

Can Europe Stop Drones Before Its Politics Gets in the Way?

A coordinated drone campaign has exposed the weak seam in European security. The hard question is no longer whether Europe needs better defences. It is whether the politics around those defences can move fast enough to matter.

EXECUTIVE TAKEAWAYS

- Russia's drone campaign over Europe has moved from nuisance-level airspace violations toward attributed attacks on European soil. Leipzig/Halle matters because it was not just another sighting; it was a military-grade device near a cargo node directly relevant to Ukraine.
- The Commission's own plan acknowledges that Europe's legal framework is fragmented. Civilian and critical-infrastructure operators can lack authority to neutralise a threatening drone, while the binding EU counter-drone framework is still years away.
- Von der Leyen's proposed Emergency Security Protocol would create a mandatory political trigger for hybrid incidents below the armed-attack threshold. That is useful, but it still leaves the harder question unanswered: what are the 27 actually prepared to do once they meet?
- The core vulnerability is decision-making. A mechanism that requires unanimity can be slowed by the same attribution disputes, veto politics, and Russian pressure that already shape EU policy on Moscow.
- The result is a genuine but incomplete step. Europe may be creating a forum before it has created the authority, rules of engagement, and shared operating picture needed to respond at drone speed.

1. THE SITUATION

The week before von der Leyen's State of the Union address provided its own case for action.

On 14 September 2026, a Russian frigate fired two flares at a Danish military helicopter conducting routine Baltic Sea surveillance. Denmark summoned the Russian ambassador and called the action "reckless." The following morning, NATO jets intercepted and shot down an explosive-laden drone that entered Lithuanian airspace from Belarus, roughly five kilometres from a hydroelectric power plant. ^{1; 2}

The following day in Strasbourg, von der Leyen cited the incidents in Denmark, Lithuania, and Poland and called for "Europe's own Article 4, or an Emergency Security Protocol." Any member state could trigger an automatic meeting of all 27 to coordinate a response to incidents below the armed-aggression threshold. She also proposed a European Security Council including Britain, Canada, Norway, and Ukraine. ^{3; 4}

Von der Leyen specifically named the Leipzig/Halle Airport attack as an example of what demanded this response, describing it as an attack using military-grade material by Russian operatives on European soil. ³ Leipzig/Halle is operationally significant: it has served as the base for Ukraine's Antonov Airlines since Russia destroyed its home base at Hostomel, and it handles NATO ally arms transport to Ukraine. ⁵

On 1 September 2026, German Interior Minister Alexander Dobrindt formally blamed Russia for the attempted Leipzig attack, citing police investigations, the pattern of the act, and intelligence findings. A US defence official separately assessed that the device bore hallmarks of GRU-linked construction. Germany closed Russia's Bonn consulate and terminated leases for the Russian House for Science and Culture in Berlin; Russia denied responsibility. ^{6; 5; 7}

Leipzig was not an isolated incident. The International Institute for Strategic Studies (IISS) documented 144 suspected drone sightings across Europe between August 2024 and February 2026, spanning a dozen NATO member states and Ireland, peaking in late 2025. The institute assessed it "highly likely" the Kremlin conducted a coordinated drone campaign. It also judged Russian-linked vessels and the shadow fleet to be likely launch and recovery platforms. ⁸ Germany alone recorded more than 1,000 suspicious drone sightings in 2025, including over defence facilities where Ukrainian soldiers were training. ⁹

In September 2025, approximately 20 Russian military drones crossed into Polish airspace, prompting Poland to invoke NATO Article 4, one of only eight invocations in the alliance's history. NATO launched Operation Eastern Sentry in response, scrambling F-16s, F-35s, Patriots, and Italian surveillance assets. ^{10; 11}

Institutionally, the Commission had already published its Action Plan on Drone and Counter-Drone Security. It proposes prevention, detection, response, and defence measures; 250 million euros for border surveillance; National Drone Security Coordinators; and a binding EU counter-drone regulatory framework by 2030. Germany moved faster at national level, granting the Bundeswehr authority to intercept, jam, and shoot down drones over German territory and committing more than 100 million euros in counter-drone spending. ^{12; 13}

2. WHY IT MATTERS NOW

The institutional response and the threat are not running at the same speed. That gap now carries operational cost.

