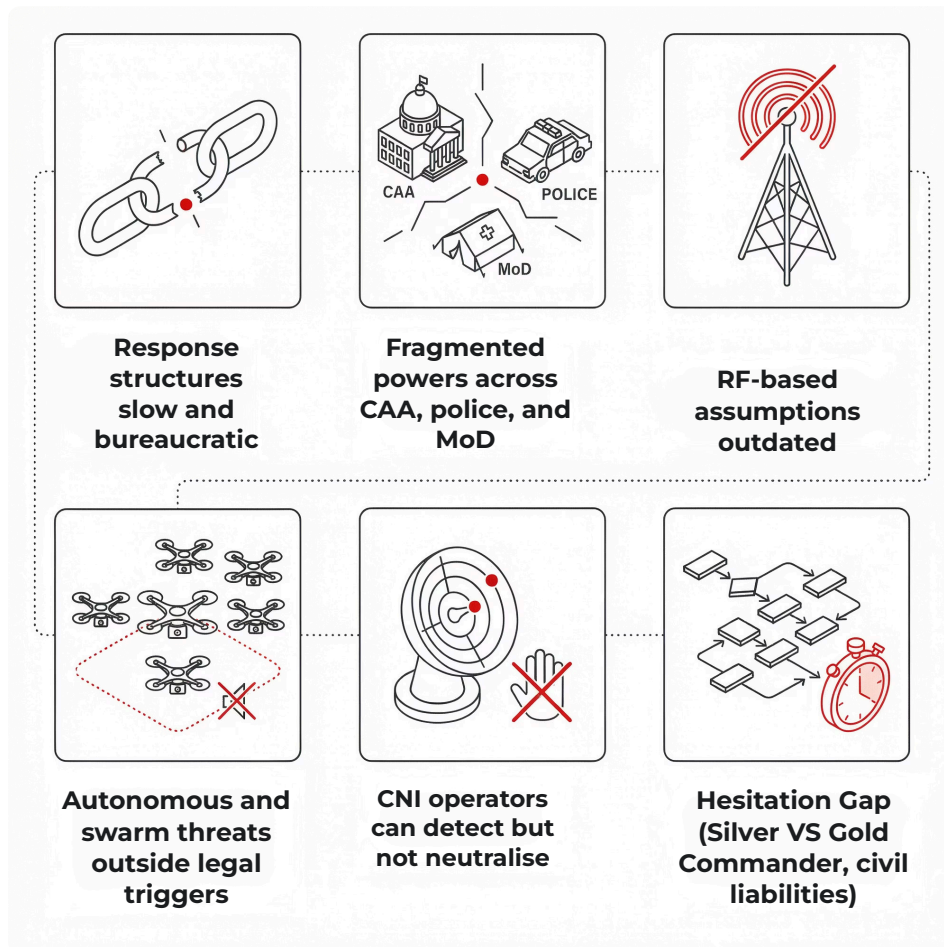
Proposed Aviation Security Act reform would allow limited armed forces assistance; politically contested.

Italy

UNCLOS constrains offshore response. In the EEZ and high seas, drone surveillance is not unlawful per se — engagement requires imminent threat under UN Charter Art. 51.

Hybrid tactics remain legally tolerable yet strategically destabilising.

Authority Without Capability, Capability Without Authority



The Core Finding

UK/EU counter-UAS capability is constrained by legal, jurisdictional, and political misalignment.

EU Regulatory Framework

The EU provides a safety and technical framework under Regulations 2019/947 and 2019/945, but all enforcement and counter-UAS authority is explicitly reserved to Member States. Under the EASA Basic Regulation (2018/1139), security and defence are excluded from EASA's mandate.

National CAAs

Implement EU safety rules; manage registries; define UAS geographical zones; may halt aerodrome operations — but hold **no interdiction authority**.

Police / Internal Security

Enforce national aviation and criminal laws; deploy limited counter-UAS tools subject to authorisation; electronic measures require telecom-regulator approval.

Defence

May support when national security is implicated or civil capabilities are exceeded; roles and powers vary significantly by Member State.



UK Regulatory Framework

The UK operates a multi-layered statutory framework. The CAA regulates civil UAS under the Civil Aviation Act 1982 and ANO 2016. Police enforcement derives from the Air Traffic Management and Unmanned Aircraft (ATMUA) Act 2021. Jamming is tightly constrained under the Wireless Telegraphy Act 2006.

1

CAA

Statutory delegation; defined enforcement authority; non-operational technical role; oversight by DfT and Parliament.

2

Police

Operational authority under ATMUAA; jamming and advanced counter-UAS subject to senior-level authorisation.

3

MoD

Jurisdiction limited to MoD sites; MACA-based escalation for civil support; countermeasures require Crown or statutory authorisation.

