DETAILED REPORTS

NATO’s Drone Airspace Crisis: How the Ukraine War Is Testing Europe’s Air Defences

Author: CNAWS Research Team • **Published:** August 16, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Europe’s eastern flank is no longer dealing with occasional drone spillover from the Russia-Ukraine war. Repeated incursions over Romania, Poland and the Baltic states are exposing a more difficult problem: NATO must defend its airspace against cheap, ambiguous and increasingly frequent unmanned threats without knowing immediately whether they are accidental, hostile or deliberately designed to test the Alliance. As fighters are scrambled and drones are shot down over NATO territory, the issue is evolving from border security into a broader challenge of attribution, escalation control and the future economics of European air defence.

A Spanish F-18 operating under NATO air policing shot down an unidentified drone over Romania in the early hours of 16 August 2026 after the aircraft entered Romanian airspace from the direction of Moldova. Romanian authorities said the drone was detected approximately 24 kilometres north of Gala?i and that the Spanish pilot established radar contact before receiving permission to engage. The destruction of the aircraft marked the fourth drone shootdown over Romanian territory in 2026 and came after Romanian F-16s had destroyed three Russian drones during a series of incursions in July.[1]

Only two days earlier, an Italian Eurofighter operating under NATO command had shot down another drone over Latvia. Italian aircraft scrambled from Lithuania while Turkish F-16s were launched from Estonia after the unidentified aircraft was detected near Rug?ji, approximately 35 kilometres from Latvia's border with Russia. NATO and Latvian authorities initially refrained from attributing the drone because its wreckage had not yet been recovered, but the incident occurred amid a growing series of Russian and Ukrainian unmanned aircraft entering NATO airspace around the Baltic region.[2]

These incidents are important not simply because NATO fighters are increasingly firing on drones over Alliance territory, but because they illustrate a larger transformation of the European security environment. The Russia-Ukraine war has generated an expanding zone of unmanned activity extending from the Black Sea through Eastern Europe to the Baltic and Finnish frontiers. Russian strike drones have repeatedly violated NATO airspace, while Ukrainian long-range attack drones have also strayed into Allied territory as Kyiv expands strikes against Russian military, energy and port infrastructure. Electronic warfare, navigation errors, contested attribution and fears of deliberate provocation have made it increasingly difficult to distinguish accidental Ukraine war spillover from deliberate grey-zone activity against NATO.

The emerging NATO drone airspace crisis is therefore not simply a problem of intercepting inexpensive unmanned aircraft. It is simultaneously an air-defence, attribution, deterrence and escalation-management challenge. NATO must find a way to detect and defeat drones without routinely expending some of its most sophisticated military assets, while also determining whether each airspace violation represents an accident, a reconnaissance mission, deliberate coercion, a false-flag operation or the beginning of something considerably more serious.

From Drone Debris to NATO Fighter Shootdowns

During the earlier stages of the Russia-Ukraine war, many drone-related incidents inside NATO territory could still be treated as dangerous consequences of fighting close to Alliance borders. Romania repeatedly discovered fragments of Russian drones after attacks on Ukrainian ports along the Danube, while Poland and other eastern NATO members scrambled aircraft when Russian missile and drone operations approached their airspace. These incidents raised diplomatic tensions but did not initially produce systematic kinetic interception.

That approach became progressively harder to sustain as the frequency and seriousness of airspace violations increased. A major turning point came in September 2025, when numerous Russian drones entered Polish airspace during a large attack against Ukraine. Polish and Allied aircraft engaged the incursion, after which NATO launched Eastern Sentry, a military activity designed to strengthen deterrence and air defence along the Alliance's eastern flank. NATO subsequently incorporated conventional air-policing and air-defence assets alongside newer counter-drone technologies under the initiative.[3]

Romania subsequently became one of the clearest examples of the changing threat. Its long border with Ukraine places it immediately beside Russian attacks against Ukrainian infrastructure around Odesa and the Danube ports, and the Romanian Defence Ministry said in July 2026 that Russian drones had entered national airspace without permission 33 times since the beginning of the full-scale war. For years Romania had generally scrambled aircraft and recovered debris rather than destroying the intruding systems, but the increasing proximity of Russian attacks gradually made that posture untenable.[4]