Challenger Research, writing in the Australian Strategic Policy Institute (*ASPI*) Strategist, put a hard number on the gap: at a European airport, the window between drone detection and disruption is under five minutes. Many airports have neither the legal authority to act inside that window nor a chain of command fast enough to reach someone who does. Belgium reportedly had a certified counter-drone police unit during airport shutdowns but requested NATO ally support instead.^{14, 15}

That five-minute window is not a future concern. Drone-related disruptions at European airports more than tripled between January 2024 and November 2025.¹⁴ The incident at Leipzig was not an airport closure but an armed device adjacent to a NATO-critical cargo platform.⁵ The threat level jumped; the legal authority to respond did not.

The IISS framed the strategic logic clearly. Europe's air-defence architecture "was designed to detect and defeat conventional air threats operating in a recognisable battlespace" and "was not built for relatively low-cost drones and deniable incursions." The Kremlin's campaign had, in the IISS's assessment, achieved "substantial impunity across European airspace", making the campaign "a series of tactical successes for the Kremlin and a strategic failure of allied air defence."¹⁶

The timing matters beyond the speech. The EU's CER Directive required member states to designate critical entities across eleven sectors by 17 July 2026, giving those entities a short window to assess and mitigate risks. If the Emergency Security Protocol becomes law, it will sit above that process. The design choice is whether it gives those entities a decision layer, or merely another consultation layer.¹⁷

The upper bound is not theoretical. The IISS record includes drones reaching nuclear-sharing sites hosting American B61-12 gravity bombs and France's ballistic-missile submarine base at Île Longue.¹⁸ The live policy question is whether Europe's proposed governance response can match the tempo of the next incident.

3. THE BIGGER PICTURE

Europe's drone governance problem has two distinct layers, and the proposed Emergency Security Protocol addresses only one of them cleanly.³

The first layer is the sub-threshold hybrid threat: drones used to test air defences, gather intelligence, probe infrastructure, and impose political cost without clearly crossing the armed-aggression threshold. Leipzig, the nuclear-site overflights, and the suspected shadow-fleet launch platforms all sit in this space. The European Council on Foreign Relations (*ECFR*) describes a dual problem: small drones disrupting civilian infrastructure, often with deniable origin, and larger military drones crossing from Russia or Belarus into EU and NATO territory, with known origin but contested attribution.¹⁰ The hybrid campaign, in this reading, is not just a military problem; it is a governance exploit.

The exploit works because the EU's legal architecture was not built for this threat type. The Commission's Action Plan states explicitly that counter-drone frameworks "remain highly fragmented across the Union," with most member states operating across dispersed provisions in aviation, police, defence, and telecommunications law, and some having no national counter-drone rules at all. Civilian and critical infrastructure operators "typically lack legal authority to neutralise a threatening drone."¹² The IISS sharpened the point: "as long as rules of engagement remain fragmented across national jurisdictions, the Kremlin will continue to exploit them. No amount of hardware will compensate for the absence of political authority to use it."¹⁶

The second layer is institutional coordination. *ECFR* warns that Europe's eastern-flank defence is becoming a "hotch-potch of NATO, EU and national projects," risking duplication and weakening the common operating picture.¹⁰ NATO is currently the more operational actor: it scrambled assets under Article 4, ran Operation Eastern Sentry, and executed the Lithuanian intercept through Baltic Air Policing. The EU's tools remain mainly regulatory and planning instruments. Some member states, according to the European Parliament Research Service, still argue that major defence initiatives should remain national or NATO-led rather than Commission-led.¹⁹

The Emergency Security Protocol sits between those two layers. It would create a mandatory forum for sub-threshold incidents that currently produce fragmented national responses.⁴ But it does not settle who can fire, jam, or neutralise a drone, in which airspace, under whose command, and under what rules. Those questions remain national until 2030 at the earliest.¹²

The EU's existing mutual-assistance clause adds another complication. Article 42.7 has been invoked only once, after the 2015 Paris attacks, and assistance was delivered bilaterally because the EU has no integrated military command.^{3, 20} The April 2026 Nicosia summit asked for an operational blueprint covering hybrid cases. By the September speech, no blueprint or delivery date had appeared publicly, and the speech itself did not mention Article 42.7.²¹

