Russia's UAV Campaign Over Europe

Charlie Edwards, Senior Fellow for Strategy and National Security; Rex Fox O'Loughlin, Analyst, Data Science, AHEL; Louis Bearn, Project Manager, AHEL

July 2026




IISS
The International Institute for Strategic Studies

Hanns Seidel Foundation

Contents

Cover

Top (l–r): The detained Boracay*, a Russian shadow-fleet tanker, off the French coast, 1 October 2025. French authorities seized the vessel in late September 2025 on suspicion of being involved in launching UAVs over Denmark between 22 and 25 September (Damien Meyer/AFP via Getty Images); Screen grab from a video showing a* Tsentr *(Centre) Group of Forces 2S5* Giatsint-*S artillery platoon and an* Orlan-*10 fixed-wing ISR UAV team operating near the Serebryansky forest, Ukraine, 16 February 2024 (Russian Ministry of Defence/Handout/Anadolu via Getty Images). Bottom (l–r): A* Le Triomphant*-class nuclear-powered ballistic-missile submarine (SSBN) at the French naval base in Île Longue, 5 December 2016 (Fred Tanneau/AFP via Getty Images); The Heide oil refinery, which was subject to UAV overflights as part of a cluster of suspected surveillance operations in late 2025 across the state of Schleswig-Holstein, Germany (Christian Charisius/Pool/AFP via Getty Images).*

Executive Summary

Between August 2024 and February 2026, Uninhabited Aerial Vehicles (UAVs) were flown in the airspace of a dozen NATO member states and Ireland, forcing repeated closures of major commercial aviation hubs, disrupting military operations and penetrating the perimeters of some of Europe's most sensitive defence installations – among them nuclear-sharing sites hosting American B61-12 gravity bombs and France's ballistic-missile submarine base at Île Longue.

This report assesses it is highly likely that the Kremlin conducted a UAV campaign over Europe. We assess it is likely that Russian-linked vessels and the 'shadow fleet' were used as launch/recovery platforms for UAVs as part of the Kremlin's wider unconventional war on Europe. The UAV campaign (largely in the latter part of 2025) operated with substantial impunity across European airspace – representing both a series of tactical successes for the Kremlin and a strategic failure of allied air defence. The Kremlin's success rests on a basic strategic insight: Europe's air-defence architecture was designed to detect and defeat conventional air threats operating in a recognisable battlespace. It was not built for, by comparison, relatively low-cost UAVs and deniable incursions with the aim of exposing gaps in detection, decision-making and legal authority – all while remaining below the threshold of a collective allied response.

Our argument is not that every reported sighting was Russian-directed, or that every reported sighting involved a UAV, but that the aggregate pattern of UAV sightings cannot be adequately explained by misidentification, hobbyist activity or opportunistic harassment alone. Attribution remains a key challenge for European governments, and none have, to date, publicly attributed a UAV sighting to Russia or gone as far as to describe a coordinated Russian UAV campaign over Western and Northern Europe. One reason, European officials have suggested to us as part of our research, is that the relevant governments focused on the national response rather than connecting the dots across Europe.

Open-source reporting of each incident in the IISS dataset suggests the Kremlin's campaign exposed political fractures within the Alliance, as well as exploiting the gap between what European militaries could do and what their governments were prepared to authorise. And the campaign demonstrated, repeatedly and in public, that the threshold for collective punishment was higher than European deterrence postures have previously assumed.

The campaign likely had a number of aims, including:

- probing the response times and decision-making thresholds of allied air defence and civil-military command structures;
- mapping vulnerabilities around critical infrastructure, including dual-use civilian hubs, military logistics nodes supporting Ukraine, and facilities associated with allied nuclear deterrence;
- imposing economic and psychological costs on European societies through the disruption of civilian aviation and public confidence in airspace security; and
- normalising low-level airspace violations below the threshold of a direct allied military response.

Our key judgement is that Europe's current counter-UAV architecture does not yet match the threat despite NATO, the European Union and national governments focusing more attention on the issue: detection is uneven, legal authorities are fragmented, response options are often disproportionate and attribution remains too slow to support timely deterrence.

The Kremlin's tactical successes in exploiting European air-defence vulnerabilities also revealed the limits of Russia's intelligence-collection options. The Kremlin has been forced to find a series of workarounds since large numbers of Russian intelligence officers were expelled from European capitals in 2022, reducing the Kremlin's intelligence infrastructure in Europe. The UAV campaign also exposed gaps in Russia's Earth-imaging and reconnaissance capacity, especially when

compared with the combined military and commercial space support available to Ukraine and NATO states.

Europe's most ambitious collective response, the European Drone Defence Initiative (EDDI), aims to build a continent-wide, 360-degree counter-drone architecture, with initial operational capability by the end of 2026. Yet the European Parliament concluded in January 2026 that the EDDI lacked the agility and doctrinal coherence required to deliver scalable results. Critically, even a fully operational EDDI will only target the UAV once it enters European airspace – there is no mandate over the vessel that launched it.

Introduction

Between August 2024 and February 2026, Uninhabited Aerial Vehicles (UAVs) were flown in the airspace of a dozen NATO member states and Ireland,[1] forcing the closure of aviation hubs including Brussels, Copenhagen, Munich, Oslo and Vilnius. The UAV flights disrupted smaller regional airports across Denmark, Germany and the Baltic states and were seen over highly sensitive military installations, including European naval facilities and air bases hosting United States nuclear weapons under NATO sharing arrangements.[2]

This report assesses it is highly likely that the Kremlin conducted a UAV campaign over Europe. We assess it is likely that Russian-linked vessels and the 'shadow fleet' were used as launch/recovery platforms as part of the Kremlin's wider unconventional war on Europe. The UAV campaign (largely in the latter part of 2025) operated with substantial impunity across European airspace – representing both a series of tactical successes for the Kremlin and a strategic failure of allied air defence.

The UAV campaign in late 2025 appears to have served a number of aims: probing the response times and decision-making thresholds of allied air defence and civil-military command structures; mapping vulnerabilities around critical infrastructure, including dual-use civilian hubs, military logistics nodes supporting Ukraine, and facilities associated with allied nuclear deterrence; imposing economic and psychological costs on European societies through the disruption of civilian aviation and public confidence in airspace security; and normalising low-level airspace violations below the threshold of a direct allied military response. These aims are not mutually exclusive, and individual incidents are likely to have served more than one.

Europe's response to the UAV campaign was constrained from the outset by a detection problem that predated the Kremlin's campaign by decades. Europe's (including the United Kingdom's) air-defence and civil-aviation radar infrastructure was designed for a different era and was focused on fast, high-altitude aircraft operating in known corridors, cooperating with aviation and surveillance systems that depended on electronic self-identification.

UAVs flying at low altitude during night-time, without broadcasting their identify and position, launched from vessels in international waters rather than crossing a land border, exploited numerous gaps in both European governments' air-defence and civil-aviation infrastructure. Ground-based radar was unable to reliably track UAVs. Airborne surveillance assets almost certainly struggled to distinguish them from background clutter. The civil-aviation system, built around cooperative users, had no mechanism to detect a UAV that deliberately chose not to announce itself (for obvious reasons). European regulators have been aware of elements of this problem for years.[3] For example, there has been a long-running debate across Europe and the UK about how to make gliders and other slow aircraft visible to air traffic control given the same detection challenge outlined above.

This report's central judgement is not that every reported sighting was Russian-directed, or that every reported sighting involved a UAV, but that the aggregate pattern of UAV sightings cannot be adequately explained by misidentification, hobbyist activity or opportunistic harassment alone. Attribution remains a key challenge for European governments, and none have, to date, publicly attributed a UAV sighting to Russia or gone as far as to describe a coordinated Russian UAV campaign over Western and Northern Europe. One reason officials have privately suggested is that, in most cases, a government was more likely to focus on their national response than connect the dots to incidents across Europe.

Subsequent investigations have challenged whether many of the reported sightings involved actual UAVs rather than conventional aircraft, visual misidentification or other benign activity. A joint investigation by the Dutch news outlets Trouw and Dronewatch examined

61 separate drone sightings reported across 11 European nations during the autumn of 2025 and found that, in 55 of those 61 sightings, there was no confirmation of a hostile or illegal UAV.[4] Several objects reported over Copenhagen at the time were possibly routine air traffic, misidentified by observers in the absence of dedicated drone-detection equipment.[5] These findings warrant scrutiny, however. In an operating environment where European detection capability was demonstrably insufficient to reliably track low-altitude, non-cooperative UAVs, a high non-confirmation rate is the expected outcome regardless of whether the sightings were genuine. The misidentification problem has been broadly acknowledged by European governments and is why this report applies a triangulated methodology across four distinct data sources. A high false-positive rate in public reporting is, if anything, analytically consistent with Russian operational design: engineering an environment of ambiguity in which genuine incursions are difficult to distinguish from noise is itself a feature of the campaign.

The increase in recreational UAV activity across Europe in recent years provides one alternative explanation for a significant proportion of reported sightings — but it does not account for the incidents central to this report. Lawful recreational use of UAVs is generally constrained by visual-line-of-sight requirements, height limits and national geographical zones around sensitive sites. The key incidents in this report occurred at night, near airports, military bases or nuclear-related infrastructure, and involved UAVs described as larger or more capable than ordinary consumer drones.[6]

While some of the Danish cases remain inconclusive, lessons from Russia's unconventional war on Europe suggest that focusing on the broader pattern of behaviour, rather than isolated incidents, is a more analytically robust approach.[7] It is notable that UAV incursions across Europe remain under active investigation by at least half a dozen or so law enforcement and intelligence agencies, and, informally, numerous European governments believe that Russia was behind a number of UAV incidents.

The shift from terrestrial sabotage (e.g., the attack on the Polish railway network in 2025) and maritime sabotage (e.g., the damage to the EstLink 2 submarine cable in 2024) to physical airspace violations by UAVs suggests a tactical evolution of the Kremlin's unconventional war on Europe. Furthermore, the use of UAVs crosses a qualitative threshold, placing unattributed state air platforms inside the sovereign airspace of NATO member states. We assess it is likely that a subset of the UAV incidents in our dataset were launched and recovered from Russian-linked commercial vessels, including shadow-fleet tankers, coastal freighters, and smaller craft, and which could have plausibly served as mobile platforms for reconnaissance UAVs operating near European ports, airports, energy infrastructure and military facilities.

This hypothesis is based on two observations of the data. Firstly, the geographic distribution of late-2025 incident clusters along North Sea, Baltic and Atlantic coasts where Russian-linked maritime traffic is constant and where shadow-fleet Automatic Identification System (AIS) irregularities have been independently documented.[8] Secondly, Russian UAV development since 2022 has produced platforms whose technical characteristics are consistent, though not uniquely so, with covert launch from a vessel.[9] The clearest example is the February 2026 incident involving the French nuclear-powered aircraft carrier *Charles de Gaulle*, where the Swedish military assessed that a UAV jammed near the aircraft carrier was of Russian origin and had been launched from the Russian spy ship the *Zhigulevsk* (IMO 4617980),[10] confirming that the maritime launch of a UAV is an operational reality.

Not all UAV incidents across Europe in 2024–26 belong in the same category. This report distinguishes between two operationally distinct types of UAV activity. The first is a covert maritime intelligence, surveillance, and reconnaissance (ISR) campaign against nuclear-deterrence infrastructure, logistics nodes, military installations and civilian aviation hubs across Northwest and Central Europe. These missions were characterised by night operations, extended endurance, platform sizes inconsistent with civilian use and a geographic distribution along European coastlines consistent with maritime launches from Russian-linked vessels and the shadow fleet. This maritime-enabled campaign is the primary subject of this report. The second is the eastern-flank strike and probing campaign: the mass

employment of *Shahed* loitering munitions and *Gerbera* decoy drones predominantly associated with Russia's ongoing air campaign against Ukraine, elements of which have either drifted into or been deliberately routed into NATO airspace.

Open-source reporting suggests that several UAV models were used in the campaign, with the choice likely to have been mission dependent and, in most cases, requiring a crew of two – a pilot and an operator. The *Orlan*-10, a compact, multi-purpose UAV in service with Russian Armed Forces since 2010,[11] has a range and payload profile consistent with stand-off collection against coastal and inland targets and fits the deck space of a mid-sized commercial vessel. Commercial specifications for the platform, including those published by Russian geospatial firms using the *Orlan*-10 for civilian aerial survey operations, document an operational range of 500 kilometres, endurance of up to 12 hours, and speeds of 90–130 km/h,[12] performance parameters consistent with maritime launch from a vessel operating well beyond visual detection range of the European coastlines in question. The *Orlan*-10's power is an internal combustion engine, a detail that may be relevant in light of witness accounts from November 2024 incidents at RAF Lakenheath, where propulsion noise was described by some observers as more characteristic of petrol engines than the electric motors typical of consumer and first-person view (FPV) drones. The available payloads include a satellite navigation spoofing module and a Global System for Mobile Communications network monitoring module alongside optical and thermal sensors, indicating the *Orlan*-10 family has active electronic warfare capability as well as passive ISR. The *Merlin*-VR offers a further plausible candidate for maritime-launched reconnaissance operations.[13] A Russian-developed fixed-wing ISR platform, the *Merlin*-VR, combines a catapult-launch profile with parachute recovery – a pairing that is well suited to vessel-based operations. Parachute recovery is operationally preferable to net-based systems in a maritime context as it reduces the deck footprint, lowers the risk of platform damage during recovery at sea, and requires less specialised crew equipment. The *Merlin*-VR's endurance and payload are consistent with the stand-off collection profile for night operations, extended loiter over fixed infrastructure, and the geographic range in the case studies identified in the dataset. Vertical-take-off-and-landing (VTOL) platforms (e.g., the *Legioner* E29 Fixed-Wing Electric Drone made by Kalashnikov) also reduce the required deck footprint, remove the need for a recovery net and offer a smaller visual signature on AIS-tracked vessels, which is operationally attractive for launching off the shadow fleet. However, the use of identifiable Russian UAV platforms carries inherent attribution risk. An alternative, and operationally credible, hypothesis is that commercially available or modified platforms were used precisely to preserve deniability, including long-range FPV systems, home-built fixed-wing aircraft or commercial UAVs modified to use cellular rather than radio frequency (RF) communications.

