ZEROFOX INTELLIGENCE

Flash

Drone Sightings Disrupt Airport Operations in Europe

F-2025-09-25a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Geopolitical, Europe and Russia, Airspace

September 25, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 8:00 AM (EDT) on September 25, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Drone Sightings Disrupt Airport Operations in Europe

| Key Findings

- Between September 22 and September 25, 2025, drone sightings near airports in Denmark and Norway resulted in the closure of multiple airports, including two of the major international hubs in Copenhagen and Oslo. While the incidents have not been linked to a suspect or motive to date, the possibility of Russian involvement cannot be ruled out.
- The drone sightings come on the heels of Polish airports being temporarily closed due to Russian drone intrusions on September 10, 2025. They also coincide with a cyberattack that caused disruptions at several major airports in Europe, stirring concerns for the European civil aviation sector.
- The recent airspace violations in Europe—all with a marked proximity to the Russia-Ukraine conflict—very likely signal a rise in drone and other airspace intrusions across northern and eastern Europe.
- In the wake of these disruptions, air carriers are likely to adopt longer routes; proceed with contingency planning, including higher insurance premiums; and experience elevated operational costs for passenger and cargo sectors.

Details

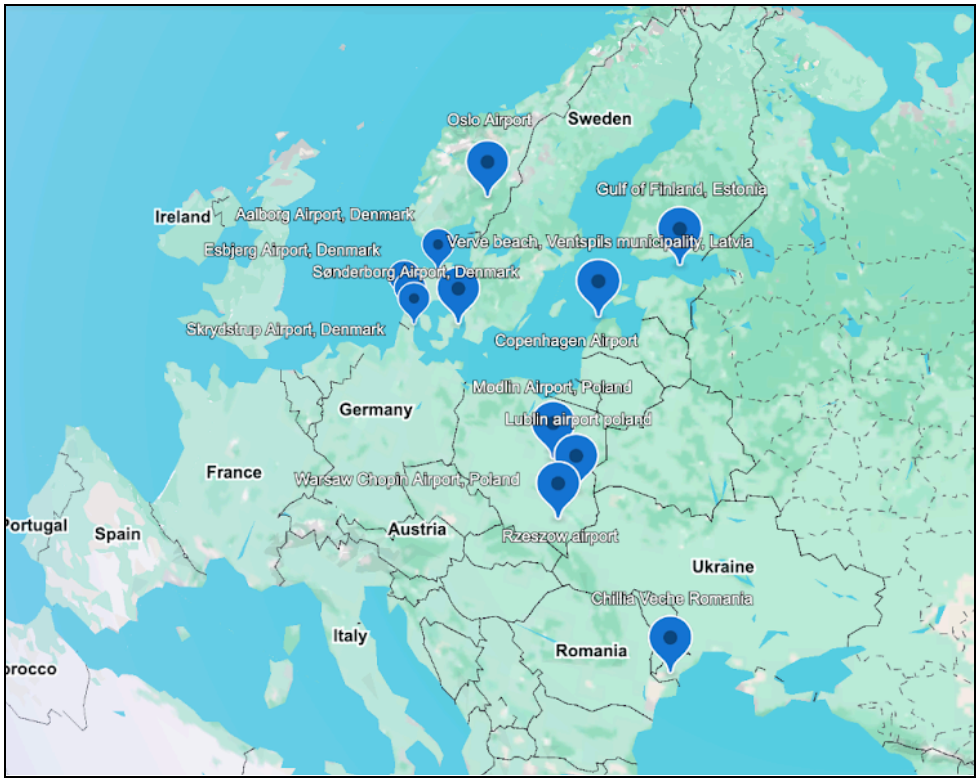
Between September 22 and September 25, 2025, drone sightings near airports in Denmark and Norway resulted in the closure of multiple airports, including two of the major international hubs in Copenhagen and Oslo. Between September 24–25, Aalborg Airport and three smaller facilities in Esbjerg, Sønderborg, and Skrydstrup in Denmark were closed due to drone activity—the second time in one week airports closed in the country for this reason.[1] The closure of the two major airports in Copenhagen and Oslo between September 22–23 resulted in at least four hours of air travel disruption, affecting over 20,000 people; these temporary airport closures resulted in flight cancellations, diversions, and delays.[2] While Copenhagen and Oslo Airports resumed operations on September 23, delays were still reported. Between the airport closures and the resumption of operations, flight tracker FlightRadar24 estimates indicate that 109 flights were cancelled and 51 were rerouted at Copenhagen Airport. At Oslo Airport, 11 flights were diverted and 19 were cancelled.[3]