4

Coordination

Bronze–Silver–Gold command structure; integrated alerting between police, CAA, and ATC; cross-government MoUs.

Capability Gaps

Low-Altitude Air Defence

National air defence architectures were not designed for persistent small-scale UAS incursions. One industry leader stated the UK has had **"essentially no air defence for 20 years"**.

Testing Pathways

Developers cannot test RF/GNSS interference, cyber interdiction, or kinetic interception in realistic environments. Adversaries iterate without equivalent legal restriction.

Autonomous and Swarm Threats

Jammers are becoming increasingly ineffective against autonomous, non-RF, and swarm-capable systems. Current legal bases do not cover these threat categories.

Electronic Warfare Frontier

Future counter-UAS challenges will centre on signal disruption and protocol manipulation, not purely kinetic interception.



Image: A Gerbera drone landed in a field in the Olesno region of Poland after being shot down by NATO aircraft.

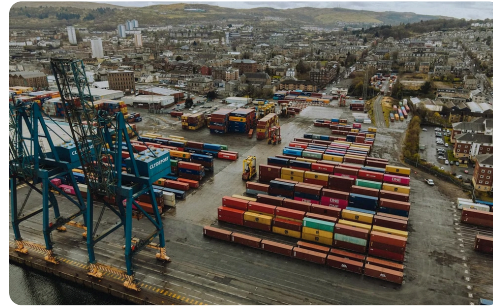
Infrastructure Implications

CRITICAL NATIONAL INFRASTRUCTURE



Aviation

Airport counter-UAS responses are constrained by political caution, strict jamming controls, and senior-level authorisation requirements. Runways remain exposed during the decisive early phase of ambiguous incidents.



Ports and Maritime

Regulations applicable to airports do not currently apply to ports. Very little capability in place.



Energy

Most operators can detect but not neutralise drones due to legal prohibitions on active measures. Reliance on private security with limited powers leaves infrastructure exposed.

Grey Zone Activity: The Hidden Blocker

Grey zone activity removes the "smoking gun" policymakers rely on to justify action. This obscures both the trigger and the perpetrator.