The consequences became particularly visible on 29 May 2026 when Romania said a Russian drone entered its territory during an attack on neighbouring Ukraine and struck an apartment building in Gala?i. A woman and a child suffered minor injuries, residents were evacuated and property was damaged. Romanian F-16s had been scrambled, but the low-flying drone remained difficult to intercept, underlining a problem that conventional European air-defence networks increasingly face when dealing with small aircraft operating at low altitude.[5]

Romania’s operational threshold changed decisively in July. Between 24 and 26 July, Romanian F-16 pilots shot down three drones during separate airspace violations, with the government identifying at least one as a Russian Shahed-type system. President Nicu?or Dan described the continued breaches as unacceptable and emphasised that Romanian airspace was simultaneously NATO and European Union airspace.[6] The Spanish F-18 engagement on 16 August therefore needs to be understood as part of this broader transition. Defence of Romanian airspace against drones has moved beyond a purely national mission and increasingly forms part of NATO’s collective air-policing and air-defence posture.

The Ukraine War’s Drone Spillover Has Reached the Baltic

The Baltic airspace problem is even more complicated because the unmanned aircraft crossing NATO borders have not exclusively been Russian. Ukraine’s expanding long-range drone campaign against Russian ports, military installations and energy infrastructure around the Baltic Sea has brought Ukrainian weapons increasingly close to Finland, Estonia, Latvia and Lithuania. Several aircraft have subsequently entered NATO territory, creating situations in which Allied fighters have had to respond to drones belonging to a country NATO is simultaneously supporting against Russian aggression.

In March 2026, Ukrainian military drones entered Estonia and Latvia after travelling through Russian territory. One struck a chimney at Estonia’s Auvere power station, while another crashed in Latvia. Finland subsequently reported suspected UAV violations and deployed fighters, while Lithuanian authorities experienced their own airspace alerts. In May, a Romanian F-16 operating under NATO command shot down a suspected Ukrainian drone over Estonia, and a French Rafale later destroyed another drone over Latvia in June.[7]

Baltic governments and Ukrainian officials have argued that Russian electronic warfare may contribute to some of these deviations by interfering with the navigation of Ukrainian aircraft attacking targets inside Russia. Latvian military officials again raised this explanation after the 14 August 2026 incident, although evidence establishing the precise mechanism behind every individual incursion has not always been publicly available. This distinction is important because attribution cannot simply be inferred from the direction from which a drone approaches NATO territory.[8]

The result is an increasingly difficult operational environment. Treating every unidentified aircraft as Russian risks misattribution and potentially unnecessary escalation, while treating repeated airspace violations as accidental creates opportunities for hostile actors to exploit ambiguity. The eastern flank is consequently experiencing an attribution crisis alongside the physical air-defence challenge, and that attribution problem may prove strategically more difficult than the mechanical task of destroying the drones themselves.

When Does Drone Spillover Become Grey-Zone Warfare?

The strategic effects of a drone incursion do not depend solely on whether the aircraft successfully strikes a target. Repeated penetrations can force NATO fighters to scramble, activate ground-based sensors, expose response times, disrupt civil aviation, generate public warnings and consume military readiness. They may also reveal information about radar coverage, interception procedures and the geographical limitations of national air-defence networks.

It would be analytically unsound to conclude that every drone entering NATO territory represents a deliberate Russian attempt to gather such intelligence. The circumstances surrounding individual incidents vary considerably, and NATO governments themselves have frequently avoided assigning intent until investigations are complete. Nevertheless, the potential for an adversary to deliberately exploit Europe’s increasingly congested and ambiguous drone environment is becoming harder to dismiss.