The maritime-launch hypothesis is supported by a convergence of opportunity, demonstrated capability and a consistent geographic pattern, but there has not yet been a public attribution by a European government linking a specific shadow-fleet vessel to a specific European incident despite officials suggesting otherwise. The remainder of this report treats the maritime-UAV nexus as the most plausible explanation for the geographic and temporal distribution of incidents, while acknowledging that confirmation will require evidence not yet in the open-source domain.

This report unpacks attribution into three distinct questions:

- Is the hardware of Russian origin or built to a known Russian manufacturing pattern?
- Who launched the platform, from where, and under whose immediate tactical direction?
- Is the Kremlin directing a coherent, top-down campaign, or is the research aggregating the disjointed actions of the Russian intelligence services, another foreign actor and/or expendable criminal proxies recruited through Telegram into a false unity?

This report employs a triangulation methodology which cross-references findings across four distinct data sources, each with acknowledged strengths and limitations:

- AIS maritime tracking data has helped to establish the co-location of shadow-fleet vessels with

incident geographies, though it cannot independently confirm hostile intent.

- The Armed Conflict Location & Event Data Project (ACLED) provides geospatial and temporal clustering of sabotage events and airspace incursions, but its density is contingent on the underlying reporting environment.
- Open-source and media reporting supplies granular local detail on the immediate impact of incidents, while remaining vulnerable to variable reliability and the laundering of unverified claims between outlets.
- Finally, semi-structured interviews with European defence and intelligence officials provide the off-record strategic context necessary to interpret these streams while remaining inherently non-falsifiable. While no single source settles the attribution question, their convergence has produced a pattern that is harder to explain by coincidence than by coordination.

The report's argument is therefore deliberately bounded. It does not claim that all 2025 sightings (particularly in the latter part of the year) were real, Russian or coordinated. It does assess that the pattern of selected UAV incidents across Europe is consistent with the Kremlin's effort to probe allied defences, test civilian-military response mechanisms and normalise low-level airspace violations below the threshold of an armed attack. The central finding is that Europe's current counter-UAV architecture is not yet matched to the threat: detection is uneven, legal authorities are fragmented, response options are often disproportionate, and attribution remains too slow to support timely deterrence.

The Kremlin's tactical successes in exploiting European air-defence vulnerabilities also revealed the limits of Russia's other intelligence-collection options. The Kremlin has been forced to find a series of workarounds since large numbers of Russian intelligence officers were expelled from European capitals in 2022, reducing the Kremlin's intelligence infrastructure in Europe. The UAV campaign also exposed significant gaps in Russia's Earth-imaging and reconnaissance capacity, especially compared with the combined military and commercial space support available to Ukraine and NATO states.[14]

Europe's most ambitious collective response, the European Drone Defence Initiative (EDDI), aims to build a continent-wide, 360-degree counter-drone architecture, with initial operational capability by the end of 2026. Yet the European Parliament warned that the unsustainably high costs of drone interceptions remain unresolved, that lengthy procurement and testing processes risk making EU capabilities obsolete by the time they are deployed, and that doctrinal and operational gaps between EU and NATO drone defence remain unabridged.[15]

1. The Kremlin's Strategic Intent

On 22 September 2025, the airspace above Copenhagen Airport was abruptly closed for four hours after suspected sightings of a UAV. The incident disrupted 190 flights and left thousands of passengers stranded.[16] Between 22 and 26 September 2025, more sightings of UAVs were reported at airports across Denmark, including Aalborg, Billund, Esbjerg and Sønderborg. Aalborg, a Royal Danish Air Force base which hosts the 721 Squadron and the Danish Jaeger Corps (a special forces unit), was forced to close twice due to UAV sightings.[17] These incursions coincided with sightings of UAVs near other highly sensitive military installations, including the base of the Jutland Dragoon regiment and Skrydstrup Air Base, where Ukrainian pilots had received training on F-16 fighter jets.[18]

In the immediate aftermath, the Danish authorities noted the UAVs were flown by 'highly capable operators' and the authorities 'were investigating several hypotheses, including the possibility that the drones were launched from ships'.[19] Suspicion focused on the *Boracay* (IMO 9332810), a Russian shadow-fleet tanker[20] that was tracked off the Danish coast during the incidents.

On 25 September 2025, Finn Borch Andersen, the head of the Danish Security and Intelligence Service, said that, while they were unable to name a specific actor behind the drones, 'We can say that this resembles a model of hybrid warfare we have seen elsewhere in Europe … I would remind you … that we assess the risk of Russian espionage in Denmark to be high, and we also assess the risk of Russian sabotage in Denmark to be high.'[21] Troels Lund Poulsen, the Danish defence minister, said, 'Everything points to this being the work of a professional actor when we are talking about such a systematic operation in so many locations at virtually the same time.'[22]

The September incidents at Copenhagen Airport and across Danish military bases have attracted international attention, but their attribution is partially complicated by subsequent investigations and the lack of any public Danish government inquiry. The Danish Defence Command's June 2026 evaluation, the first official military assessment of the incidents, concluded that, even within Denmark's own armed forces, observations ranged from probable commercial aircraft to confirmed drone activity, and that no validated baseline of normal drone activity existed against which to judge the incidents. But an incident on 3 January 2025 provides more concrete evidence. Up to 20 large UAVs were observed flying in formation over the port of Køge, a commercial harbour 39 km southwest of Copenhagen, before disappearing into Køge Bay at high speed.[23] In 2022, the port served as the primary embarkation point for Denmark's largest military deployment in two decades in support of NATO's Enhanced Forward Presence on the eastern flank.[24] For Russian military planners seeking to map NATO's logistical arteries to the Baltic states, it is highly likely that Køge harbour was a priority, and the January 2025 overflight, confirmed by Danish police, constitutes one of the clearest uncontested examples of UAVs flying over a dual-purpose logistics site.

On 28 September 2025, French naval commandos intercepted and boarded the *Boracay* off the coast of Saint-Nazaire.[25] The boarding revealed that alongside the Chinese captain, the ship was carrying two Russian nationals employed by the Moran Security Group, a Russian private military company founded by former Federal Security Service (FSB) officers. One of them had previously worked for the Wagner Group, the private military company linked to Russia's military intelligence (GRU). The two Russian nationals were reportedly tasked with gathering intelligence, protecting the vessel and ensuring the captain strictly adhered to Russian interests, providing direct evidence of a shadow-fleet vessel linked to Russian intelligence structures. It is possible the *Boracay* was under surveillance following the September UAV incidents over Denmark. More importantly, the identification of two Russian private military contractors confirmed the militarisation of shadow-fleet tankers, not as a hypothesis but as operational practice.[26]

Evidence suggests that individual incidents were designed to achieve multiple strategic objectives simultaneously, including collecting intelligence, testing military responses, creating societal disruption and sustaining strategic ambiguity. The November 2025 UAV incursions over the Netherlands are one example. A single operation could have likely included surveillance of Volkel Air Base; triggered Dutch ground-based air defences, measuring the Dutch and Belgian Quick Reaction Alert (QRA) mission reaction times; and forced the suspension of air traffic at nearby Eindhoven Airport, thereby imposing some economic costs and creating public unease. Assessed through this lens, the aims of reconnaissance by battle, economic attrition and psychological pressure as well as normalising low-level violations potentially provide the overarching operational framework. The following section describes each aim in more detail:

Reconnaissance by Battle

The Kremlin's UAV campaign exhibits the tactical logic of *razvedka boyem*, the Soviet and Russian doctrine of reconnaissance by battle.[27] In its conventional ground-combat application, military units are deployed in deliberate contact with an adversary's defensive positions, not primarily to seize ground but to compel the defender to activate fire systems and commit reserves, forcing disclosure that passive surveillance cannot achieve.[28] The analytical extension to the air domain is direct rather than metaphorical: the UAV functions as the attacking probe; NATO air-defence responses (e.g., radar activation revealing frequency ranges, scrambled fighters exposing intercept protocols) generate intelligence.[29]

The strategic objective of the campaign was possibly determined by the Strategic Operation for the Destruction of Critically Important Targets framework,[30] which the Russian General Staff identify as a decisive opening operation in high-intensity conflict, requiring comprehensive prior targeting data on the adversary's logistics, command infrastructure and air-defence architecture. The UAV campaign almost certainly would have generated data on radar blind spots, interception corridors and rules-of-engagement thresholds across European airspace.[31] The unprecedented incursion of up to 24 Russian UAVs into Polish airspace on the night of 9–10 September 2025 illustrates the compounding nature of these objectives.[32] By triggering a joint allied response that scrambled Polish F-16s, Dutch F-35s and Italian airborne early-warning aircraft, the incident provided Russia with an opportunity to observe allied reaction times, command procedures and air-defence responses.[33]

The specific flight paths of several *Gerbera* decoy drones directed towards Rzeszów-Jasionka Airport in Poland would have allowed the Kremlin to probe air defences. The incursion inflicted direct economic and psychological costs by forcing temporary airport closures, damaging civilian property in the village of Wyryki[34] and exploiting domestic political debates regarding the conflict.

The Cold War 'ferret missions' offer a useful historical analogue for understanding Russia's UAV campaign over Europe. US reconnaissance flights were partly designed to make the Soviet Union's air-defence system react. By flying along, and in some cases across, Soviet airspace, they helped identify radar sites, command-and-control arrangements, interception procedures and gaps in coverage. The Kremlin's contemporary UAV activity appears to draw on the same operational logic.[35]

Mapping Critical Infrastructure: Nuclear and Dual-use Sites

Based on an analysis of the data, an objective of the Russian UAV campaign in 2025 was likely the surveillance of Europe's nuclear and dual-capable infrastructure. The pattern was most pronounced at nuclear infrastructure sites which have been reported to host American B61-12 gravity bombs and are forward deployed under NATO.[36] [37] In November 2025, Belgian authorities observed UAVs over Kleine-Brogel.[38]

Logistics and Supply Chains

A second dimension of this aim likely supported the mapping of logistical infrastructure supporting the Ukrainian war effort. German federal authorities recorded over 1,000 suspicious drone sightings in 2025.[39] German Interior Minister Alexander Dobrindt has attributed the pattern to a state actor seeking to generate uncertainty, while stopping short of formally

identifying Russia.[40] Drone activity has clustered around facilities connected to Ukrainian aid, including sites where Ukrainian personnel are trained on *Patriot* air-defence systems (Husum Schwesing Airport) and M1 *Abrams* tanks (the US base in Grafenwoehr).

Economic Attrition and Psychological Warfare

The third aim brings together two related but operationally distinct effects. The first is economic attrition: exploiting the gap between UAV systems and the expensive responses needed to detect, track and defeat them.[41] The repeated closure of major commercial airports imposed real costs on European governments and private-sector companies. Copenhagen Airport was closed for four hours on 22 September, disrupting 190 flights and leaving thousands of passengers stranded. Within 48 hours, more incidents had affected five airports across Denmark.

Coordinated information operations have followed the media reporting of UAV sightings, with Russian-aligned networks, including elements of the Doppelganger operation previously documented by EU DisinfoLab and Viginum,[42] amplifying narratives that deny Russian involvement, attribute incidents to Ukrainian provocation or accuse European governments of manufacturing a crisis. The intent is to erode a public's confidence in their government's ability to protect them, highlight vulnerabilities with airspace security and all the while dilute political consensus around continued support for Ukraine.

Recovered UAVs in Poland reportedly carried Polish and Lithuanian SIM cards, suggesting an effort to exploit civilian mobile networks for connectivity, telemetry or navigation. Combined with the maritime-launch hypothesis examined in Section 2 and the use of expendable platforms, it is consistent with the aim of pushing attribution costs onto European investigators while preserving plausible deniability at the strategic level.

While the 22 September incident over Copenhagen Airport is contested, the pattern of drone sightings over Denmark in 2025 exhibits elements of all four aims in compressed form, not least given the proximity of Aalborg, Skrydstrup and the Jaeger Corps base. A better question, therefore, is whether the Danish experience is less an outlier than a concentrated expression of the Kremlin campaign's logic. The Køge incident provides a robust evidence base: up to 20 drones, confirmed by police officers on the scene, operating without permits over a port that serves as NATO's primary Baltic logistics gateway before disappearing into Køge Bay in a manner consistent with maritime launch. Section 2 examines how the maritime dimension, the shadow-fleet and commercial vessels that were tracked off the Danish coast during the incidents, provides the operational mechanism that ties these purposes together.

Normalising Airspace Violations

A final aim operates differently from the others. Reconnaissance by battle, infrastructure surveillance and economic attrition produce visible effects. Normalisation works more slowly. Its purpose is to change what European governments, publics and institutions treat as requiring a response. While each airspace violation may carry no meaningful consequence, it is the cumulative effect that changes the acceptable baseline of what counts. Repeated low-level intrusions, ambiguous attribution and divided political responses all raise Europe's tolerance of what once upon a time would not have been treated as routine. The information campaign reinforces the effect. Narratives denying Russian involvement, or blaming allied incompetence, reduce the political cost of each incident. It also, importantly, conditions the public to see ambiguity as the normal state of European airspace. Over time, this risks creating a permissive environment in which more serious activity, including pre-conflict suppression of allied air defence, is preceded by a period in which the meaning of a 'violation' has already been weakened.