That leaves a structural ambiguity. The Emergency Security Protocol is presented as the missing layer below Article 42.7, yet the public proposal does not explain how a sub-threshold consultation would escalate, which instrument would govern the transition, or who decides when the threshold has been crossed.^{3, 21}

4. NEXUS THREAD

The simple story is that Europe has recognised the drone threat and is building collective security capacity. Von der Leyen's proposal shows political will; Leipzig and Lithuania show urgency; the Action Plan supplies the regulatory track. That story is partly true. It is also too clean.

The Emergency Security Protocol creates political authority to call a meeting. It does not create political authority to act.

That gives the proposal three practical tests. First, can it create a shared incident picture quickly enough for governments to agree on what happened before the information environment is polluted? Second, can it connect political consultation to operational permissions for police, military, aviation, and infrastructure authorities? Third, can it produce consequences for the attacker that are fast enough to change incentives? Without those links, the protocol risks becoming a signalling device: useful for showing seriousness, weaker as a tool for stopping the next probe.

That distinction matters because the bottleneck is not awareness. IISS identifies fragmented rules of engagement, a cost-exchange ratio that favours the attacker, and weak maritime accountability for Russia-linked vessels.¹⁶ A meeting of 27 governments does not by itself harmonise law, buy cheaper interceptors, or police launch platforms at sea.

The unanimity rule deepens the problem. The proposed protocol would be governed by the same decision rule that has previously paralysed EU action on Russia, the rule under which Russia sanctions decisions have been blocked or delayed.²² A protocol that requires all 27 governments to agree on both the threat and the response before anything happens is, in structural terms, more vulnerable to that exploit than a mechanism that sets a lower decision threshold.

The hybrid campaign is calibrated for exactly that weakness. Deniable attacks stay below the level where mandatory collective response clearly begins. According to Alto Intelligence's study, they are often followed by online activity that confuses attribution, spreads blame across several actors, and weakens trust in authorities.²³ If the response mechanism needs unanimity on attribution, the information operation is already inside the decision loop.

There is a serious counter-reading: defenders of the proposal can argue that sub-threshold hybrid incidents currently produce no mandatory EU-level trigger at all.⁴ Even a constrained consultation mechanism may be better than 27 governments processing the same Russian probing campaign separately. NATO Article 4 also began as consultation; its weight came from use, habit, and precedent.

That counter-reading works only if convening produces shared assessment and coordinated action. The evidence is mixed. The Nicosia blueprint for Article 42.7 had not appeared publicly by September.²¹ The binding counter-drone framework is years away.²² Belgium reportedly had a counter-drone unit but did not deploy it.¹⁵ The pattern is not only institutional indecision; it is institutional deferral.

The protocol therefore makes the gap visible more than it fills it. That still matters. A mandatory forum creates accountability pressure that scattered national handling does not. But the clean narrative, "Europe is building collective security capacity", needs one important correction: a convening is not a capability.

5. NEXUS CALCULATION

A four-year gap between commitment and binding rules

Policy Marker	Date
EU counter-drone Action Plan published	February 2026
Binding EU counter-drone regulatory framework target	2030
Governance gap, Action Plan to binding rules	4 years

A four-year governance gap separates Europe's first coordinated counter-drone political commitment from the earliest date a binding EU legal framework could exist. This gap is confirmed in the Commission's own Action Plan.

During those four years, the incident rate is not static. **Drone-related airport disruptions more than tripled from January 2024 to November 2025.**¹⁴ The point is simple: the policy timetable runs to 2030, while the disruption trend was already accelerating before that timetable began.¹²