- These incidents follow recent airport closures in Poland due to Russian drone intrusions reported on September 10.[4] They also coincide with the cyberattack that caused disruptions at several major airports in Europe, stirring concerns for Europe's civil aviation sector.
- Danish Prime Minister Mette Frederiksen has called the Copenhagen drone incident "the most severe attack on Danish infrastructure so far."[5] While she has stated that Russian involvement cannot be ruled out, a Russian spokesman has denied allegations of Russian involvement.[6]
- Although the Danish police said that they have not found an immediate connection between the Copenhagen and Oslo incidents, the two countries are cooperating in the ongoing investigations.

[1] hXXps://edition.cnn[.]com/2025/09/24/europe/denmark-aalborg-airport-closed-drones-latam-intl
[2] hXXps://apnews[.]com/article/drone-denmark-police-security-8e8119cfbc0e276cee1f37ff5ead11d8
[3] hXXps://x[.]com/flightradar24/status/1970349807374942332
[4] hXXps://www.reuters[.]com/business/aerospace-defense/poland-downs-drones-its-airspace-becoming-first-nato -member-fire-during-war-2025-09-10/
[5] hXXps://www.bbc[.]com/news/articles/cqxz3lzlqr3o
[6] hXXps://www.themoscowtimes[.]com/2025/09/23/kremlin-denies-role-in-drone-flights-that-disrupted-airports-in-denmark-and-norway-a90599

- On September 23, Norway's government issued a statement claiming that Russia had violated its airspace at least three times in 2025 but did not confirm whether the most recent incident is connected to previous, likely Russian incursions.[7]

While the Denmark and Norway incidents have not yet been definitely linked to Russia, Europe is already on edge about Russian violations of North Atlantic Treaty Organization (NATO) member countries' airspace following multiple other incidents. In September 2025, Poland, Estonia, Romania, and Latvia reported airspace violations—either by drones or military jets—that were largely attributed to Russia.[8][9][10]



Drone and other airspace intrusions reported between September 1–25

Source: ZeroFox Intelligence

[7] hXXps://www.reuters[.]com/world/europe/norway-says-russia-violated-its-airspace-three-times-2025-2025-09-23/

[8] hXXps://www.nato[.]int/cps/en/natohq/opinions_237718.htm

[9] hXXps://www.bbc[.]com/news/articles/c80g7g5rmlno

[10] hXXps://eng.lsm[.]lv/article/society/defence/19.09.2025-decoy-drone-tail-washed-up-on-beach-near-ventspils-latvia.a614975/

Implications

The recent airspace violations in Europe indicate that such intrusions are very likely to increase in northern and eastern European regions, likely driven by proximity to the Russia-Ukraine conflict and Russian efforts to probe NATO's defenses. The incidents in Denmark, Norway, and Poland—regardless of attribution—almost certainly underscore how quickly airport operations can be disrupted by airspace violations.

- While permanent airspace closures in northern and eastern European regions (apart from those already in force like Ukraine) are unlikely, air travel and air cargo through these regions are likely to experience intermittent disruptions for at least the next six to 12 months.
- Airports that are key to the movement of military and humanitarian aid to Ukraine are very likely to be targeted by Russian drone incursions to hamper support efforts. This was observed in Poland's Rzeszów-Jasionka Airport closure during the September drone intrusions; the airport is a key logistical hub for aid to Ukraine.