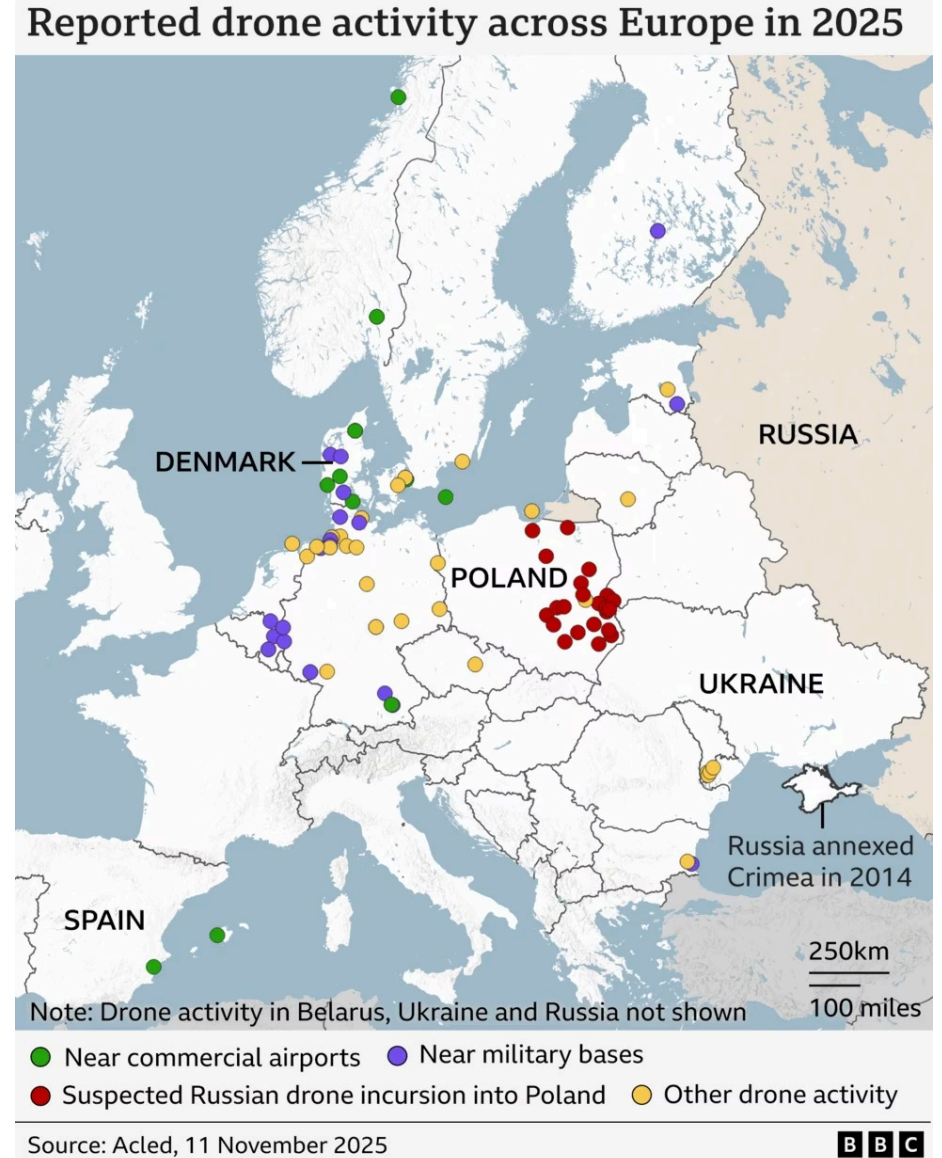
No Clear Trigger

Incidents are designed to be ambiguous. No single event is sufficient to force political change.

No Clear Perpetrator

A well-executed grey zone attack leaves uncertainty about both responsibility and intent — paralyzing MOD decision-making.

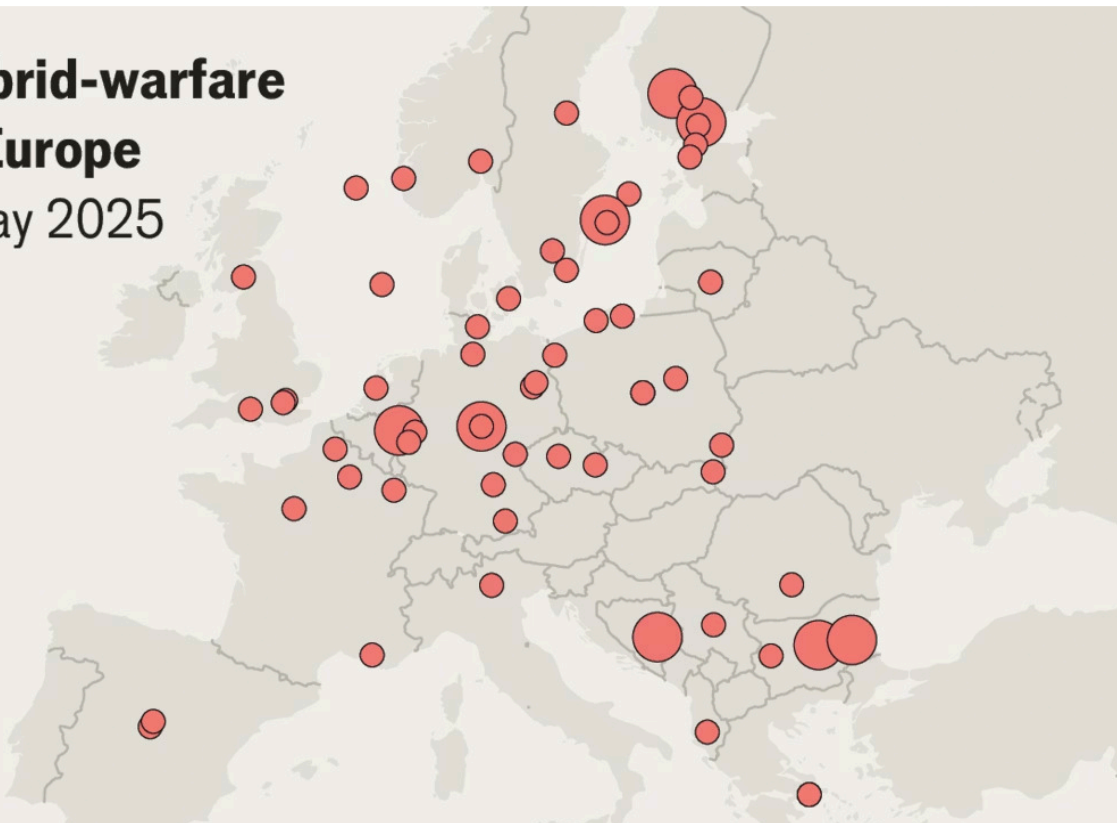
"The grey zone will continue to exist because of the accountability-responsibility gap. Drones are in the same space." — Critical infrastructure, airports, ports, minerals



From Nuisance to Strategic Threat

Russian hybrid-warfare attacks in Europe

Jan 2018-May 2025



Key Findings

- Incidents tend to be geographically clustered closer to NATO's **northern and eastern flanks**.
- Drone types range from commercial models for plausible deniability to **3D-printed swarms** and military-grade units.
- Operations thus far have primarily been **intelligence-gathering** in nature.

Source: The Economist 2025

Three Systemic Deficits



These three deficits collectively create operational paralysis, prolong airport closures, expose critical infrastructure, and hinder development of advanced counter-UAS technologies.