Lithuanian Defence Minister Robertas Kaunas said in August 2026 that Lithuanian intelligence believed Russia could potentially use captured Ukrainian-made drones in provocations against Baltic countries. Such an operation could generate a particularly difficult attribution problem because the platform and technical components recovered after an attack might initially point towards Ukraine rather than Russia. Lithuania, Poland, Latvia and Estonia have therefore increased security around critical infrastructure amid wider intelligence concerns about potential sabotage or staged attacks.[9]

Reuters reported that regional officials were particularly concerned about the political consequences of such an operation. One Baltic intelligence assessment cited in the reporting suggested that a false-flag incident could be intended less to produce major physical destruction than to create confusion inside NATO over responsibility and the appropriate response. Russia has rejected Western warnings of planned covert attacks and characterised such allegations as attempts to justify increased militarisation near its borders.[10]

This environment makes unmanned systems especially useful for grey-zone warfare against NATO. Commercially available components, contested electronic environments, cross-border flight paths and the difficulty of recovering wreckage can delay attribution. A captured Ukrainian system could theoretically produce misleading forensic evidence, while genuine Ukrainian drones straying across NATO territory provide ready-made material for competing narratives. The central strategic problem is therefore ambiguity: the same physical event can plausibly represent an accident, technical malfunction, electronic interference, intelligence collection, deliberate provocation or hostile attack.

NATO’s Article 5 Challenge Is Closely Tied to Attribution

A drone crossing NATO airspace does not automatically constitute an Article 5 event. The North Atlantic Treaty applies collective defence when an Ally suffers an armed attack, and NATO retains political discretion over the form of assistance provided by individual members. The Alliance has also made clear in the wider context of hybrid threats that hostile actions below the threshold of conventional military attack can, in sufficiently serious circumstances, contribute to a decision to invoke Article 5.[11]

Drones make this threshold considerably harder to interpret because similar platforms can produce very different strategic situations. A Ukrainian strike drone that loses navigation and enters Latvia before crashing is not strategically equivalent to a Russian reconnaissance UAV deliberately penetrating Latvian airspace to test radar coverage. Neither is equivalent to a swarm directed against a NATO airbase or a captured Ukrainian drone deliberately used in a false-flag operation against civilian infrastructure.

The tactical response in each scenario may nevertheless appear similar: detect the aircraft, track it and, if necessary, destroy it. The strategic response is entirely different because intention, provenance and operational context determine whether the event should be treated as an accident, a sovereignty violation, a hostile intelligence operation or an armed attack. This is why NATO counter-drone defence cannot be separated from intelligence fusion and forensic attribution. Destroying the aircraft resolves the immediate physical threat, but identifying its launch point, operator, mission and relationship to wider military activity determines the political and military response that follows.

The Fighter-versus-Drone Cost Problem

NATO currently possesses some of the most sophisticated combat aircraft in the world, and fighters such as the F-16, F-18, Rafale and Eurofighter remain extremely capable instruments for air policing. They can rapidly reach an unidentified contact, visually inspect it and destroy it when necessary. The Romanian and Latvian incidents demonstrate how multinational NATO air-policing deployments can also provide smaller eastern-flank members with immediate access to advanced capabilities operated by other Allies.

However, using high-performance combat aircraft as the routine answer to inexpensive unmanned systems is difficult to sustain if the number of incursions continues to rise. The problem extends beyond comparing the purchase price of a drone with the cost of an air-to-air missile. Fighter operations consume fuel, maintenance hours, aircrew availability, ground support and finite sortie-generation capacity. Every scramble also represents readiness that cannot simultaneously be allocated elsewhere.

The distinction between isolated incursions and mass becomes crucial. A few unidentified drones can be treated as an air-policing problem, but repeated waves of dozens or hundreds would become a capacity and economic problem for Europe's integrated air and missile defence system. The experience of Ukraine has demonstrated that a defender can achieve technically successful interceptions and still lose the economic exchange if cheap attackers consistently force the expenditure of much more expensive interceptors.

NATO's response increasingly reflects this lesson. Eastern Sentry incorporates technologies specifically intended to address unmanned threats, while countries such as Poland and Romania have begun deploying specialised interceptor-drone systems alongside conventional fighter aircraft and surface-to-air defence. Romania tested the American-developed Merops counter-UAS system in April 2026 as part of a broader NATO effort involving interceptor drones, radars, sensors and jamming equipment. Merops was already operating in Ukraine and Poland and was subsequently incorporated into Romanian air defence.[12]

The significance of systems such as Merops lies less in any one particular technology than in the economics of defence. Europe requires weapons capable of defeating relatively cheap drones without consuming its most sophisticated missile inventories on every engagement. Interceptor drones, electronic warfare, guns and specialised short-range counter-UAS systems can therefore occupy the space between passive monitoring and the use of high-end fighters or surface-to-air missiles.