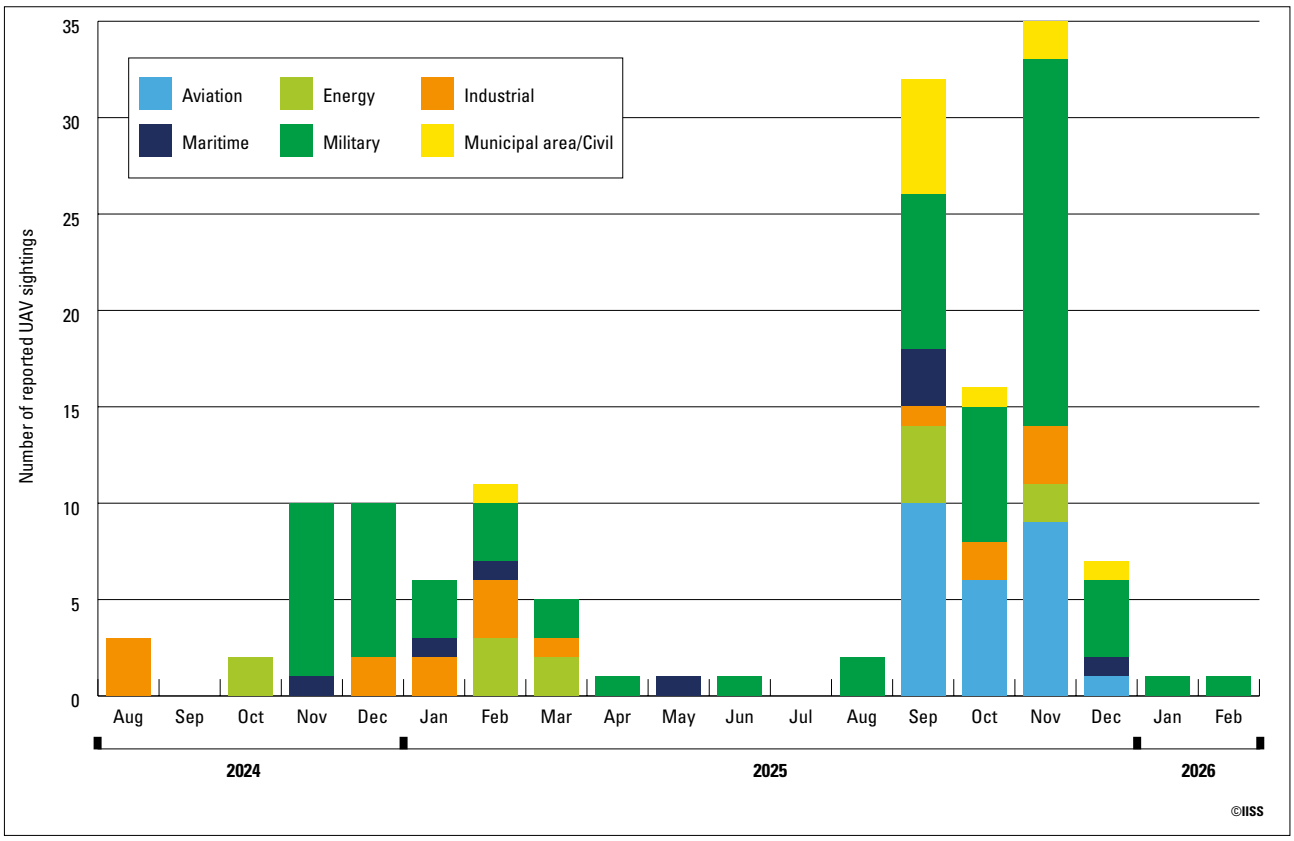
2. The Maritime-UAV Nexus

Between August 2024 and February 2026, there was a large increase in reported UAV sightings over a dozen European states. Using a combination of data from ACLED and news reporting, we have compiled a dataset of 144 such incidents. Those that have been assessed to be hobbyist activity or spillover from the war in Ukraine have been removed. From this dataset, a pattern emerged: approximately 48% of sightings occurred over military facilities, 18% over civilian airports, and 26% over critical infrastructure including ports, energy installations and industrial sites. UAV sightings over civilian airports often resulted in the closure of the airport, creating further costs. Sightings usually occurred at night or in the early hours of the morning before sunrise. For example, the UAV incidents at the US Ramstein Air Base in Germany, Île Longue, Kleine-Brogel and Volkel began early in the evening and continued late into the night. The Île Longue incursion occurred on the night of a supermoon that provided good visibility.

UAV incidents were variously described in media reporting as 'larger than the usual commercial hobby drones',[43] 'fixed-wing drones',[44] 'military style'[45] and 'professional devices with wing spans of three to six meters'.[46] The pattern of night-time flights combined with descriptions of the UAVs suggests that these were military-type UAVs, not typical of ordinary recreational quadcopters.

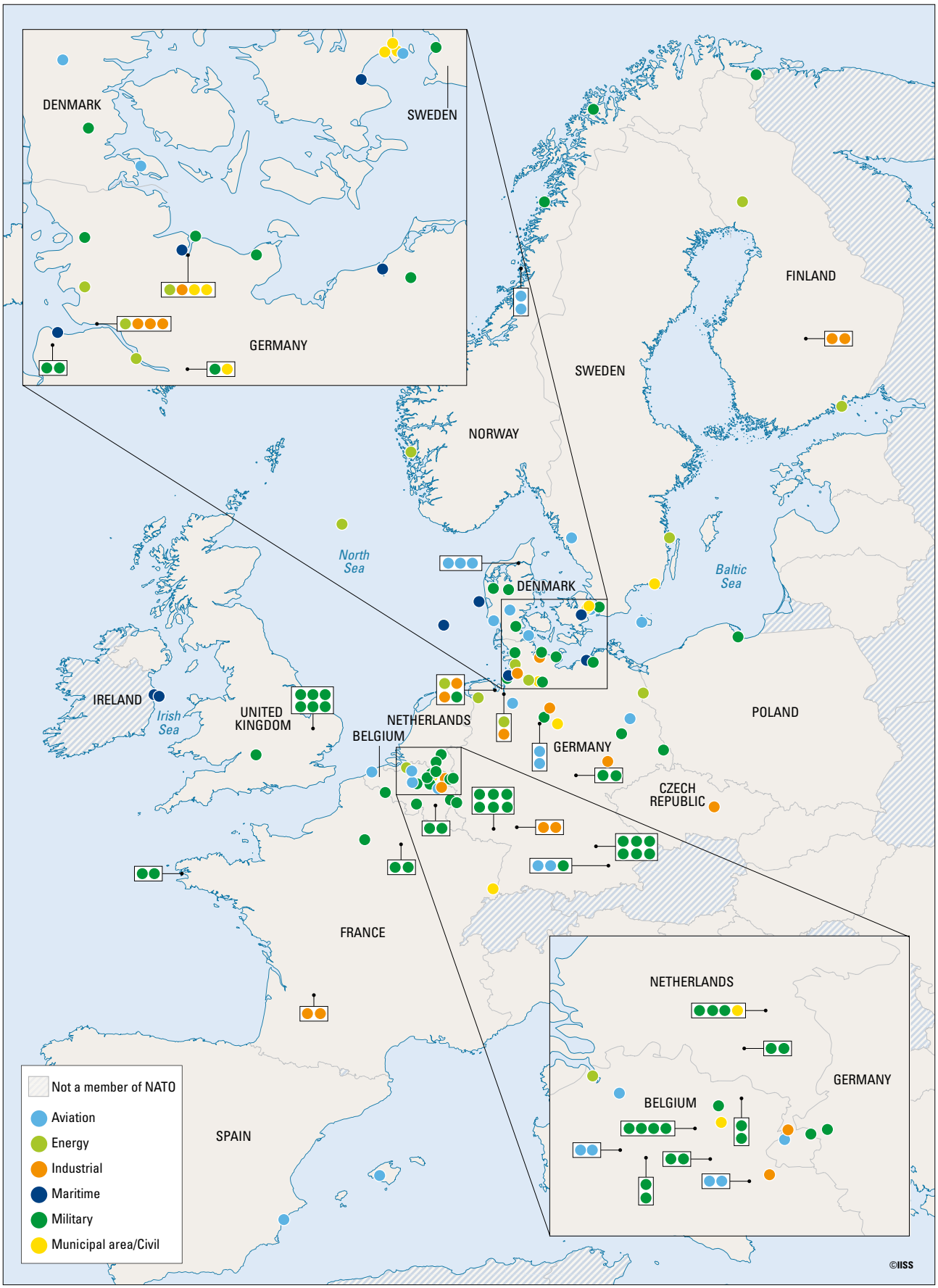
The largest increase in sightings occurred between September and December 2025, when the number of reported incidents jumped from an average of four per month (August 2024–August 2025) to 22.5 per month. Figure 2.2 clearly shows this cluster. Germany recorded

Figure 2.1: **Selected reported UAV sightings in Europe by site, August 2024–February 2026**



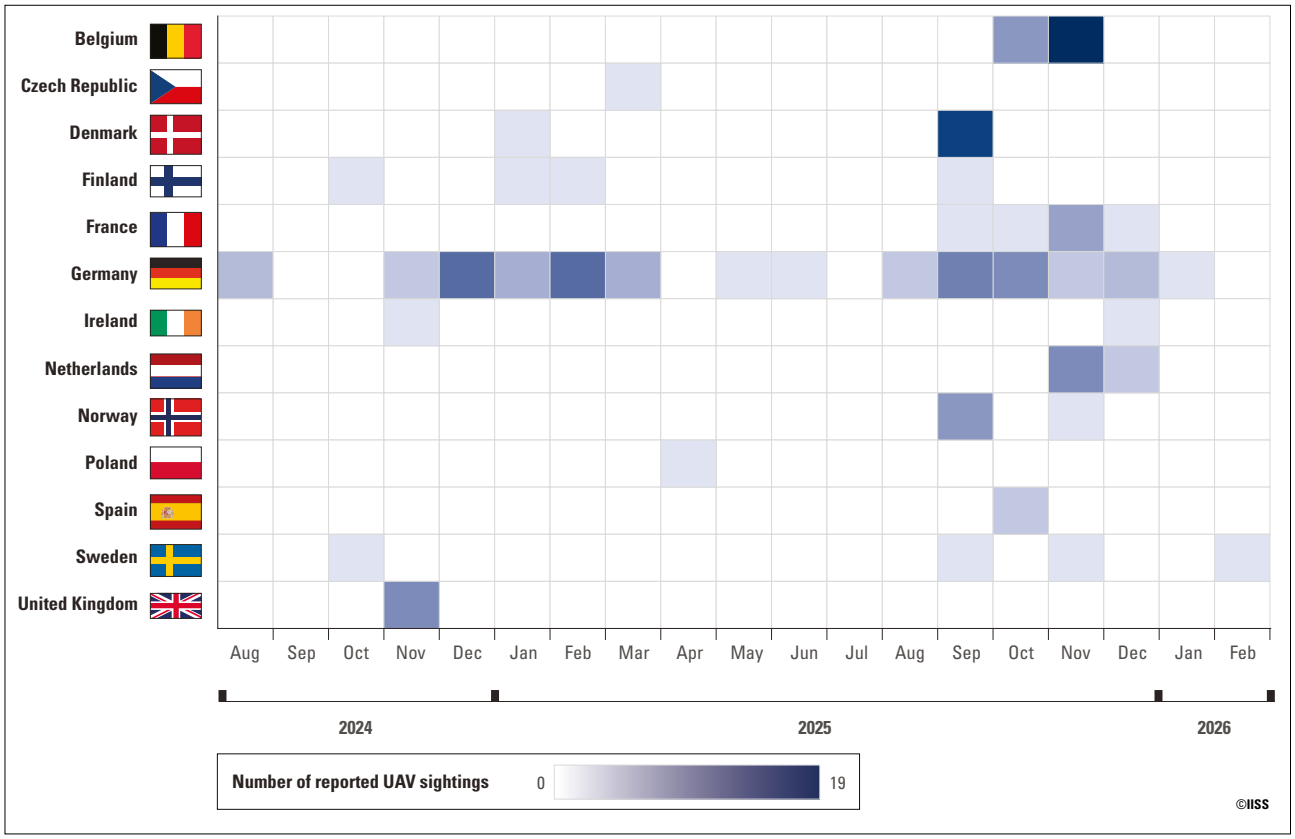
UAV = uninhabited aerial vehicle
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com

Map 2.1: **Selected reported UAV sightings in Europe by location and site, August 2024–February 2026**



UAV = uninhabited aerial vehicle
Note: Sightings of UAVs related to the war in Ukraine are not shown.
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com

Figure 2.2: **Selected reported UAV sightings in Europe by month, August 2024–February 2026**



UAV = uninhabited aerial vehicle
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com

the largest number of incidents of any European country, with 58 reported UAV sightings between August 2024 and February 2026. It was followed by Belgium with 25 sightings, Denmark with 16 and the Netherlands recording nine. France recorded eight, while the UK and Norway each recorded seven. Finland and Sweden had four sightings each, with the most recent incident occurring at Malmö, Sweden, during the visit of the *Charles de Gaulle* in February 2026. Ireland and Spain each reported two incidents and the Czech Republic and Poland each had a single sighting.

Between the end of November 2024 and March 2025, six separate incidents of 'possible spy drones' were reported over Ramstein, which remain unexplained. Concurrent incidents were reported over Bundeswehr facilities including Ingolstadt-Manching Airport and Neuburg Air Base in December 2024 and early January 2025, which Bavaria's State Criminal Police Office investigated as a security threat.

Other similar incidents were also reported in the vicinity of industrial facilities including the BASF chemical plant in Ludwigshafen and the defence firm Rheinmetall, which is involved in the manufacturing of artillery ammunition and the *Lynx* infantry fighting vehicles, training of Ukrainian personnel and establishing manufacturing and maintenance hubs in Ukraine. Earlier in the year, there were reports of UAV sightings in the north of Germany, including over an industrial park at Brunsbüttel, northwest of Hamburg. The industrial park includes a liquefied natural gas (LNG) facility created in response to Russia's invasion of Ukraine and a new floating LNG terminal amid concerns about Germany's energy imports. German prosecutors said they considered the UAV overflights related to 'espionage activity for sabotage purposes.'[47] Reports noted that the UAV overflights of Brunsbüttel began on 8 August and approached from the sea. While media reporting suggested the UAVs as possibly *Orlan*-10s, consistent with the platform profile outlined in Section 1 and based on distance and recorded speeds exceeding 100 km an hour, the type of UAV has not been confirmed by the German authorities.