Stakeholder Findings

- "Rules of engagement are the primary issue." — Industry stakeholder
- "There is no ownership of responsibility." — Industry stakeholder
- "We lack a clear kinetic response framework." — Industry stakeholder

PART 3

Public Attitudes

Awareness of UAS risks varies significantly across UK and European stakeholders. This asymmetry has direct consequences for governance, trust, and procurement decisions.

The Coming Crisis

77%

Russia as Threat

of Britons think Russia is a moderate or major threat to Europe (Electoral Calculus, 2025)

45%

Attack Risk

of Britons think the UK is at risk of military attack

55%

Defence Confidence

confident the UK can defend against an attack — down from 70% in 2022 (Ipsos)

"The next big change will happen as a result of a crisis and there will very likely be an overcorrection." — Critical infrastructure, airports, ports, minerals

"We have absolutely no idea how badly our infrastructure is defended." — Media commentator

UAS Data (UK)



Emergency Services

Support for drone use by emergency responders



Infrastructure Inspection

Support for using drones to inspect infrastructure



Security & Surveillance

Support for security and surveillance applications



Concerned About Misuse

Voters worried about the misuse of drones

Policymakers believe drones are not salient for voters — and they are broadly correct. Drones don't come up organically.

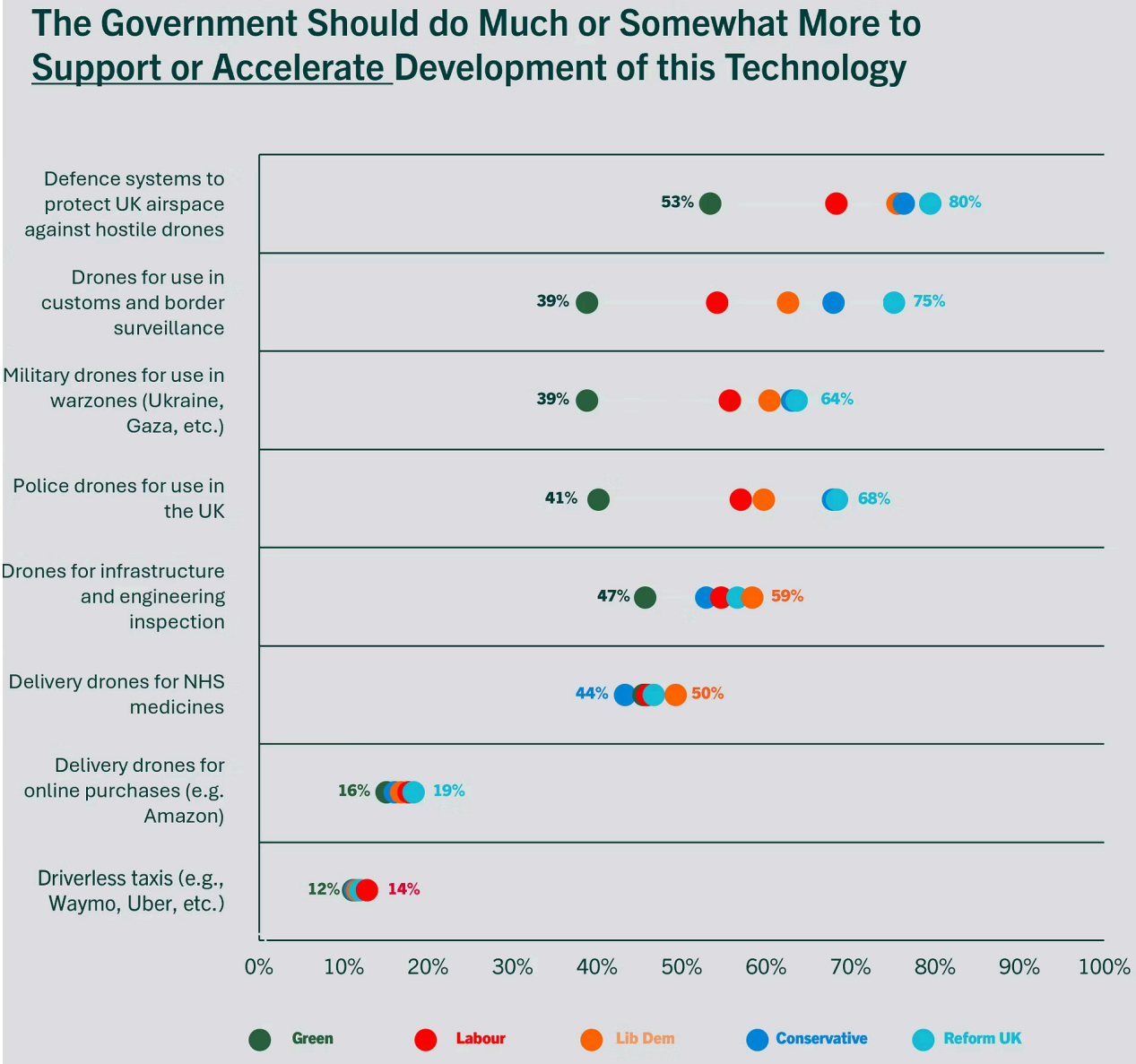
Yet when asked directly, public support is striking. **NATS 2025 data** reveals strong backing across multiple use cases.