NATO Is Building a Layered Counter-Drone Architecture

The Alliance has already begun institutionalising these lessons through the Layered Counter-UAS Initiative-X, or LCI-X. Romania hosted the first major LCI-X experimentation event in April 2026, bringing together approximately 500 personnel and around 215 technical systems at the Capu Midia training range. Finland hosted the second event in June, where NATO focused on connecting individual counter-UAS cells into a scalable network or "mosaic" that could eventually operate through common command-and-control structures.[13]

The emerging architecture is deliberately layered because no single sensor or weapon can reliably deal with the entire drone threat. Small unmanned aircraft may require combinations of radar, electro-optical sensors, passive radio-frequency detection and intelligence feeds before they can even be identified. Electronic warfare may be sufficient against some remotely controlled systems, whereas autonomous or hardened aircraft may require kinetic destruction. Guns and interceptor drones can address lower-cost threats, while conventional surface-to-air missiles and fighter aircraft remain necessary against larger UAVs, cruise missiles and sophisticated combined attacks.

Command and control binds these layers together. A future NATO counter-drone network must allow information collected by one Ally's sensor to support an engagement by another country's aircraft or ground-based interceptor, potentially after the target has crossed national boundaries. The Latvia incident on 14 August demonstrated this multinational character in miniature: Italian Eurofighters based in Lithuania and Turkish F-16s based in Estonia responded to a threat inside Latvian airspace under NATO command.[14]

For this reason, Europe's air-defence problem cannot be solved simply by purchasing additional weapons. NATO requires a shared low-altitude air picture, interoperable rules of engagement, common identification procedures and

sufficiently rapid information exchange to allow multiple national forces to operate as parts of the same counter-UAS architecture.

Towards a Baltic-to-Black Sea Counter-UAS Belt

The European Union is developing a parallel framework. In February 2026, the European Commission published its Action Plan on Drone and Counter-Drone Security, calling for greater technological development, industrial production, interoperability and coordination against malicious unmanned systems. The plan complements broader European defence projects including the European Drone Defence Initiative and Eastern Flank Watch.[15]

The geographical logic behind these programmes is becoming increasingly compelling. NATO's exposed eastern frontier extends from Finland and the Baltic states through Poland and Central Europe to Romania and the Black Sea. Drone activity generated by the Russia-Ukraine war now affects several points along this arc, which means individual national defensive bubbles around Vilnius, Warsaw, Bucharest or Riga are unlikely to provide an adequate long-term solution.

What Europe increasingly requires is a Baltic-to-Black Sea counter-UAS belt built from overlapping rather than isolated national systems. Such a network would combine low-altitude radar coverage, passive sensors, electronic intelligence, air policing, electronic warfare and relatively inexpensive kinetic interceptors. Mobile assets would protect critical infrastructure and reinforce sectors experiencing heightened activity, while common command-and-control standards would allow threats to be tracked as they cross national borders.

This does not necessarily mean constructing a literal continuous "drone wall." Geography, terrain, civilian aviation and the enormous length of NATO's eastern frontier make such imagery misleading. The more practical objective is a federated network whose individual components can share data and reinforce one another rapidly enough that a drone crossing one national boundary does not disappear from the wider Alliance air picture.

Romania Demonstrates Why Law Matters as Much as Technology

Europe's counter-drone challenge also has a legal dimension. Before 2025, Romania did not possess a sufficiently clear peacetime framework for dealing with unauthorised drones entering national airspace. Romanian lawmakers subsequently adopted legislation allowing illegal UAVs to be neutralised, brought under control or destroyed depending on their assessed threat, while treating destruction as a last resort. The framework also allows Allied military systems deployed in Romania to participate under relevant collective-defence arrangements.[16]

This legal evolution is directly relevant to the August 2026 incident because the aircraft that destroyed the drone was Spanish rather than Romanian. As NATO counter-UAS operations become increasingly multinational, similar questions will emerge elsewhere concerning national sovereignty and delegated engagement authority. Governments will need clear procedures governing when foreign Allied fighters may fire inside national airspace, when electronic warfare may be employed and how counter-drone systems can operate near civilian airports, towns and critical infrastructure.