Establishing Co-location

Establishing the co-location of shadow-fleet vessels with UAV incident windows requires triangulating across multiple data streams because the primary tool available for tracking commercial maritime traffic, the AIS, is itself subject to deliberate manipulation. AIS transmits a vessel's identity, position, course, speed and cargo data at regular intervals over VHF radio frequencies, and it is designed to reduce collision risk and enable port state control (the inspection of foreign-registered ships).[48]

In principle, AIS provides a near-real-time map of commercial traffic in any given maritime space. In practice, AIS is only as reliable as its operators' compliance. The system's VHF architecture means that transponders can be switched off entirely, their data spoofed to broadcast false positions, or their signals relayed from a third vessel to create an alibi location for a ship operating elsewhere. The deliberate exploitation of these vulnerabilities is well documented in the context of sanctions evasion, but its systematic application in coordination with the Kremlin's unconventional war on Europe represents a qualitatively different analytical challenge.[49]

Since 2022, Russian oil exports have relied increasingly on a fleet of ageing, re-flagged tankers acquired through multi-layered holding structures in jurisdictions including Marshall Islands, Panama and Sierra Leone, with management companies typically registered separately in the United Arab Emirates or Türkiye. Estimates of the size of Russia's shadow fleet vary. Windward AI, a shipping data company, suggests the shadow fleet numbers approximately 1,300 tankers.[50] The KSE Institute's tracking shows the fleet remains central to Russian seaborne oil exports, with shadow tankers accounting for 70% of crude exports in February 2026.[51] While the aim is to frustrate sanctions enforcement and complicate port state control, it has the secondary effect of obstructing any intelligence attribution of hybrid activities conducted from those vessels.

AIS manipulation by the shadow fleet takes several forms. The most straightforward is 'going dark' by switching off the transponder, which removes the vessel from AIS-derived tracking displays entirely. A more sophisticated technique is Global Navigation Satellite System (GNSS) spoofing, part of broader navigation warfare, in which a vessel continues to broadcast AIS signals whilst transmitting false coordinates, creating the appearance of normal transit while the ship operates in a different location. A third method involves identity theft, using ghost ships that sail under the stolen identities of legitimately operating vessels to deliberately generate contradictory monitoring data.

For UAV launch operations, the most relevant technique is 'dark sailing' – sailing close enough to a target coastline to bring embarked UAVs within range. It is plausible that a Russian-linked vessel and/or shadow-fleet tanker approaches the operating area, switches off its AIS transponder while a launch or recovery of a UAV takes place, and resumes normal transmission once clear of the area. AIS gaps cannot by themselves prove hostile intent. However, when AIS data is overlaid with Synthetic Aperture Radar (SAR) satellite imagery, which can detect vessels at night and through cloud, investigators can potentially identify ships that are physically present but not broadcasting. In January 2026, a joint declaration by a group of Baltic and North Sea coastal states formally registered concern about the deterioration of maritime safety in the region, citing GNSS interference, AIS data manipulation and the risks of the shadow fleet operating in their shared waters.[52]

The ship-to-ship (STS) transfer mechanism is also worth considering in the context of the Kremlin's UAV campaign. STS transfers in which a vessel exchanges cargo with a waiting tanker in an offshore anchorage and both vessels have their transponders switched off can sever the traceable link between sanctioned Russian crude and its eventual destination.[53] The posture required for an STS transfer including offshore loitering, possible AIS gaps and commercial cover could mask other activity, including UAV launch or recovery.

Given the constraints outlined above, AIS data is a necessary but insufficient source on its own. SAR satellite imagery detects vessel presence through radio-wave reflection regardless of AIS transmission; because SAR radio waves penetrate cloud cover and darkness to reflect off metal hulls, it is particularly useful for identifying dark ships operating without transponders. An example is the unidentified vessel detected in the Irish Sea during the 1 December 2025 drone incident near Dublin, which could indicate the vessel was present with its AIS turned off (see Map 2.7).

A further complication is the use of Russian naval assets to escort shadow-fleet vessels through European waters, such as the Steregushchy-class corvette *Boikiy* escorting the *General Skobelev* (IMO 9503304), an oil tanker, through the English Channel in January 2026.[54] Naval escorts of civilian vessels in international waters are not unlawful under the United Nations Convention on the Law of the Sea, but they complicate enforcement operations. A mix of commercial cover, legal ambiguity and deliberate manipulation of the maritime surveillance picture are therefore central to the campaign's design.

On 22 November 2024, during a five-day defence engagement port visit to Hamburg by the UK Royal Navy's flagship aircraft carrier HMS *Queen Elizabeth*, the water protection team reported the sighting of a 1.5 metre UAV hovering near the carrier's anchorage in the early morning. The drone threat was allegedly disrupted by teams equipped with HP-47 jamming systems; however, the drone flew away in the direction of the Tollerot container terminal.[55]

In December 2025, students from the Axel Springer Academy of Journalism and Technology obtained a classified Federal Criminal Police Office (BKA) report which assessed that Germany experienced 1,072 incidents involving 1,955 drones in 2025. Their investigation concluded that a coordinated pattern of UAV sightings over sensitive sites in Germany including military bases, industrial facilities, commercial ports and civilian airports may have been linked to Russian-linked vessels transiting the North and Baltic Seas.

The students had reports on several specific vessels, including the cargo ship *Scanlark* (IMO 8505915) which German special forces boarded after the vessel returned to Kiel on 7 September 2025. Its mostly Russian crew was suspected of launching a drone on 26 August 2025 over a German naval vessel to reconnoitre and take photographs.[56]

According to the BKA documents, 'individual incidents indicate complex operations drawing on larger financial and logistical resources', suggesting that the incidents were not the work of hobbyists. By analysing the ships' AIS and some satellite imagery, the journalists were able to correlate anomalies in Russian-linked vessel movements in the Baltic and North Sea areas to 19 incidents of UAV overflights. The three ships identified in the investigation were Antigua and Barbuda-flagged cargo vessels the *Hav Dolphin* (IMO 9073854) and the *Hav Snapper* (IMO 9001813); and the Russian-flagged freighter the *Lauga* (IMO 9111060), formerly the *Ivan Shchepetov*, whose unusual loitering movements coincided with the drone sightings. The *Hav Dolphin* was specifically singled out for investigation by Germany and the Netherlands after the vessel left Kaliningrad in early May 2025 and anchored off the coast of Kiel for eight days, during which there were UAV sightings at the German submarine base at Eckernförde.[57] A separate but contemporaneous incident involved the *Lauga* and the launch of seven UAVs over the German patrol boat *BP 81 Potsdam*. The *Lauga* had previously been associated with Russian military cargo operations in Syria.[58] Most of the vessels operated within Germany's exclusive economic zone (EEZ) during the incidents.

The picture is further complicated by the possibility that some of the Russian-linked vessels and/or shadow fleet operated as a network relay system – with one or two vessels deploying and recovering drones and a third providing signals intelligence to give the UAV and its operator targeting data. More recently, on 26 February 2026, an unauthorised drone launched from the Russian *Alpinist*-class (Project 503R) signals intelligence vessel *Zhigulevsk* during the *Charles de Gaulle* port visit to Malmö. The *Zhigulevsk* entered Sweden's 12-nautical-mile (about 22km) territorial waters and the UAV was neutralised about seven miles (12km) from the carrier's anchorage.[59] The incident was notable considering the pace with which the threat was identified.[60]

Where land-based operations have relied on low technology and untrained local proxies sufficient for arson and simple sabotage, UAV operations require a degree of specialised training. This creates a different challenge as skilled operatives are harder to explain and conceal than disposable recruits. Russian-linked vessels, including the shadow fleet, resolve this problem by providing effective cover for skilled operatives while also serving as convenient launch and recovery platforms – reinforcing the strategic advantages of sea-based hybrid activity.[61]

Depending on the type of UAV, it could be catapult-launched, hand-launched or VTOL. China has configured

Map 2.2: **Positions of selected Russian shadow-fleet tankers around Denmark, 22 September 2025**

AIS = Automatic Identification System; **UAV** = uninhabited aerial vehicle
Note: Copenhagen Airport was closed due to UAV sightings at 5.26pm UTC.
Source: Global Fishing Watch

medium cargo vessels as drone carriers using comparable methods[62] and all three approaches are practicable on the large open decks of shadow-fleet tankers. The UAV would likely be piloted from either the launch vessel or a second ship acting as a signals relay. The flat terrain of the Netherlands and northern Germany, where most sightings occurred, would allow signals to pass unimpeded from a vessel in the North Sea to a UAV operating several hundred kilometres inland. The UAV could subsequently be recovered aboard ship using a net, or possibly deliberately ditched in the North Sea, eliminating any physical evidence of its use.

In September 2025, the French military boarded and detained the shadow-fleet vessel *Boracay* on suspicion of acting as a launchpad for drones which were seen over Denmark that month.[63] The first incident occurred on 22 September 2025, when two or three UAVs were seen by an air traffic controller over Copenhagen Airport, leading to the closure of the airport from 7.26pm local time (5.26pm UTC) for around four hours.[64]

Map 2.3: **Positions of selected Russian shadow-fleet tankers around Denmark, 24 September 2025**

AIS = Automatic Identification System; **UAV** = uninhabited aerial vehicle
Source: Global Fishing Watch

Figure 2.3: **The *Arctica* anchored offshore Fredericia, Denmark, approximately 200 km from Copenhagen (55.576368, 9.883213), 23 September 2025**

Source: satellite imagery ©2026 Vantor

Map 2.2 shows the positions of Russian shadow-fleet ships around Denmark at the time of the incident.

Two days later, on 24 September, UAVs were sighted over the Copenhagen area in the early hours of the morning local time on 23 September by eyewitnesses in Brøndby Strand at 1.14am (11.14pm UTC), then on 24 September at Hvidore at 2.30am (12.30am UTC) and Amager at 2am (12am UTC). That night, UAVs were sighted by workers at Esvagt[65] flying over the North Sea. At Aalborg Airport, UAVs were seen at 9.44pm (7.44pm UTC),[66] and a few minutes later reports were made of UAV activity near the southerly airports Esbjerg, Skrydstrup and Sønderborg. At Aalborg, the UAVs 'flew over a very large area over a couple of hours',[67]suggesting that they were military-grade UAVs equipped for long endurance flights. Map 2.3 shows the shadow-fleet ship traffic around Denmark.

In Maps 2.2 and 2.3, the *Boracay*, the ship implicated in these incidents by France, can be seen moving from the Baltic to the North Sea around the northern tip of Denmark. Other ships on similar paths include the *Sea Maverick* (IMO 9265885) and *Jin Hui* (IMO 9430272), the latter seized by Sweden on 3 May 2026 and the captain arrested on suspicion of using false documents relating to its flying of the Syrian flag.[68]

Also nearby were ships *Arctica* (IMO 9305556) and *Vladimir Rusanov* (IMO 9750701), both of which were docked in Denmark at the time. Figure 2.3 shows satellite imagery of the *Arctica* anchored near the Danish town of Fredericia. At the northern port of Skagen, the *Vigo* (IMO 9208136) was docked.

According to AIS data, the *Arctica* was also transiting around Denmark earlier in the year, on 3 January 2025, when 20 drones were reported flying over the port of Køge.[69] An eyewitness described the drones disappearing 'out towards the harbour and beyond the sea'.[70]

Map 2.4: **Positions of selected Russian shadow-fleet tankers around Denmark, 3 January 2025**

AIS = Automatic Identification System; **UAV** = uninhabited aerial vehicle
Source: Global Fishing Watch

During the time of this incident, the movements of the tanker *Mulan* (IMO 9340465) between Norway and Denmark showed an unusual zigzag pattern, which it had been sailing since 26 December 2024. This area of the North Sea hosts several underwater telecommunications cables which connect Norway and Denmark. The vessel was contacted by the Norwegian Coastal Administration on 28 December and claimed they were waiting for better weather conditions, before leaving on 4 January 2025.[71] The ship is owned by sanctioned company Plio Energy, which has engaged in deceptive practices like shutting off its AIS for ship-to-ship transfers to sanctioned vessels.[72]

Incidents Over US and NATO Air Bases

One of the earliest incidents in our dataset occurred in Germany on 26 November 2024, when UAVs were sighted over Ramstein, which serves as the headquarters of both the US Air Forces in Europe–Air Forces Africa[73] and NATO Allied Air Command.[74] UAV flights over the base continued into early 2025. Reports documenting the November incidents indicate the UAVs were likely launched from Russian-linked vessels operating in the North Sea or Baltic Sea.[75]

During this operational window, between 20 and 26 November 2024, sophisticated UAVs were also observed operating over several US air bases in the UK, including RAF Fairford, Feltwell, Lakenheath and Mildenhall. RAF Lakenheath is a highly sensitive

Map 2.5: **Positions of selected Russian shadow-fleet tankers around Germany and the UK, 26 November 2024**

AIS = Automatic Identification System; **UAV** = uninhabited aerial vehicle
Note: The time of UAV sightings is unknown.
Source: Global Fishing Watch

site reportedly undergoing preparations to house US nuclear weapons.[76] [77] Following a public appeal for information, approximately 170 sightings were reported, of which around half were considered credible, either corroborated by multiple witnesses or supported by imagery that could not be deconflicted with known air traffic. Operational security appeared sophisticated. The UAVs entered the airspace around the RAF bases at low altitude with their lights visible and departed at higher altitudes. Arrival and departure directions varied across the incident period. Witness reports indicate more than one platform type may have been involved. Some observations were consistent with multirotor UAVs; others with fixed-wing platforms. The propulsion noise of the UAVs was inconsistent across accounts, with some observers describing sounds more typical of petrol engines than electric motors. By coincidence, the *Hav Dolphin*, a ship that was likely involved in a UAV incident in Germany in 2025, was docked in the UK at the time of the incidents.