The Latent Opportunity

Voters see a future for drones but aren't clamouring for their adoption. They perceive drones as speculative — existing in faraway battlefields or arriving "soon" for civilian use. They feel like a technology about to arrive, not one demanding urgent attention today.

- ❑ 34% of voters worry specifically about the military use of drones as weapons — a (low) ceiling on defence-framed advocacy.

Cross-Party Sea Change



53%

Lowest Support

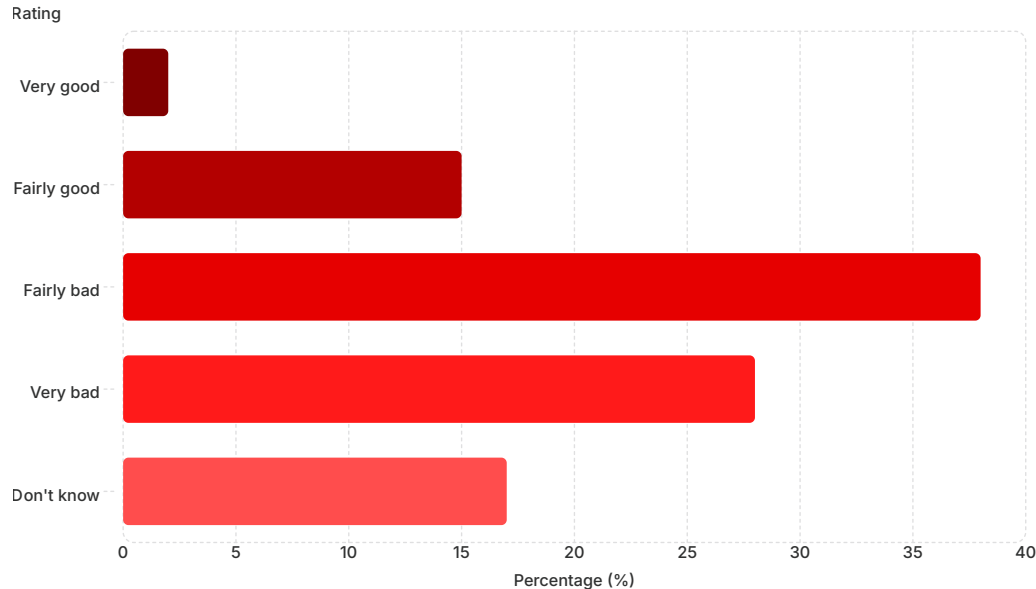
Green voters back accelerating UK defence systems against hostile drones

80%

Highest Support

Reform support for defence systems to protect UK airspace

UK Infrastructure Delivery: Public Confidence



YouGov, 3,532 UK adults, June 2022. "Generally speaking, do you think the UK is good or bad at delivering major infrastructure projects?"

Implications for Drone Policy

- 66% of adults rate UK infrastructure delivery as fairly or very bad.
- Confidence in UK defence capability has fallen from 70% (2022) to 55% (recent Ipsos poll).
- Scepticism about delivery stacks the deck against dynamic drone innovation policy.
- "If there's a positive story to tell, they aren't telling it." — CNI professional



The Political Dimension: Delivery Confidence Is Low



Structural delivery scepticism constrains ambition

66% of UK adults consider the UK bad at delivering major infrastructure projects (YouGov, 2022). Drone policy is not exempt from this perception.



No single department owns the problem

"Drones tend to be used in ways that aren't very clear cut, which makes them awkward to deal with through existing policies and structures." — Conservative staff member



Crisis remains the most probable catalyst

"When a crisis happens, we'll hold the government to account - the message will be for Labour to get a grip." — Conservative staff member.

European Attitudes

Public concern is demonstrably rising yet no systematic EU-wide measurement of civilian threat perception exists — itself a governance gap.

The data simply does not exist.



The Awareness Crisis

One paper by Stolz et al. (2024) looked at drone opinions in general.

The word cloud shows the risks and concerns 2998 European Participants associate with drones. The bigger the words, the more frequently they were stated by the participants.

Citizens across 6 European countries thought of privacy, people, falling and accidents before invasion or grey zone related words.

PART 4

Findings & Discussion

Multiple cross-cutting risks identified across defence primes, policymakers, infrastructure operators, and industry leaders.

Political Salience



Political Salience: Critically Low

Source: 23 interviews across defence, industry, CNI, and politics.