These questions cannot be resolved after a crisis has already begun. Small unmanned aircraft compress warning and decision times, meaning that legal authority, operational procedures and tactical rules of engagement must be established before an unidentified drone appears on radar.

The Greater Strategic Danger Is Normalisation

Perhaps the most serious long-term risk is not a spectacular drone attack against NATO territory but the gradual normalisation of repeated incursions. Once unidentified drones crossing Allied borders become routine, governments

face a difficult balance between operational fatigue and deterrence. Scrambling fighters for every contact consumes resources and disrupts operations, but ignoring lower-level violations may unintentionally signal that limited penetrations will be tolerated.

Grey-zone strategies thrive in exactly this space. Persistent incidents can test NATO's response thresholds without presenting the kind of unequivocal attack that would immediately generate political consensus across the Alliance. Each violation may appear too small to justify a major response, yet the cumulative effect can degrade confidence, impose costs and gradually alter expectations about what constitutes normal behaviour along NATO's borders.

A credible response therefore does not require treating every drone as the opening stage of a Russian attack. Instead, NATO needs to demonstrate that unidentified aircraft can be detected, followed, intercepted and attributed without forcing policymakers into a binary choice between passivity and major escalation. Effective counter-drone defence is, in this sense, also a form of deterrence: the ability to defeat low-level incursions cheaply and routinely reduces their value as tools of coercion or intelligence collection.

What NATO Needs Next

The first requirement is persistent low-altitude surveillance across the eastern flank. Traditional NATO air-defence systems remain highly capable against aircraft, missiles and larger aerial threats, but small UAVs flying close to terrain present different detection problems. The Gala?i incident in May illustrated this vulnerability when the incoming drone flew approximately 10 kilometres through Romanian territory at low altitude before striking a building.[17] A wider network of specialised low-altitude radars, electro-optical sensors and passive detection systems will therefore be necessary around likely approach corridors and critical infrastructure.

The second requirement is sufficient numbers of affordable effectors. Fighters, Patriot-class systems and sophisticated surface-to-air missiles cannot disappear from the defence equation, particularly when adversaries can combine drones with cruise and ballistic missiles. Yet they must sit above cheaper layers composed of interceptor drones, electronic warfare systems, guns and other short-range solutions capable of absorbing the numerical burden of unmanned attacks.

The third requirement is faster cross-border attribution and command and control. An aircraft may originate in Ukraine, transit Russian territory, suffer electronic interference and subsequently enter a Baltic NATO member, creating a chain of events that cannot be understood by examining only the final few kilometres of its flight. Radar tracks, electronic signatures, intelligence reporting, recovered components and wider operational activity must therefore be fused across national and organisational boundaries.

Ukraine's battlefield experience provides NATO with an unusually large body of real-world evidence on exactly these problems. The NATO-Ukraine Joint Analysis, Training and Education Centre in Poland is already intended to transfer operational lessons from the war into Allied strategies and capabilities, while NATO's LCI-X programme is using those lessons to test counter-UAS technologies against threat profiles modelled on Russian tactics and equipment.[18]

Conclusion: The Ukraine War Is Already Reshaping NATO Air Defence

The unidentified drone destroyed over Romania on 16 August 2026 may ultimately prove to have been Russian, Ukrainian or of another origin, just as investigations are necessary to establish the provenance of the drone destroyed over Latvia two days earlier. Their unresolved attribution does not reduce their strategic significance. On the contrary, uncertainty about origin demonstrates precisely why the NATO drone airspace crisis is becoming difficult to manage.