NATO countries, including Denmark, are meeting on September 26 to discuss countermeasures against drone and other airspace intrusions and have proposed a "drone wall"—a cooperative effort between Estonia, Latvia, Lithuania, Poland, and Finland to strengthen NATO's eastern border.[1112] Some defense technology companies are already part of this effort, including the makers of Eirshield, an anti-drone platform.[13] However, deploying such systems is expected to take two to three years.[14] In the immediate term, NATO countries are likely to adopt measures such as increased air policing, rapid NOTAMs (notice to airmen), and temporary low-altitude restrictions around affected regions.

[11] hXXps://www.euronews[.]com/my-europe/2025/09/23/we-cannot-wait-eu-calls-for-drone-wall-to-deter-russia-after-new-incident-in-denmark

[12] hXXps://www.euronews[.]com/next/2025/09/21/europe-wants-to-build-a-drone-wall-to-protect-its-eastern-flank-from-russia-is-it-feasible

[13] Ibid.

[14] hXXps://www.rferl[.]org/a/nato-eastern-sentry-russia-drones-poland/33536306.html

Affected Sectors

For air carriers, avoiding riskier eastern and northern European airspace is likely to result in longer flight routes and require planning for disruption contingency, including insurance—and hence, increased operational costs.

- The uncertainty and surging costs are likely to force some airline carriers to suspend eastern European routes, adding to the congestion in air traffic westward.
- Airlines' insurance premiums are likely to rise, increasing operational costs; even temporary closures or no-fly zones due to conflict heighten risk for airline policies.
- Airlines are already managing Middle East disruptions from the Israel-Hamas conflict (which recently stretched into Qatar's airspace) and intermittent India-Pakistan closures in the past few months; the new northern and eastern Europe drone incidents add to conflict corridor risks.

Flight disruptions are also likely to have a ripple impact on the affected region's tourism and hospitality sectors, as the industries may experience cancellations in Nordic and eastern European destinations. Hotels and event organizers are likely to incur losses if inbound flights are canceled.

- Travelers are likely to feel the financial pinch in the form of higher ticket prices for flights on these routes. Travelers will also have to factor in costs of possible delays, diversions, and cancellations.
- In the near term, airport destinations in western Europe are likely to briefly become more expensive due to an increase in air traffic stemming from airlines opting for safer corridors and diversions.

Ground handlers are also likely to be overwhelmed by stranded passengers and checked baggage and cargo due to temporary airport shutdowns. Airports will likely require overtime and surge staffing to restore normal operations.

- Manual check-ins and paper-based handling are likely when systems are overloaded or disrupted due to signal jamming (in case of military responses).

Time-sensitive air cargo supply chains are likely to be impacted by short-term backlogs in the event of airport closures. Even if consignments are rerouted, the diverted traffic is likely to congest alternative airport logistical hubs and result in spill-over delays affecting other regions.

- Disruptions to air cargo supply chains are very likely to impact perishable goods such as fresh produce, medical vaccines, and emergency industrial parts. For these industries, operational costs and transit times are likely to increase to account for rerouting of goods by road.
- Temporary price hikes are likely for perishable goods due to the additional transportation costs and possible lack of supply.
- Traders will likely need to use alternatives to air transportation (including by sea, road, or rail), prolonging delivery times. While air transport is often the most expensive form of trade, re-routing to alternative transportation methods will likely be inflationary.

Conclusion

The Denmark and Norway incidents very likely indicate Europe's growing vulnerability to airspace intrusions stemming from Russia–Ukraine tensions, although direct links to Russia remain unconfirmed. The incidents' timing on the heels of Polish, Baltic, and Romanian airspace violations underscores a pattern that is very likely to persist in northern and eastern Europe in coming six to 12 months. While NATO's proposed "drone wall" offers a long-term fix, interim disruptions—such as delays, reroutes, higher insurance costs, and strained cargo and tourism sectors—are likely to increase in the face of a heightened threat environment.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%