Kleine-Brogel Air Base in northeast Belgium, which houses US nuclear weapons, saw a series of incursions in early November.[78] Over three consecutive nights, UAVs repeatedly entered the airspace around the base, while simultaneous sightings were reported over the military facility in Leopoldsburg. Belgian Defence Minister Theo Francken publicly stated the incidents resembled a spy operation.[79] Small UAVs were used to test the radio frequencies of Belgian security services, which allowed the operators to bypass countermeasures when larger drones were subsequently sent in; as Francken noted, the base's jammers failed because the operators adapted to the frequencies, concluding that 'an amateur doesn't know how to do that'.[80]

Volkel in the Netherlands was targeted by UAVs on at least three separate days in November and December 2025. Volkel is a highly sensitive site because it hosts dual-capable aircraft tasked with delivering US forward-deployed B61-12 gravity bombs under NATO's nuclear-sharing arrangements.[81] Volkel is located deep inland; to reach it from the sea, UAVs would have had to bypass closer, more accessible coastal targets such as naval dockyards and other air bases, demonstrating a highly motivated and deliberate effort to survey NATO's nuclear-deterrence infrastructure.

The most significant of the UAV flights occurred on the evening of 21 November 2025, when a highly coordinated flight of UAVs flew into Dutch airspace between 7pm and 9pm local time (6pm and 8pm UTC). During this period, up to ten UAVs were spotted operating directly over Volkel. Base security personnel engaged the UAVs, using ground-based weapons to shoot them down. However, open-source reporting suggests the UAVs successfully evaded a direct hit, and no wreckage was recovered. This wave of UAVs simultaneously disrupted the civilian aviation sector, as UAVs were also sighted operating over Eindhoven Airport during the same time frame.[82] Eindhoven serves as a major European commercial transport hub and co-hosts the Royal Netherlands Air Force's transport and aerial refuelling aircraft; the resulting security alerts forced a brief suspension of civil air traffic across the southern Netherlands, inflicting further economic and logistical friction.

Incursions at Volkel continued into the following month. On the morning of 7 December, a drone was sighted operating near the base, prompting two F-35As (which were airborne at the time) to chase the unidentified UAV until it left Dutch airspace. The UAV incidents suggest a deliberate effort to evaluate NATO's integrated air-defence protocols. Belgium and the Netherlands formally share airspace protection responsibilities, employing a joint QRA system where they take turns policing the skies for classic air threats.

Maritime tracking data from these incident windows is consistent with the shadow-fleet launch hypothesis. As illustrated in Map 2.6, during the November incursions over Volkel and Eindhoven, multiple suspicious vessels including the *Arctica*, the *Cgas Leopard* (IMO 9578012), and the *Tranquil Sea* (IMO 9323340), also known as the *Eagle S*,[83] were loitering in international waters and at anchorages off the Dutch and French coasts near Rotterdam and Dunkirk. Three days after the incident, on 14 November, the *Tranquil Sea* changed flag from Honduras to Sierra Leone. The presence of these vessels aligns with the geographic and temporal distribution of the UAV flights, providing a plausible offshore launch and recovery platform capable of penetrating deep into European airspace.

Map 2.6: **Positions of selected Russian shadow-fleet tankers around the Netherlands, 21 November 2025**

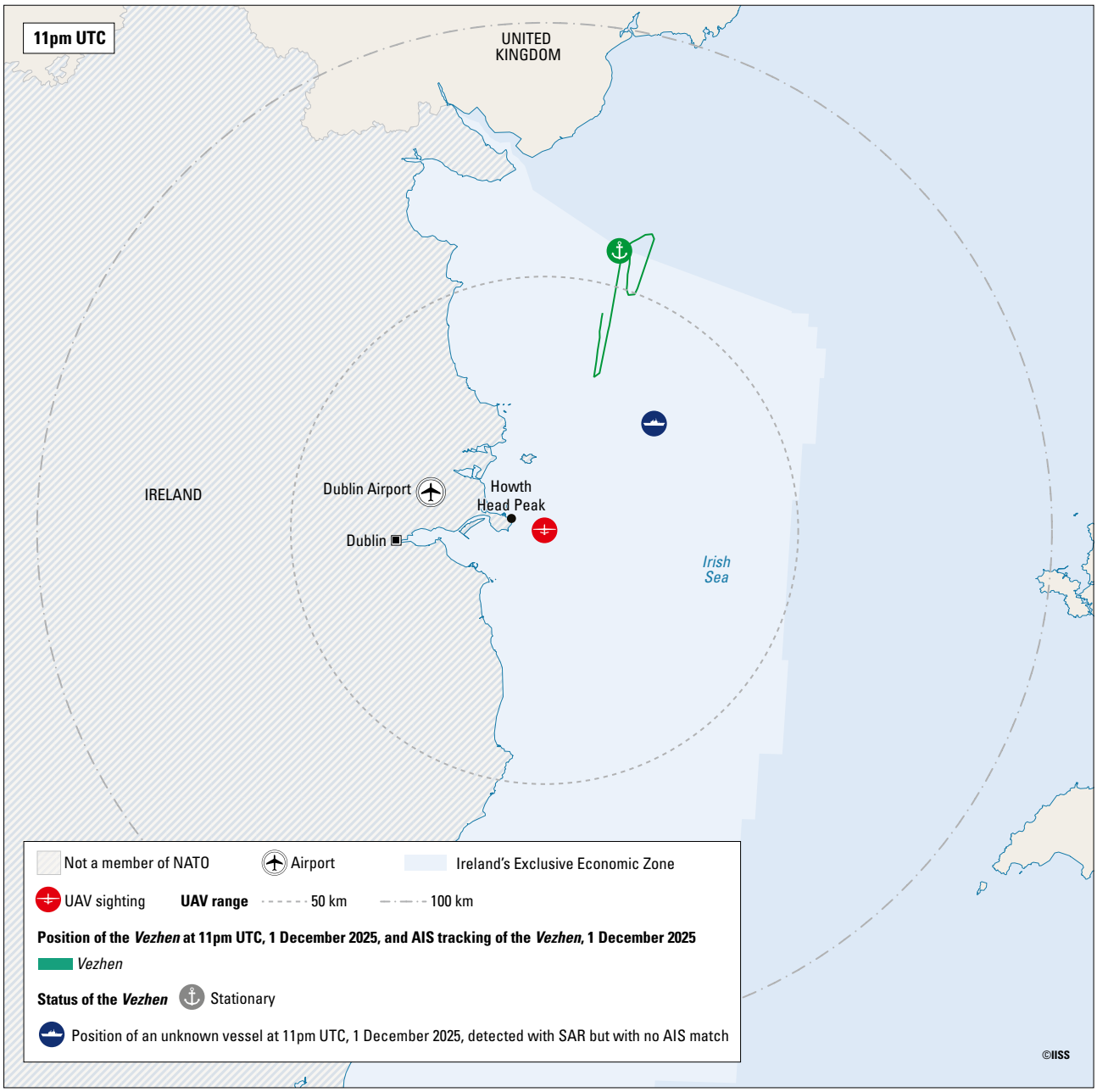
AIS = Automatic Identification System; **UAV** = uninhabited aerial vehicle
Notes: UAVs were sighted between 6pm and 8pm UTC. No AIS data is available for the *Cgas Leopard* during this period.
Source: Global Fishing Watch

AIS Blackouts

On 1 December 2025, Ukrainian President Volodymyr Zelenskyy arrived at Dublin Airport for his first official visit to Ireland. Ireland had, earlier in the year, donated a substantial portion of its ageing *Giraffe Mark IV* air-defence systems to protect towns and cities in Ukraine from Russian aerial attacks, demonstrating the commitment of the Irish government to assisting Ukraine with non-lethal capabilities.[84] At around 10.30pm UTC, four UAVs were spotted in the air off the coast of Dublin. The UAVs were described as 'large, hugely expensive, of military specification' and flew for up to two hours over the Irish Navy ship LÉ *William Butler Yeats*. By the time its crew had spotted the UAVs, they were heading towards the Irish coast. Given the location of the UAVs, which would have meant the ship's weapons pointing towards the Irish coast, the decision was made not to fire at them.[85]

At the time of the incident, the Maltese-flagged ship *Vezhen* (IMO 9937270) was loitering inside the

Map 2.7: **Position of the *Vezhen* and an unknown vessel in the Irish Sea, 1 December 2025**



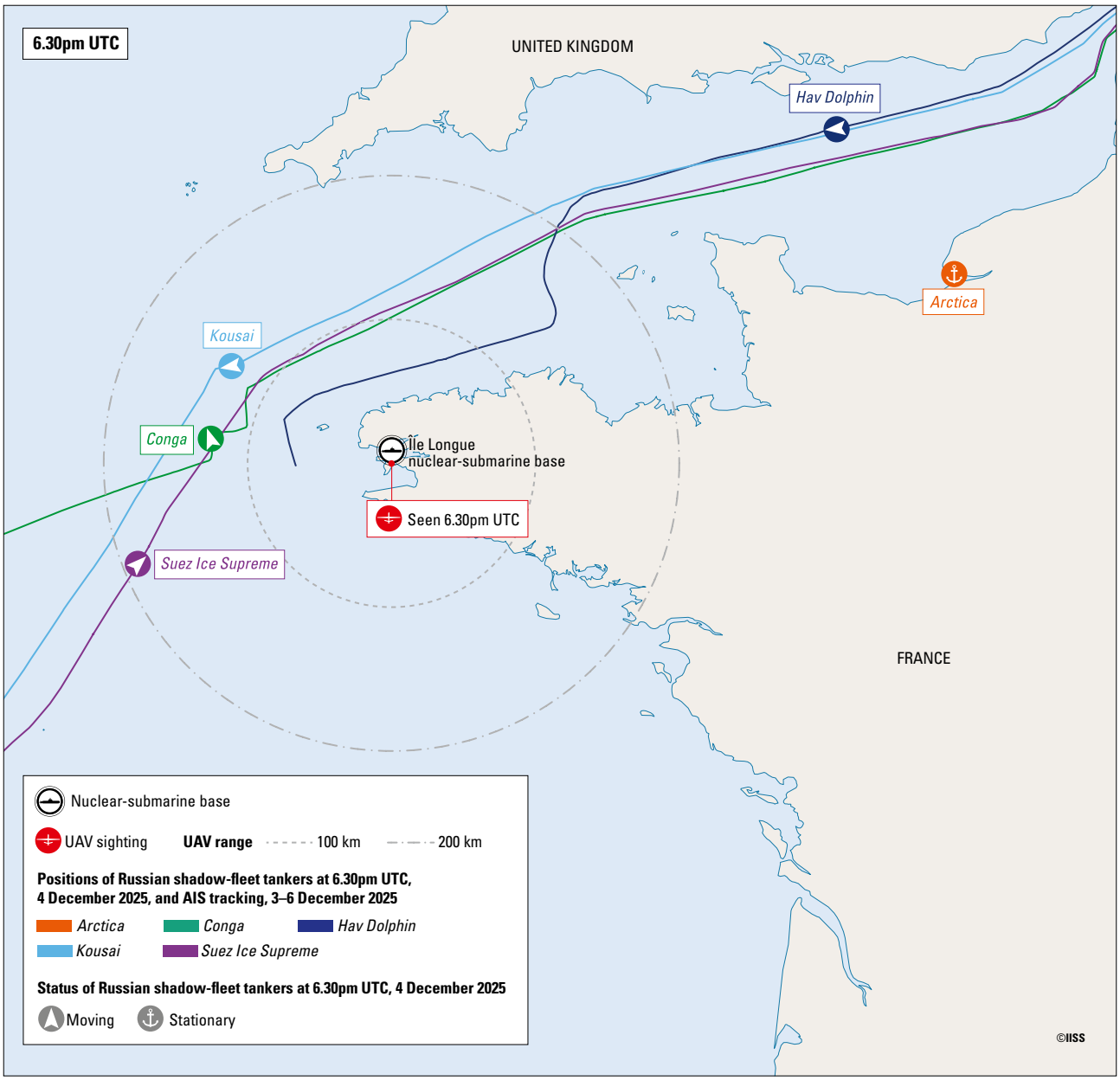
AIS = Automatic Identification System; **SAR** = Synthetic Aperture Radar; **UAV** = uninhabited aerial vehicle
Sources: Global Fishing Watch, Marine Regions

Irish EEZ, approximately 60 km from the location of the UAVs. The *Vezhen*, owned by Bulgarian company Navigation Maritime Bulgare, was previously seized and its crew detained by Swedish authorities on 27 January 2025 in connection with damage to Baltic undersea fibre-optic cable.[86] The vessel was released after the incident was deemed to be accidental.[87] The *Vezhen* entered Ireland's EEZ around 8am UTC and loitered for the next three days before departing on the evening of 4 December.

Also in the Irish Sea at the time of the UAV incident was another ship, visible on SAR imagery but not on AIS. The ship was located less than 40 km from the *William Butler Yeats*. Map 2.7 shows the tracks from the *Vezhen* and the position of the unidentified ship.

Finally, in early December 2025, French officials detected five UAVs over the Île Longue nuclear-submarine base in Brittany. The submarines there are equipped with the bulk of the country's nuclear stockpile of submarine-launched ballistic missiles (SLBMs). The five UAVs were detected

Map 2.8: **Positions of selected Russian shadow-fleet tankers around France, 4 December 2025**



AIS = Automatic Identification System; **UAV** = uninhabited aerial vehicle
Source: Global Fishing Watch

around 7.30pm local time (6.30pm UTC) on 4 December. Visibility was noted to be unusually clear at the time of the incident owing to a full supermoon. It's likely the UAV overflight was a surveillance activity, as this followed the operationalisation of the M51.3 SLBM on 24 October 2025.[88] Notably, the *Hav Dolphin* was approximately 350 km from Île Longue at 7.30pm local time (6.30pm UTC), when the UAVs were seen. The *Marven*, the name at the time for the *Arctica*, was docked approximately 370 km away. The closest ships were *Kousai* (IMO 9285835), *Conga* (IMO 9412000) and *Suez Ice Supreme* (IMO 9296418). The closest of these, the *Conga*, was just over 100 km away.