Europe’s eastern frontier now borders a battlespace saturated with long-range drones, electronic warfare, deep-strike campaigns and competing intelligence narratives. Russia’s attacks on Ukrainian infrastructure repeatedly bring weapons close to NATO territory, while Ukraine’s expanding campaign against targets deep inside Russia increasingly sends its own drones through a heavily contested electronic environment. At the same time, regional governments are warning that this ambiguity could be deliberately manipulated through hybrid or false-flag operations.

NATO has already shown that it can destroy individual drones. The more demanding challenge is building a European air-defence system capable of handling persistent, ambiguous and potentially massed unmanned threats without exhausting expensive missile inventories, overwhelming fighter fleets or unnecessarily escalating every border violation into a confrontation with Russia. Eastern Sentry, LCI-X, European counter-drone initiatives and the growing deployment of dedicated interceptor systems indicate that the Alliance has begun moving in this direction.

The deeper lesson extends beyond the current Ukraine war. Future air defence will not be defined exclusively by advanced combat aircraft, ballistic missiles and traditional surface-to-air systems. It will increasingly involve thousands of comparatively inexpensive unmanned aircraft operating at low altitude, exploiting civilian technologies and moving through a battlespace saturated with electronic warfare. In that environment, the ability to determine who launched a drone and why it is there may become almost as strategically important as the ability to shoot it down.

For NATO, that transformation has already begun along the eastern flank.

Endnotes

1. Reuters, “Romania Shoots Down Drone Breaching Its Airspace—Defence Ministry,” August 16, 2026, https://www.reuters.com/business/aerospace-defense/romania-shoots-down-drone-breaching-its-airspace-defence-ministry-2026-08-16/; Reuters, “Romania Shoots Down Third Russian Drone, as President Calls Breaches ‘Intolerable,’” July 26, 2026, https://www.reuters.com/business/aerospace-defense/romania-shoots-down-third-russian-drone-president-calls-breaches-intolerable-2026-07-26/.
2. Reuters, “Italian NATO Fighter Jet Shoots Down Drone in Latvian Airspace,” August 14, 2026, https://www.reuters.com/business/aerospace-defense/latvia-shoots-down-drone-its-airspace-finland-restricts-parts-baltic-sea-2026-08-14/.
3. North Atlantic Treaty Organization, “NATO Launches ‘Eastern Sentry’ to Bolster Posture along Eastern Flank,” September 12, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank; Supreme Headquarters Allied Powers Europe, “Eastern Sentry to Enhance NATO’s Presence along Its Eastern Flank,” September 12, 2025, https://shape.nato.int/news-releases/eastern-sentry-to-enhance-natos-presence-along-its-eastern-flank.
4. Reuters, “Romania Shoots Down Third Russian Drone, as President Calls Breaches ‘Intolerable,’” July 26, 2026, https://www.reuters.com/business/aerospace-defense/romania-shoots-down-third-russian-drone-president-calls-breaches-intolerable-2026-07-26/.
5. Reuters, “Romania Says Russian Drone Hit Apartment Block, NATO Vows to Defend Alliance Territory,” May 29, 2026, https://www.reuters.com/world/europe/apartment-building-hit-by-drone-romanias-galati-close-ukraine-border-radio-says-2026-05-29/.
6. Reuters, “Romania Shoots Down Third Russian Drone, as President Calls Breaches ‘Intolerable,’” July 26, 2026, https://www.reuters.com/business/aerospace-defense/romania-shoots-down-third-russian-drone-president-calls-breaches-intolerable-2026-07-26/.
7. Reuters, “Drone Incursions Sow Fear, Chaos along NATO’s Baltic and Finnish Borders,” May 27, 2026, https://www.reuters.com/business/aerospace-defense/drone-incursions-sow-fear-chaos-along-natos-baltic-

finnish-borders-2026-08-14/; Reuters, “Errant Ukrainian Drones Fuel Tensions on NATO’s Eastern Flank,” May 27, 2026, https://www.reuters.com/business/aerospace-defense/errant-ukrainian-drones-fuel-tensions-natos-eastern-flank-2026-05-27/.