Policymakers frame drones through existing priorities: jobs, industrial growth, sovereign capability.



Awareness of the regulatory environment is minimal. Enforcement constraints are poorly understood.



"Outside of a small group engaged in defence policy, no one is thinking about this. It's not politically salient." — Labour SpAd



Without political salience, structural reform lacks the incentive to proceed.

Awareness vs Concern by Work Category

1 Defence Industry: Highest Awareness & Concern

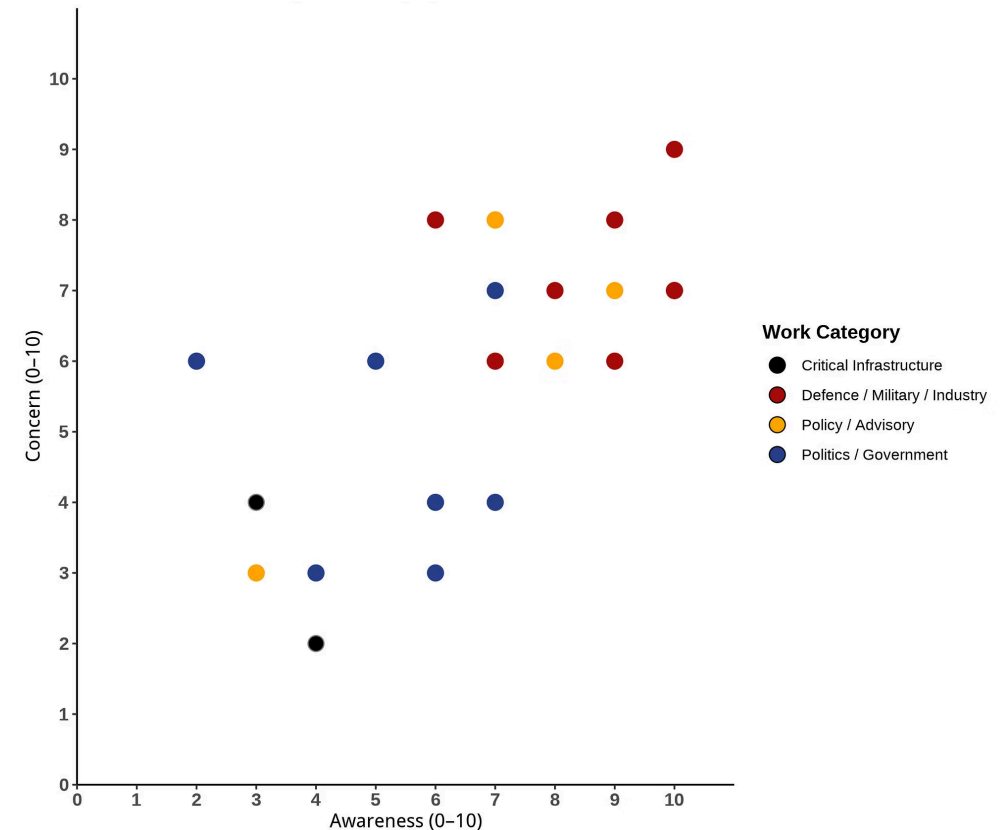
Cluster in the top-right quadrant (awareness 6–10, concern 6–9), consistently the most informed and most alarmed stakeholder group.

2 Politics/Government: Low Awareness, Inconsistent Concern

Politicians cluster in the lower-left to mid-range (awareness 2–7, concern 2–7), confirming that political salience remains structurally insufficient.

3 Critical Infrastructure: The Blindspot Persists

CNI operators remain low on both axes (awareness 2–5, concern 4–6), reinforcing the gap between those at greatest risk and those least prepared.