French authorities opened a formal investigation the following day. However, despite concerns over the reconnaissance of a nuclear submarine base, French officials have not attributed the incident to a state actor. This cautious posture mirrors the response to previous incidents across France and the rest of Europe between late 2024 and December 2025. While maritime tracking data during the incident windows consistently identifies the presence of suspicious vessels previously implicated in UAV activity, such as the *Hav Dolphin*, within a few hundred kilometres of the coast, the evidence remains circumstantial.

3. Europe's Response

The Kremlin's UAV campaign in late 2025 over Europe achieved a strategic effect that very likely exceeded its operational cost. Based on open-source reporting, and from the perspective of how European governments responded to the UAV incidents, the Kremlin was likely able to map reaction times, coverage gaps and limitations across European integrated air defences. While NATO's response to the UAV incursion across Polish airspace demonstrated its response time and capability, it also highlighted the cost-exchange ratio that could deplete Western interceptor stockpiles faster than governments replenish them.[89]

Open-source reporting of each incident in the IISS dataset suggests the Kremlin's campaign exposed political fractures within the Alliance, exploiting the gap between what European militaries could do and what their governments were prepared to authorise. And the campaign demonstrated, repeatedly and publicly, that the threshold for collective punishment was higher than European deterrence postures have previously assumed.[90]

Following the UAV incidents, some European governments reviewed their legislation and institutional frameworks. In Germany, the Bundeswehr were only legally authorised to shoot down UAVs if they were flying directly over military installations, leaving the protection of airspace strictly to law enforcement. Following numerous incidents, the authorities approved an amendment explicitly allowing the police to shoot down UAVs,[91] while Dobrindt suggested new legislation to permit the military to engage suspicious aircraft outside of designated military zones.[92] The legislative push was reinforced by institutional consolidation. Dobrindt announced the creation of a joint national UAV defence centre (Drohnenabwehrzentrum) designed to bring together the competencies of the federal police, state authorities and Bundeswehr. The new centre aims to establish a shared threat picture and formalise a rapid, unified response to the escalating drone threat, effectively bridging the perilous gap between civilian law enforcement and military air defence.

The response by UK and US authorities to the November 2024 incidents around Lakenheath illustrated a distinct set of operational constraints. Similarly to the Belgian incidents, RF jammers proved ineffective. In one case, a police helicopter attempted to track the UAVs but was stood down over safety concerns. The deployment of an anti-UAV directed-energy weapon was suggested but ultimately not progressed.

NATO's Innovation Range for uninhabited systems in Latvia became operational in March 2026, while the Netherlands hosted a drone and counter-drone exercise in May 2026. An EU Counter-drone Centre of Excellence is planned for Geel, Belgium, by early 2027. While each of the examples represents genuine political will and, in some cases, real investment, an overriding lesson of Europe's response to Russia's unconventional war is not to mistake activity for achievement.

A number of European NATO allies have formally declared they would use force to defend their airspace against future incursions. Lithuania, for example, explicitly authorised the peacetime shootdown of drones crossing its borders.[93] Romania established specific legal frameworks through Law 73/2025, granting its military explicit authorisation to intercept and destroy hostile drones while providing guidelines to manage the risks of civilian collateral damage.[94]

The UAV incursion into Polish airspace in September 2025 prompted Warsaw to invoke Article 4 (Members will consult together whenever territorial integrity is threatened) for the eighth time in NATO's history. In response, the Alliance launched *Operation Eastern Sentry*[95] on 12 September to reinforce its integrated air and missile defences from the Baltic to the Black Sea. The new mission built on the framework established by *Operation Baltic Sentry*, initiated in January 2025 to deter Russian maritime sabotage and shadow-fleet operations following the sabotage of Baltic undersea cables.

Operation Eastern Sentry has been described as an improvised shield rather than a coherent strategy. It is likely to have first and foremost been designed as a

deterrence signal given the temporary reallocation of assets already deployed by participating nations and the lack of a dedicated budget, separate legal mandate, or new command structures.[96]

Political Authority and Escalation Risk

European governments have responded to the Kremlin's UAV campaign with neither unity nor consistency. Some, like Poland, showed willingness to act: Prime Minister Donald Tusk declared that the Polish Armed Forces would 'shoot down all flying objects when they violate our territory and fly over Poland'.[97] Others remained politically hesitant, constrained by strict rules of engagement, the imperative to avoid civilian casualties, and fears of escalation. NATO's official position compounded the incoherence. Secretary General Mark Rutte maintained that the Alliance would not shoot down drones as a matter of policy, describing restraint as 'a proportionate response',[98] a stance directly at odds with Tusk's position, and one that sat uneasily alongside the broader reliance on ambiguity that Rutte articulated. Whatever its intent, that posture likely raised the Kremlin's tolerance for risk and reinforced its confidence that European governments would not enforce red lines with action. The absence of a unified approach has undermined NATO's ability to project power.

Recognising the cost of this self-deterrence, NATO Military Committee Chair Admiral Giuseppe Cavo Dragone said in late 2025 that the Alliance was evaluating 'being more aggressive or being proactive instead of reactive', and he suggested that pre-emptive action against Russian 'hybrid infrastructure' could, in certain circumstances, constitute defensive action.[99] His remarks provoked condemnation from the Kremlin, with Russia's Foreign Ministry spokesperson Maria Zakharova calling them 'extremely irresponsible', and internal discomfort within the Alliance, with Italy publicly distancing itself from Cavo Dragone's position.[100] The episode illustrated the core dilemma facing the Alliance: credible deterrence-by-punishment requires pre-agreed escalation ladders but constructing them demands a political consensus that did not and does not currently exist – not least because European governments are still unsure how to respond.

For example, a Russian *Geran* one-way attack UAV entered Romanian airspace in September 2025 during an attack on Ukrainian infrastructure along the Danube. The drone penetrated roughly 10 km inland and operated for nearly 50 minutes before disappearing from radar approximately 20 km southwest of Chilia Veche.[101] Two Romanian F-16 fighter jets scrambled from Fetești Air Base intercepted and tracked the UAV.

Under the newly established Romanian Law 73/2025, the pilots had legal authorisation to destroy the UAV, and Defence Minister Ionuț Moșteanu confirmed that the pilots 'were very close to bringing it down' before the UAV departed towards Ukraine. The Romanian General Inspectorate for Emergency Situations, however, cited the unacceptable risk that falling debris or explosive blast effects could harm civilians – who had been issued RO-Alert warnings, under Romania's national emergency public-warning system, in northern Tulcea County to seek shelter – as the primary reason for their restraint.[102] The incident happened just days after Polish forces shot down Russian UAVs, exposing contrasting national responses and interpretations of Alliance protocol. The Romania–Poland contrast made those disagreements visible to everyone, and Russian information operations quickly amplified the perception of Alliance disarray by portraying NATO as indecisive and incapable of protecting its Eastern members.[103]

The Economics of UAVs and European Air Defence

Restoring economic sustainability to European air defence requires not just the procurement of cost-effective counter-UAV systems but their integration under a unified command-and-control architecture. There has been some progress with the procurement of capability. Poland and Romania received the first deployments of the US-made Merops system in November 2025 – battle-tested in Ukraine, where it has accounted for an estimated 40% of Russian *Shahed* drones destroyed.[104] Denmark has indicated its intention to purchase the system. Separately, NATO's *Bold Machina* exercise in the Netherlands demonstrated a passive detection prototype integrating multiple sensor platforms using artificial intelligence to identify drones. However, a simulation of hybrid attack scenarios conducted in April

2026 highlighted the challenge: UAV and electronic warfare operations compress decision timelines, obscure attribution and blur the division between civilian disruption and military effect, making collective action harder at precisely the moment it is most needed.[105]

In an attempt to forge a unified response, European Commission President Ursula von der Leyen proposed the establishment of a drone wall, officially rebranded as the EDDI, which is intended to be fully functional by the end of 2027.[106] The EDDI is envisioned as a continent-wide, multi-layered network of radar, acoustic and radio-frequency sensors integrated with electronic jamming systems and kinetic interceptors. However, a number of political, geographic and operational challenges undermine its viability.

Internally, the EDDI has exposed divisions among EU member states regarding funding mechanisms, technical feasibility and the centralisation of defence authority. Reflecting this scepticism, French President Emmanuel Macron explicitly dismissed the proposal as 'more sophisticated, more complex than suggested',[107] while German Defence Minister Boris Pistorius rejected the concept entirely at the Warsaw Security Forum, stating Europe needs drone defence, but not by a drone wall, noting it cannot realistically be built within the next three to four years.[108] Although the commission shifted the project's branding to the EDDI to emphasise a 360-degree network rather than a physical barrier, the differences among European leaders meant the initiative entered its early phases with no consensus on funding and scope.[109]

The European Parliament identified a further three structural challenges, warning of the unsustainably high cost of drone interceptions, that lengthy certification, procurement and testing processes risk making EU capabilities obsolete by the time they are deployed, and that doctrinal and operational gaps between EU and NATO drone defence remain unabridged.[110] These are not minor challenges, and the Kremlin's campaign has exposed the gap between, for example, a threat that is evolving over weeks and a procurement process measured in years.

Furthermore, the EDDI arguably doesn't address the threat of drones launched *within* Europe or from waters off the coast of Europe. Following the expulsion of trained intelligence officers, Russian services now rely on a decentralised gig-economy model, using encrypted apps like Telegram to recruit low-level criminals, vulnerable migrants and disposable agents.[111] These proxies can easily purchase commercial-grade drones and deploy them near critical infrastructure, including military bases and airports. For example, in the UK, there were reports of multiple unidentified UAV flights around RAF Fairford, Lakenheath and Mildenhall in November 2024. According to reports, the flights around RAF Lakenheath described the incidents as large 'non-hobby'-sized UAVs. Despite only a handful of blurry photographs of possible UAVs, a possible explanation is reconnaissance of sensitive infrastructure, including facilities linked in open sources to preparations for a potential future nuclear mission. This remains unconfirmed.[112]

Conclusion

The Kremlin's tactical successes rest on the basic strategic insight that Europe's air-defence architecture was designed for a different era and built to detect and defeat conventional air threats operating in a recognisable battlespace. It was not developed for repeated, low-cost and deniable incursions with the aim of exposing gaps in detection, decision-making and legal authority while remaining below the threshold of collective allied response.

Assessing the Kremlin's UAV campaign requires looking beyond what European governments would typically accept as measures of success. No UAVs were recovered intact at the nuclear sites they flew over, no operatives were apprehended launching UAVs from shadow-fleet vessels, and only the *Zhigulevsk* incident involving the *Charles de Gaulle* resulted in a public attribution to a specific Russian UAV. The incident validates a much broader vulnerability: by proving that maritime UAV launches are technically and operationally feasible, it also confirms that Russian-linked vessels, and the shadow fleet, could readily serve as a network of mobile signal and reconnaissance platforms operating inside European waters.[113]

Looking at the campaign from the perspective of the Kremlin, one could determine that the value lies in what European governments and NATO disclose. The campaign is likely to have generated operational value to Russian planners: radar exposure, reaction times, interception corridors, rules-of-engagement thresholds and the geography of NATO's reinforcement routes across Europe and to Ukraine. Most importantly, the campaign highlights the visible gap between military capability and political willingness to act. The pattern documented in this report – 144 incidents across 13 European states, clustered around nuclear-related sites, Ukraine-support infrastructure and major commercial aviation hubs – is consistent with a coherent deniable Russian campaign.

The evidence most strongly supports aims one and three of the campaign – reconnaissance by battle and economic attrition combined with psychological warfare – as the primary strategic logic of the campaign. The concept of reconnaissance by battle explains not only the incidents where UAVs succeeded in their apparent missions but also those where they were intercepted or jammed since, under that doctrine, allied responses are themselves the intelligence product. The campaign's fourth aim is assessed as equally highly likely as a concurrent objective as it generated sustained political anxiety, imposed disproportionate defensive costs, and normalised airspace violations at a level that European governments were unable to respond to.

The clustering of incidents around nuclear-sharing sites and Ukraine-support infrastructure is too consistent to be coincidental, suggesting aim two of the campaign, mapping critical infrastructure, including facilities associated with allied nuclear deterrence and military logistics nodes supporting Ukraine, is likely valid as a specific ISR targeting priority. One further uncertainty bears stating explicitly: whether the campaign reflects centralised Kremlin direction or the convergent behaviour of competing Russian intelligence agencies the FSB, GRU and Foreign Intelligence Service, pursuing parallel objectives in a culture of competitive signalling, cannot be resolved from open sources alone. Privately, some European governments assess the orchestration as too coherent for pure coincidence, hence the assessment this was a Kremlin-led campaign – but this assessment is only made with medium confidence.

The maritime dimension is the most important unresolved vulnerability. If Russian-linked vessels can launch, support or relay UAV operations from international waters or European EEZs, they can complicate attribution, exploit commercial cover and avoid the warning indicators associated with land-border incursions. AIS manipulation, flags of convenience, opaque ownership and specialist personnel aboard commercial vessels increase the burden on European investigators and slow down political response. European counter-drone initiatives have also conspicuously failed to account for the maritime dimension.[114]

Despite European governments moving relatively quickly to adapt their responses to UAV incidents, there remain a number of gaps. Firstly, legal frameworks governing UAV interception remain fragmented across civil aviation, domestic law enforcement and military rules of engagement. Secondly, the current response is economically unsustainable, and it will continue to be so until new capability is built and fully functional. The September 2025 response over Poland illustrated the asymmetry with particular clarity. Finally, even as the EDDI has broadened, it remains an initiative focused on the eastern flank, while the incidents in the dataset point to challenges created by UAVs being launched in the maritime domain or inland.