8. Reuters, “Italian NATO Fighter Jet Shoots Down Drone in Latvian Airspace,” August 14, 2026, https://www.reuters.com/business/aerospace-defense/latvia-shoots-down-drone-its-airspace-finland-restricts-parts-baltic-sea-2026-08-14/; Reuters, “Lithuanian Lawmakers Shelter, Vilnius Air Traffic Suspended Due to Drone Incursion,” May 20, 2026, https://www.reuters.com/business/aerospace-defense/lithuanias-vilnius-airport-suspends-flights-due-drone-warning-2026-05-20/.
9. Reuters, “Lithuania Says Russia Could Use Ukrainian Drones against Baltic Region,” August 6, 2026, https://www.reuters.com/world/lithuania-says-russia-could-use-ukrainian-drones-against-baltic-region-2026-08-06/; Marek Strzelecki and Andrius Sytas, “Poland and Baltics Shield Infrastructure, Fearing a Russian False-Flag Strike,” Reuters, August 10, 2026, https://www.reuters.com/world/europe/poland-baltics-shield-infrastructure-fearing-russian-false-flag-strike-2026-08-10/.
10. Marek Strzelecki and Andrius Sytas, “Poland and Baltics Shield Infrastructure, Fearing a Russian False-Flag Strike,” Reuters, August 10, 2026, https://www.reuters.com/world/europe/poland-baltics-shield-infrastructure-fearing-russian-false-flag-strike-2026-08-10/.
11. North Atlantic Treaty Organization, “Collective Defence and Article 5,” updated November 12, 2025, https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5; North Atlantic Treaty Organization, “Countering Hybrid Threats,” updated January 29, 2026, https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.
12. Reuters, “Romania Tests AI-Powered Drone Interceptors as Ukraine War Gets Closer,” April 24, 2026, https://www.reuters.com/business/aerospace-defense/romania-tests-ai-powered-drone-interceptors-ukraine-war-gets-closer-2026-04-24/; Reuters, “Romania Says Russian Drone Hit Apartment Block, NATO Vows to Defend Alliance Territory,” May 29, 2026, https://www.reuters.com/world/europe/apartment-building-hit-by-drone-romanias-galati-close-ukraine-border-radio-says-2026-05-29/.
13. NATO Allied Command Transformation, “Layered Counter-UAS Initiative,” 2026, https://www.act.nato.int/activities/lci-x/; NATO Allied Command Transformation, “From Experimentation to Capability: LCI-X Crucible 1-26 in Romania,” April 24, 2026, https://www.act.nato.int/article/lcix-1-26/; NATO Allied Command Transformation, “NATO Advances Counter-UAS Integration Through LCI-X Crucible 2-26,” June 10, 2026, https://www.act.nato.int/article/lci-x-crucible-2/.
14. Reuters, “Italian NATO Fighter Jet Shoots Down Drone in Latvian Airspace,” August 14, 2026, https://www.reuters.com/business/aerospace-defense/latvia-shoots-down-drone-its-airspace-finland-restricts-parts-baltic-sea-2026-08-14/.
15. European Commission, Directorate-General for Defence Industry and Space, “Commission Publishes the Action Plan on Drone and Counter-Drone Security,” February 11, 2026, https://defence-industry-space.ec.europa.eu/commission-publishes-action-plan-drone-and-counter-drone-security-2026-02-11_en; European Commission, “Hybrid Threats,” 2026, https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.
16. Reuters, “Romanian Lawmakers Adopt Law to Shoot Down Drones Breaching Airspace,” February 26, 2025, https://www.reuters.com/world/europe/romanian-lawmakers-adopt-law-shoot-down-drones-breaching-airspace-2025-02-26/.
17. Reuters, “Romania Says Russian Drone Hit Apartment Block, NATO Vows to Defend Alliance Territory,” May 29, 2026, https://www.reuters.com/world/europe/apartment-building-hit-by-drone-romanias-galati-close-ukraine-border-radio-says-2026-05-29/.

18. NATO Allied Command Transformation, “Layered Counter-UAS Initiative,” 2026, https://www.act.nato.int/activities/lci-x/; North Atlantic Treaty Organization, “Relations with Ukraine,” updated July 9, 2026, https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-ukraine.