Awareness vs Government Approval (UK/EU) by Work Category

- **Defence Primes: Aware and Unimpressed**

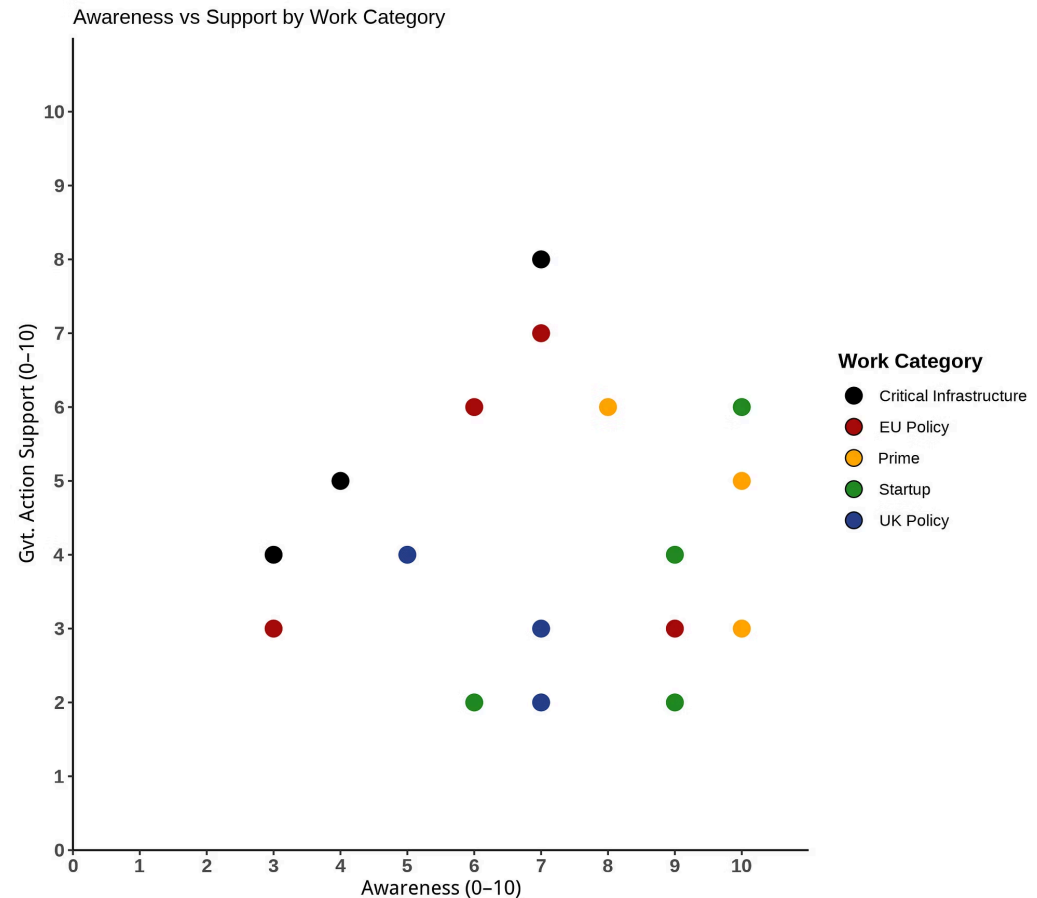
High awareness (8–10), low approval (3–5). Reflecting direct operational knowledge that current government responses are inadequate.

- **Startups: Frustrated by Inaction**

High awareness, widely scattered approval (2–6). Driven by first-hand experience of regulatory barriers blocking solutions or projects.

- **Policy Advisors: Lower Awareness, Lower Scrutiny**

Lower awareness and low-to-moderate approval (2–4).



Stakeholder Perceptions

Interviews across defence, industry, CNI, and politics revealed consistent themes of frustration, confusion, and urgency.

"Rules of engagement are the primary issue — there is no ownership of responsibility."

"Jammers are becoming obsolete and unlikely to succeed in real-world incidents."

"It is political difficult to tackle this topic over hospitals, schools and other funding concerns."

Authority Vacuum

Multiple departments assume others are in charge, reinforcing a "vacuum of responsibility."

Readiness Gap

Failures stem from both RoE gaps and slow technological iteration.

Political Caution

Liability, low public visibility and competing political concerns.