Authorising advanced military assets against a UAV of uncertain origin over civilian airspace and, in some cases, over densely populated areas requires decisions that European governments have proven reluctant to take quickly, consistently or in coordination. The path to a credible European response requires legal clarity. The first point to note is that 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. The second is economic rebalancing: until the cost-exchange ratio is inverted, European governments risk relying on an expensive and finite response – the EDDI will go some way to managing this but will not be functional for a number of years. The third, and hardest, is maritime accountability. As long as Russian-linked vessels and the shadow fleet can loiter in international waters or European EEZs and launch UAVs with effective impunity, the campaign's primary enabling mechanism remains intact. The *Zhigulevsk* incident demonstrated that attribution is possible. The question is whether European governments are prepared to act on it.

Notes

1 For example, Germany registered more than 1,000 suspicious UAV flights in 2025; Holger Münch, chief of the Federal Criminal Police Office (BKA), attributed the drones to a state actor aiming to sow uncertainty but stopped short of attributing all sightings to Russian UAVs.

2 'Drones Seen Near Air Base Storing U.S. Nuclear Weapons Resemble "Spy Operation," Belgium's Defense Minister Says', CBS News, 3 November 2025, https://www.cbsnews.com/news/drones-near-belgium-air-base-storing-us-nuclear-weapons-spy-operation/.

3 See, for example, European Union Aviation Safety Agency and EUROCONTROL, 'EASA and EUROCONTROL release Electronic Conspicuity Use Cases for Safer Shared Airspace', EASA, 20 May 2026, https://www.easa.europa.eu/en/newsroom-and-events/news/easa-and-eurocontrol-release-electronic-conspicuity-use-cases-safer-shared#group-easa-downloads.

4 Wiebe de Jager, '61 European Drone Sightings Analysed: Here's What We Know', Dronewatch Europe, 29 November 2025, https://www.dronewatch.eu/61-european-drone-sightings-analysed-heres-what-we-know/.

5 'Kronvidne i drone-sag: Politiet siger, at det ikke var droner' [Key Witness in Drone Case: Police Say it Wasn't Drones], Frihedsbrevet, 18 March 2026, https://frihedsbrevet.dk/hun-var-den-frste-til-at-se-droner-over-kbenhavns-lufthavn-nu-deler-hun-politiets-konklusion-det-var-ikke-droner/.

6 European Union Aviation Safety Agency, 'Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and 2019/945), https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu.

7 Charlie Edwards and Nate Seidenstein, 'The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure', IISS, 19 August 2025, https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/.

8 Keir Mather MP, 'The Growing Risks to Maritime Safety', Department for Transport, UK Government, 26 January 2026, https://www.gov.uk/government/publications/the-growing-risks-to-maritime-safety/the-growing-risks-to-maritime-safety.

9 Spencer Faragasso, 'Russian Military UAV Used in Ukraine Depends on Foreign Parts', Institute for Science and International Security, 11 May 2022, https://isis-online.org/isis-reports/russian-military-uav-used-in-ukraine-depends-on-foreign-parts; Rosoboronexport, 'Orlan-10E', Rosoboronexport official product catalogue, https://roe.ru/en/production/aerospace-forces/complexes-with-uavs/orlan-10e/#.

10 Paul Kirby, 'Drone Jammed Near French Aircraft Carrier Was Probably Russian, Says Sweden', BBC News, 27 February 2026, https://www.bbc.co.uk/news/articles/c1mj3e2nz8ko.

11 IISS, 'The Uninhabited War in Ukraine', in *UAVs: ISR, Deterrence and War* (IISS, 2026), https://www.iiss.org/globalassets/media-library---content--migration/files/publications---free-files/strategic-dossier/uavs-2026/iiss_ch-3-uavs-isr-deterrence-and-war_032026.pdf.

12 'ORLAN: Unmanned High-Precision Aerial Survey Complex for Russian Territory', https://gnss.spb.ru/orlan/orlan-bespilotnyj-ositel.

13 Dylan Malyasov, 'Russian Heavy Spy Drone Crashes in Turkey', *The Defence Blog*, 20 December 2025, https://defence-blog.com/russian-heavy-spy-drone-crashes-in-turkey/.

14 Andrew Radin et al., *Lessons from the War in Ukraine for Space: Challenges and Opportunities for Future Conflicts*, RAND Corporation, 2025, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2950-1/RAND_RRA2950-1.pdf.

15 European Parliament, 'Drones and New Systems of Warfare – the EU's Need to Adapt to Be Fit for Today's Security Challenges', 22 January 2026, https://www.europarl.europa.eu/doceo/document/TA-10-2026-0020_EN.html.

16 Tamsin Paternoster and Noa Schumann, 'Fact-checking Europe's "Drone Problem": Why Are Airports Closing?', Euronews, 20 November 2025, https://www.euronews.com/my-europe/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shuttering-over-drone-sightings.

17 Aleksandar Brezar, 'Denmark's Aalborg Airport Closes Again over Another Suspected Drone "Hybrid Attack"', Euronews, 26 September 2025, https://www.euronews.com/2025/09/26/denmarks-aalborg-airport-closes-again-over-suspected-drone-hybrid-attack.

18 'Training of Ukrainian F-16 Personnel Is Moving Along', Defence Command Denmark, https://www.forsvaret.dk/en/news/2024/eng-f-16-og-ukrainere/.

19 'Denmark Links Drones at Copenhagen Airport to Hybrid Attacks across Europe', CNN, 23 September 2025, https://www.cnn.com/2025/09/23/europe/denmark-drones-hybrid-attacks-intl.

20 'Estonian Navy Detains Stateless Tanker with Dozens of Deficiencies', The Maritime Executive, 13 April 2025, https://maritime-executive.com/article/estonian-navy-detains-stateless-tanker-with-dozens-of-deficiencies.

21 David Brennan, 'Mystery Drones Over Denmark Are "Hybrid Attack", Defense Minister Says', ABC News, 25 September 2025, https://abcnews.com/International/mystery-drones-denmark-hybrid-attack-defense-minister/story?id=125918649.

22 *Ibid*.

23 Tejaswini Deshmukh, 'Denmark Police Launch Investigation After Mysterious Drones Appear over Køge Harbor', Regtechtimes, 6 January 2025, https://regtechtimes.com/denmark-police-launch-investigation-after-myster/.

24 Danish Ministry of Defence, 'Største danske udsendelse af mandskab og materiel i Europa i 23 år' [Largest Danish Deployment of Personnel and Equipment in Europe in 23 Years], 24 April 2022, https://www.fmn.dk/da/nyheder/2022/storste-danske-udsendelse-af-mandskab-og-materiel-i-europa-i-23-ar/.

25 Hugh Schofield and Aleks Phillips, 'Captain of Tanker Linked to Russian "Shadow Fleet" Charged', BBC News, 2 October 2025, https://www.bbc.co.uk/news/articles/cqxz1wvqvzqo.

26 'France Sentences Chinese Captain of Suspected Russian "Shadow Fleet" Tanker to One Year in Jail', *Le Monde*, 30 March 2026, https://www.lemonde.fr/en/france/article/2026/03/30/france-court-sentences-chinese-captain-of-suspected-russian-shadow-fleet-tanker-to-one-year-in-jail_6751941_7.html.

27 Jana Tauschinski and Sam Jones, 'Russia's Hybrid Warfare Puts Europe to the Test', *Financial Times*, 9 December 2025, https://www.ft.com/content/2084e87d-d491-4852-8449-f90b73d4788b?syn-25a6b1a6=1. See also Michael Kofman et al., 'Russian Military Strategy: Core Tenets and Operational Concepts', CNA, https://www.cna.org/analyses/2021/10/russian-military-strategy-core-tenets-and-concepts.

28 Ivan U. Kłyszcz and Marek Kohv, 'Confronting the Russian Hydra: Continuity and Innovation in the Grey Zone', International Centre for Defence and Security, 15 December 2025, https://icds.ee/en/confronting-the-russian-hydra-continuity-and-innovation-in-the-grey-zone/.

29 Will Brown et al., 'From Shield to Sword: Europe's Offensive Strategy for the Hybrid Age', European Council on Foreign Relations, 6 March 2026, https://ecfr.eu/publication/from-shield-to-sword-europes-offensive-strategy-for-the-hybrid-age/.

30 Michael Kofman et al., 'Russian Military Strategy: Core Tenets and Operational Concepts'.

31 Clint Reach, Alexis A. Blanc and Edward Geist, 'Russian Military Strategy: Organizing Operations for the Initial Period of War', RAND Corporation, 22 November 2022, https://www.rand.org/pubs/research_reports/RRA1233-1.html.

32 Charlie Edwards, 'The Paradox of Russian Escalation and NATO's Response', IISS, 26 September 2025, https://www.iiss.org/online-analysis/online-analysis/2025/09/the-paradox-of-russian-escalation-and-natos-response/.

33 Christopher Solomon, 'Russian Offensive Campaign Assessment, September 10, 2025', Institute for the Study of War, 11 September 2025, https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment-september-10-2025/.

34 '"Immediately Clarify the Incident" – Home Damaged During Russian Drone Incursion May Have Been Hit by Polish Missile, Media Reports', Kyiv Independent, 16 September 2025, https://kyivindependent.com/immediately-clarify-the-incident-home-damaged-during-russian-drone-incursion-may-have-been-caused-by-polish-missile-media-report/.

35 On Cold War 'ferret' and peripheral reconnaissance missions, see Thomas R. Johnson, 'American Cryptology During the Cold War, 1945–1989', National Security Agency, 1995, https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/nsa-60th-timeline/1990s/19950000_1990_Doc_3188691_American.pdf; George A. Brown, 'Project Home Run Operations', in 'Dedication and Sacrifice: National Aerial Reconnaissance in the Cold War', National Security Agency, https://media.defense.gov/2021/Jul/13/2002761784/-1/-1/0/DEDICATION-SACRIFICE.PDF; and John R. Schindler, 'A Dangerous Business: The U.S. Navy and National Reconnaissance During the Cold War', National Security Agency, https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/dangerous_business.pdf.

36 Daniel Salisbury, 'Radioactive Measures: Hybrid Threats and Nuclear Risks in Europe and Beyond', IISS, June 2026.

37 Clement Charpentreau, 'Dutch Air Force Fails to Intercept Unknown Drones over Volkel Air Base', AeroTime, 24 November 2025, https://www.aerotime.aero/articles/dutch-air-force-unknown-drones-volkel-air-base.

38 'Survol d'une base de sous-marins nucléaires: ni drone abattu, ni pilote identifié' [Overflight of a Nuclear Submarine Base: no Drone Shot Down, no Pilot Identified], Marine & Océans, 5 December 2025, https://marine-oceans.com/actualites/survol-dune-base-de-sous-marins-nucleaires-ni-drone-abattu-ni-pilote-identifie/.

39 'Germany Records Nearly 2,000 Unidentified UAVs in its Airspace, Investigation Connects Sightings to Russia-Linked Ships', The Insider, 11 December 2025, https://theins.press/en/news/287659.

40 'Drohnen Über Münchner Flughafen – Statement von Innenminister Dobrindt' [Drones over Munich Airport – Statement by Interior Minister Dobrindt], 3 October 2025, https://www.youtube.com/watch?v=XiyLQRz_HDU.

41 Gabriella Calder, 'Building Europe's "Drone Wall": Embracing and Scaling Cheap Defensive Technologies', European Leadership Network, 16 December 2025, https://europeanleadershipnetwork.org/commentary/building-europes-drone-wall-embracing-and-scaling-cheap-defensive-technologies/.

42 Eginhards Volāns et al., 'Handbook on the Role of Non-State Actors in Russian Hybrid Threats', European Centre of Excellence for Countering Hybrid Threats, December 2025, https://www.hybridcoe.fi/publications/handbook-on-the-role-of-non-state-actors-in-russian-hybrid-threats/.

43 AFP, 'Unidentified Drones Spotted over German Military, Industrial Sites', Kyiv Post, 13 December 2024, https://www.kyivpost.com/post/43841.

44 Miranda Bryant, 'Danish PM: Airport Drone Incursion a "Serious Attack" on Critical Infrastructure', *Guardian*, 23 September 2025, https://www.theguardian.com/world/2025/sep/23/drone-sightings-cause-disruption-delays-norway-denmark-airports.

45 Niall O'Connor, 'Four Unidentified Military-style Drones Breached No-fly Zone to Target Zelenskyy's Arrival in Dublin', TheJournal.ie, 4 December 2025, https://www.thejournal.ie/drones-dublin-ireland-hybrid-warfare-russia-6893104-Dec2025/.

46 Malte Kirchner, 'Northern Germany: Concern After Drone Overflights at Night', Heise Online, 4 March 2025, https://www.heise.de/en/news/Northern-Germany-concern-after-drone-overflights-at-night-10303070.html.

47 'Germany Investigates Drone Flights over Industrial Park', DW.com, 22 August 2024, https://www.dw.com/en/germany-investigates-drone-flights-over-industrial-park/a-70021895.

48 Zuzanna Nowak, 'Shadow Fleet in the Baltic Sea – Limits of Tolerance', Opportunity, 20 April 2026, https://theopportunity.pl/en/publications/report-shadow-fleet-in-the-baltic-sea-limits-of-tolerance.

49 International Maritime Organization, 'Urging Member States and all Relevant Stakeholders to Promote Actions to Prevent Illegal Operations in the Maritime Sector by the "Dark Fleet" or "Shadow Fleet"', 11 December 2023, https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/AssemblyDocuments/A.1192(33).pdf.

50 'Illuminating Russia's Shadow Fleet', Windward, https://windward.ai/knowledge-base/illuminating-russias-shadow-fleet/.