SOURCES

1 Radio Free Europe / Radio Liberty — RFERL, Explosive-Laden Drone Shot Down Over Lithuania — 15 September 2026

Source



2	Bloomberg — NATO Shoots Down Drone That Entered Lithuanian Airspace — 15 September 2026	Source
3	Breaking Defense — EU chief calls for new hybrid response protocol, increased defense ties to non-members — 16 September 2026	Source
4	Associated Press (via KSAT) — KSAT / AP wire, EU chief von der Leyen calls for EU security mechanism to respond to drone incidents and sabotage — 16 September 2026	Source
5	CNN — Germany blames Russia for drone attack on Leipzig airport — 1 September 2026	Source
6	Defense News — German government blames Russia for Leipzig airport drone attack with explosives — 2 September 2026	Source
7	Al Jazeera — Germany accuses Russia of failed drone attack on Leipzig airport in August — 1 September 2026	Source
8	TVP World — IISS: Russia used shadow fleet in drone campaign on Europe — 2 July 2026	Source
9	ABC News / Associated Press — Russia waged drone campaign over Europe, launched drones from shadow fleet — 2 July 2026	Source
10	European Council on Foreign Relations (ECFR) — ECFR, Buzzkill: How to defend Europe against drones — 18 August 2026	Source
11	Gulf News — Why drones over Poland have put Europe on edge (<i>accessed 23 September 2026</i>)	Source
12	European Commission — Action Plan on Drone and Counter-Drone Security — 11 February 2026	Source
13	DroneXL — Germany shoot down Russian drone threat — 1 March 2026	Source
14	Australian Strategic Policy Institute (The Strategist) — Challenger Research / ASPI Strategist, Who has authority to deal with drones? In most of Europe, that's unclear — 25 May 2026	Source
15	Inside Unmanned Systems — Europe must upgrade its counter-drone strategy now (<i>accessed 23 September 2026</i>)	Source
16	Unmanned Airspace — IISS report: Russia likely conducted a drone campaign against Europe using its shadow fleet (<i>accessed 23 September 2026</i>)	Source
17	Aerotime Hub — Drone threat to Europe's infrastructure is surging — 25 May 2026	Source
18	International Institute for Strategic Studies (IISS) — International Institute for Strategic Studies, Russia's UAV Campaign Over Europe (<i>accessed 23 September 2026</i>)	Source
19	European Parliament Research Service — Drones and new systems of warfare: Adapting the EU (<i>accessed 23 September 2026</i>)	Source
20	Al Jazeera — Can the EU's Article 42.7 offer Europe NATO-like collective defence? — 30 April 2026	Source
21	Grosswald.org (independent policy analysis) — Grosswald.org, Von der Leyen Proposes a European Article 4, a European Security Council and a Strategic Enablers Instrument — 16 September 2026	Source
22	TechTimes — EU Counter-Hybrid Playbook Debuts; Same Veto That Froze Russia Sanctions Governs It — 17 September 2026	Source
23	European Council on Foreign Relations (ECFR) — ECFR, From shield to sword: Europe's offensive strategy for the hybrid age (<i>accessed 23 September 2026</i>)	Source

FOR FURTHER READING

Selected reading for further context.

Primary documents and official texts

European Commission — DG Defence Industry and Space, Commission publishes the Action Plan on Drone and Counter-Drone Security — 11 February 2026 → Retrieved. Summarises co-ownership principle; proposes €250 million counter-drone border initiative; National Coordinator mechanism.	Read
European Commission — Drone security policy page (<i>accessed 23 September 2026</i>) → Consulted background page for drone security policy and related Action Plan material.	Read

Analysis and commentary

UAV-Defence — The EU Counter-UAS Action Plan explained for security buyers — 1 June 2026 → Consulted background analysis of the EU Counter-UAS Action Plan and 2030 regulatory target.	Read
--	------

Bird & Bird — European Commission Counter-UAS Action Plan — 25 March 2026 → Retrieved. Legal analysis of COM(2026) 81; quotes Commission's own acknowledgement of fragmentation; notes Action Plan is political message not regulation; questions telecoms-operator enforcement role.	Read
---	------

Reporting

ABJ Drone Academy — Europe Is Tightening Drone Identification Rules — 21 September 2026 → Retrieved. Reports EASA September 2026 NPA security opinion; Germany's formal attribution of Leipzig/Halle (4 August) to Russia; Germany raised national threat assessment.	Read
France24 — NATO fighter jets shoot down drone over Lithuania after latest incursion — 15 September 2026 → Consulted as supporting reporting on the Lithuanian drone intercept; not used as a cited public reference in the final text.	Read