From Insight to Action

Stakeholder Insights

"Over-regulation costs more than innovation." —
Witold Strzelecki, BSP

"No adequate (UK) air defence for 20 years." —
Defence Director

"Supply chain reliance is a major gap." —
European Parliament Advisor

Strategic Imperatives

01

Align Authority with Capability

02

Reduce Supply Chain Exposure

03

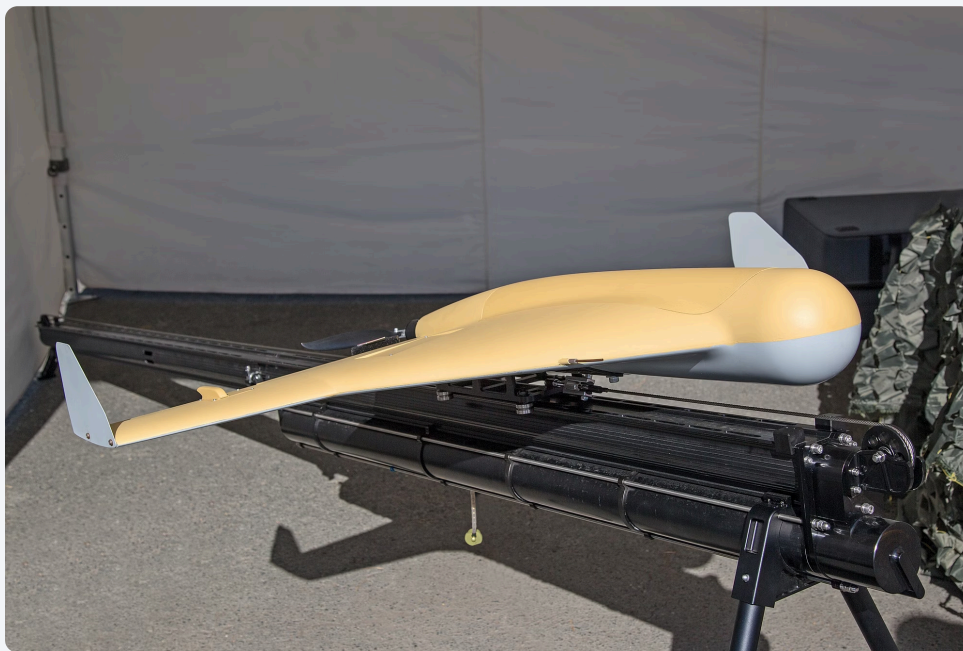
Reform Procurement for Iteration

04

Raise Saliency Before Crisis

PART 5

Implications for Industry



Improved (as of 2024) KUB-BLA loitering munition equipped with a more powerful warhead

Key Concerns

1

Innovation Constrained

Lack of accessible testing spaces. Compliance costs frequently exceed R&D investment for smaller firms.

2

Funding Architecture

"You need an entire team just to handle the regulations." — EU Industry Professional

3

Competitive Erosion

Fragmented testing architecture and slow iteration cycles further erode competitiveness versus peers.

4

Delivery Confidence

"If you build a start-up here, you're probably looking for an early opportunity to move it to the Middle East or the US." — Reform candidate



24-Month Forward Scenarios (Best Case)

1 Airport Paralysis

Detection occurs but few airports empowered to jam or neutralise. Detection to disruption is less than 5 minutes. Runways close. Economic disruption reaches millions per hour.

2 Critical Infrastructure Exposure

Sustained, persistent probing of energy, ports and data infrastructure.

3 Erosion of Competitiveness

Relative lag in European counter-UAS capability as adversaries iterate faster. Regulations prevent C-UAS testing. The technology gap widens. Sovereign capability falls further behind.

None require open conflict. The consequences are no less severe.

Supply Chain Dependence: A Second Layer of Risk



- China dominates commercial drone manufacturing.
- China also controls **critical upstream components embedded within European counter-UAS systems.**
- Final assembly in Europe creates the appearance of resilience. Upstream concentration preserves correlated failure risk.
- C-UAS systems are therefore exposed not at integration level, but at **component depth.**

90%+

Rare earth magnet processing controlled by China
(Core to motors and radar subsystems)

70-80%

Estimated share of global commercial drone component manufacturing concentrated in China

What Industry Should Be Asking

01

Capability

Does our current counter-UAS capability address autonomous, non-RF, and swarm threats — or only RF-dependent platforms?

03

Procurement (Start-ups)

Are our acquisition cycles aligned with the iteration speed of the threat — or are we optimising for platform longevity in a software-defined environment?

02

Supply Chain

What proportion of our critical components originate from strategically exposed sources, and what is our plan to reduce that dependency?

04

Crisis Readiness (Primes)

If a high-visibility incident occurs tomorrow, in what position are primes ready to ramp up production capabilities?

PART 6

Conclusion

A Structured Anticipation approach for policymakers.

A Three-Pillar Policy Response



Collaborative Measures

- Shared airspace monitoring platforms
- Joint attribution mechanisms for cross-border intelligence sharing
- More designated sites for C-UAS/UAS testing



Rules of Engagement

- Harmonise neutralisation thresholds
- Include civil aviation authorities in decision-making
- Allow more authorisation for C-UAS interception (including CNI operators)



Institutional Reform

- Update standards for hostile UAS
- Adopt a harmonised counter-UAS directive
- Expand education and awareness on C-UAS across key stakeholders in policy and business sectors

The Strategic Choice

Amid escalating hybrid threats, drones have become a defining feature of Europe's security environment, with UAS evolving faster than governance.

"we regulate every seven years; this problem is changing by the month." Defence Expert.

1

Ad Hoc (Default Trajectory)

Fragmented regulatory adjustment. Episodic, reactionary funding increases.

2

Structured Anticipation (Required Response)

Align regulatory tempo with technological development.
Clarify authority. Reduce supply chain dependency.
Embed counter-UAS resilience into infrastructure planning.

PART 7

Q&A



1

Strategic Advisory Retainers

Multidisciplinary advisory service, providing monthly horizon scans, supply chain monitoring, and real-time strategic counsel.

2

Integrated Risk Intelligence

Deep dive research encompassing our OSINT, geopolitical and regulatory capabilities.

3

Policy Roundtables & Executive Briefings

Expert-convened discussions, bringing together policymakers, industry leaders, and researchers.

4

Specialist OSINT Investigations

Targeted investigations using satellite imagery, trade data, procurement records, and network analysis.

For enquiries contact: edward@challengerresearchgroup.com or visit: challengerresearchgroup.com