51 'Shadow Tanker Fleet Grows More Slowly as Western Sanctions Target Russian Oil', Reuters, 13 August 2025, https://www.reuters.com/business/energy/shadow-tanker-fleet-grows-more-slowly-western-sanctions-target-russian-oil-2025-08-13/; and Benjamin Hilgenstock et al., Russian Shadow Fleet Tracker, March 2026, KSE Institute, https://kse.ua/about-the-school/news/russian-shadow-fleet-tracker-march-2026-share-of-russian-flagged-shadow-tankers-jumps-from-3-to-21-in-nine-months/.

52 Keir Mather MP, 'The Growing Risks to Maritime Safety'.

53 Anna Caprile and Gabija Leclerc, 'Russia's "Shadow Fleet": Bringing the Threat to Light', European Parliamentary Research Service, November 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/766242/EPRS_BRI(2024)766242_EN.pdf.

54 Royal Navy, 'Royal Navy Intercepts Russian Ships in the English Channel', 23 January 2026, https://www.royalnavy.mod.uk/news/2026/january/23/20260123-royal-navy-intercepts-russian-ships-in-the-english-channel.

55 Global Defense News, 'Suspicious Drone Spies on British Aircraft Carrier HMS Queen Elizabeth in Germany', Army Recognition Group, 25 November 2024, https://www.armyrecognition.com/news/navy-news/2024/

suspicious-drone-spies-on-british-aircraft-carrier-hms-queen-elizabeth-in-germany.

56 Henk van Ess, 'They Droned Back', Digital Digging, 10 December 2025, https://www.digitaldigging.org/p/they-droned-back.

57 Yle News, 'Cargo Ship Suspected of Carrying Russian Spy Drones Heads towards Vaasa', 25 August 2025, https://yle.fi/a/74-20179177.

58 'Report: Cargo Ships Searched After Incidents with Unidentified Drones', Maritime Executive, 10 June 2025, https://maritime-executive.com/article/report-cargo-ships-searched-after-incidents-with-unidentified-drones.

59 'What Incident with Russian Zhigulevsk Spy Ship Launching Drone Toward French Charles de Gaulle Aircraft Carrier Tells Us', Defense Express, 10 March 2026, https://en.defence-ua.com/analysis/what_incident_with_russian_zhigulevsk_spy_ship_launching_drone_toward_french_aircraft_carrier_charles_de_gaulle_tells_us-17769.html.

60 Le Monde with AFP, 'Swedish Military Jams Drone near French Aircraft Carrier', 26 February 2026, https://www.lemonde.fr/en/international/article/2026/02/26/swedish-military-jams-unknown-drone-near-france-s-top-aircraft-carrier_6750902_4.html.

61 'Danish Police Investigate Mystery Drone Sightings', DW.com, 1 April 2025, https://www.dw.com/en/danish-police-investigate-mystery-drone-sightings/a-71217317.

62 Tyler Rogoway, 'Chinese Cargo Ship Converted to Launch Advanced Combat Drones Emerges (Updated)', The War Zone, 2 January 2026, https://www.twz.com/sea/chinese-cargo-ship-with-electromagnetic-catapult-to-launch-advanced-combat-drones-emerges.

63 Dan Sabbagh, 'French Military Detain Two After Boarding Russia-linked Oil Tanker Suspected of Launching Drones', *Guardian*, 1 October 2025, https://www.theguardian.com/world/2025/oct/01/france-oil-tanker-russia-drone-denmark.

64 Stine Jacobsen and Surbhi Misra, 'Drone Sightings Disrupt Flights at Copenhagen, Oslo Airports', Reuters, 23 September 2025, https://www.reuters.com/business/aerospace-defense/copenhagen-airport-halts-traffic-due-drone-sightings-police-says-2025-09-22/.

65 'Denmark Links Drone Sorties to State Actor, Latvia Says; Russia Denies Involvement', Reuters, 25 September 2025, https://www.reuters.com/world/europe/denmark-reopens-airports-after-drone-disruption-2025-09-25/.

66 Aleks Phillips and Adrienne Murray, 'Denmark Says "Professional Actor" Behind Drone Incursions over Its Airports', BBC News, 24 September 2025, https://www.bbc.co.uk/news/articles/c7401vk4lgzo.

67 Le Monde, 'Danish authorities say "professional actor" behind drone flights over airports', 25 September 2025 https://www.lemonde.fr/en/international/article/2025/09/25/danish-airports-disrupted-by-drones-of-unknown-origin_6745731_4.html.

68 'Sweden Seizes Shadow Fleet Tanker Jin Hui: The False Flag Problem Is Bigger Than One Ship', Windward, https://windward.ai/knowledge-base/sweden-seizes-shadow-fleet-tanker-jin-hui-the-false-flag-problem-is-bigger-than-one-ship/.

69 'Danish Police Investigate Mystery Drone Sightings', DW.com.

70 Laurits Hjortkjær Henningsen, 'Her Er de Mystiske Droner: – Aldrig Set Noget Lignende' [Here Are the Mysterious Drones: – Never Seen Anything Like This], Ekstra Bladet, 4 January 2025, https://ekstrabladet.dk/krimi/her-er-de-mystiske-droner-aldrig-set-noget-lignende/10486537.

71 Line Omholt-Jensen, 'LNG Carrier Ship Zigzags Close to Underwater Cables in the North Sea', Maritime Optima, 9 January 2025, https://maritimeoptima.com/maritime-news/lng-carrier-ship-zigzags-close-to-underwater-cables-in-the-north-sea.

72 United States Department of State, 'Further Sanctions to Degrade Russia's Ability to Operationalize the Arctic LNG 2 Project', 5 September 2024, https://2021-2025.state.gov/further-sanctions-to-degrade-russias-ability-to-operationalize-the-arctic-lng-2-project/.

73 'U.S. Air Forces in Europe–Air Forces Africa', Air Force, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/609838/us-air-forces-in-europe-air-forces-africa/.

74 'NATO Allied Air Command Home', ac.nato.int, https://ac.nato.int/.

75 Chris Lunday, 'Germany Reportedly Suspects Russia After Drone Sightings over Key Airbase', Politico, 9 February 2025, https://www.politico.eu/article/german-military-suspects-russia-espionage-spy-defense-war-drone-key-airbase/.

76 Hans Kristensen and Eliana Johns, 'Reawakening a Nuclear Legacy: the Potential Return of the US Nuclear Mission to RAF Lakenheath', Federation of American Scientists, 26 February 2025, https://fas.org/publication/increasing-evidence-that-the-us-air-forces-nuclear-mission-may-be-returning-to-uk-soil/.

77 Richard Holmes, 'Suspected Russian Links to Drones over UK Air Bases Revealed', i Paper, 21 February 2025, https://inews.co.uk/news/russian-links-drone-sightings-uk-air-base-3542584.

78 Belga News Agency, 'Defence Minister: Drones at Kleine-Brogel Air Base Probably Used for Espionage', 2 November 2025, https://www.belganewsagency.eu/defence-minister-drones-at-kleine-brogel-air-base-probably-used-for-espionage.

79 George Wright, 'Drones Spotted Over Belgian Military Base for Third Night, Minister Says', BBC News, 3 November 2025, https://www.bbc.co.uk/news/articles/c20e8qzllewo.

80 Haye Kesteloo, 'Belgium Authorizes Military to Shoot Down Drones After Three Nights of Suspected Espionage at Nuclear Weapons Base', DroneXL, 4 November 2025, https://dronexl.co/2025/11/04/belgium-authorizes-military-to-shoot-down-drones/.

81 'US Nuclear Bombs "Based in Netherlands" – Ex-Dutch PM Lubbers', BBC News, 10 June 2013, https://www.bbc.co.uk/news/world-europe-22840880.

82 Aleks Phillips, 'Mystery Drones Halt Air Traffic Near Dutch City of Eindhoven', BBC News, 22 November 2025, https://www.bbc.co.uk/news/articles/cewjlr0v02ro.

83 Reuters, 'Finnish Coastguard Boards Tanker Suspected of Causing Power and Internet Cable Outages', *Guardian*, 26 December 2024, https://www.theguardian.com/world/2024/dec/26/finnish-coastguard-boards-eagle-s-oil-tanker-suspected-of-causing-power-cable-outages.

84 Connor Gallagher and Martin Wall, 'Ireland to Donate Air Defence Systems to Ukraine as War Enters Fourth Year', *Irish Times*, 24 February 2025, https://www.irishtimes.com/ireland/2025/02/24/ireland-to-donate-air-defence-systems-to-ukraine-as-war-enters-fourth-year/.

85 Niall O'Connor, 'Four Unidentified Military-style Drones Breached No-fly Zone to Target Zelenskyy's Arrival in Dublin'.

86 Alexander Martin, 'Sweden's Elite Armed Police Used Helicopter to Board Suspected Sabotage Ship', The Record, 29 January 2025, https://therecord.media/sweden-vezhen-ship-armed-police-boarded-helicopter.

87 Mike Schuler, 'Sweden Close Baltic Sea Cable Damage Investigation, Ruling Accident Not Sabotage', gCaptain, 14 October 2025, https://gcaptain.com/sweden-close-baltic-sea-cable-damage-investigation-ruling-accident-not-sabotage/.

88 Xavier Vavasseur, 'France's M51.3 Submarine Launched Ballistic Missile Enters Operational Service', Naval News, 29 October 2025, https://www.navalnews.com/naval-news/2025/10/frances-m51-3-submarine-launched-ballistic-missile-enters-operational-service/.

89 Chris Kremidas-Courtney, 'What Moscow Learned from Its Drone Breach of Poland, European Policy Centre, 15 September 2025, https://www.epc.eu/publication/what-moscow-learned-from-its-drone-breach-of-poland/.

90 Jennifer Kavanagh, 'No Cause for Alarm: the Case for a Measured Response to Russian Air Incursions', War on the Rocks, 20 October 2025, https://warontherocks.com/no-cause-for-alarm-the-case-for-a-measured-response-to-russian-air-incursions/.

91 German Federal Ministry of the Interior, 'Greater Powers for Drone Defence and the Protection of Airports', 19 November 2025, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2025/11/luftsicherheitsgesetz.html?nn=9919724.

92 Elsa Conesa and Jean-Pierre Stroobants, 'Germany and Belgium Latest to Report Suspicious Drone Flyovers', *Le Monde*, 3 October 2025, https://www.lemonde.fr/en/international/article/2025/10/03/germany-and-belgium-also-report-suspicious-drone-flyovers_6746054_4.html.

93 Sebastian Clapp, 'Eastern Flank Watch and European Drone Wall', European Parliamentary Research Service, 21 October 2025, https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)777962.

94 'False Narratives Analysis of Russian Drone Incidents in Romanian Airspace', European Digital Media Observatory, 17 September 2025, https://edmo.eu/publications/false-narratives-analysis-of-russian-drone-incidents-in-romanian-airspace/.

95 NATO, 'Eastern Sentry to Enhance NATO's Presence Along Its Eastern Flank', 12 September 2025, https://shape.nato.int/news-releases/eastern-sentry-to-enhance-natos-presence-along-its-eastern-flank.

96 Ruslan Bortnik, 'Operation Eastern Sentry: A Reflexive Response with Variations', Hungarian Institute of International Affairs, 22 December 2025, https://hiia.hu/wp-content/uploads/2025/12/Bortnik-Operation-Eastern-Sentry-A-Reflexive-Response-with-Variations.pdf.

97 'Poland Will Shoot Down Objects in Clear-cut Airspace Violations, Prime Minister Says', Reuters, 23 September

2025, https://www.reuters.com/world/poland-will-shoot-down-objects-clear-cut-airspace-violations-prime-minister-says-2025-09-22/.

98 'Address by NATO Secretary General Mark Rutte at the 71st Annual Session of the NATO Parliamentary Assembly in Ljubljana', 13 October 2025, https://www.nato.int/en/news-and-events/events/transcripts/2025/10/13/address.

99 Richard Milne, 'Nato Considers Being "More Aggressive" Against Russia's Hybrid Warfare', *Financial Times*, 30 November 2025, https://www.ft.com/content/dbd93caa-3c62-48bb-9eba-08c25f31ab02?syn-25a6b1a6=1.

100 'Words Must Be Carefully Weighed – Meloni on Cavo Dragone', ANSA, https://www.ansa.it/english/news/2025/12/03/words-must-be-carefully-weighed-meloni-on-cavo-dragone_4261de74-23c7-450f-a6b9-5390a8a07297.html.

101 'Romanian Defence Ministry Says Radars Caught Russian Drone Breaching Air Space', Reuters, 17 April 2026, https://www.reuters.com/world/romanian-defence-ministry-says-radars-caught-russian-drone-breaching-air-space-2026-04-17/.

102 Ivanna Kostina, 'Romania Issues Air-raid Warning Over Risk of "Objects Falling from Airspace"', Ukrainska Pravda, 13 September 2025, https://www.pravda.com.ua/eng/news/2025/09/13/7530738/.

103 A useful summary is provided by Zero Fox, 'Brief: Russian Disinformation Surrounding Drone Incursions into Poland', 10 November 2025, https://www.zerofox.com/intelligence/brief-russian-disinformation-surrounding-drone-incursions-into-poland/.

104 Emma Burrows, 'A New System to Identify and Take Down Russian Drones Is Being Deployed to NATO's Eastern Flank', Associated Press, 6 November 2025, https://www.ap.org/news-highlights/spotlights/2025/a-new-system-to-identify-and-take-down-russian-drones-is-being-deployed-to-natos-eastern-flank/.

105 Jason Israel, Anatoly Motkin and Hanna Myshko, 'Blurred Borders: NATO Needs Answers to Hybrid Attacks', Center for European Policy Analysis, 29 April 2026, https://cepa.org/article/blurred-borders-nato-needs-answers-to-hybrid-attacks/.

106 European Commission, 'Readiness Roadmap 2030', 16 October 2025, https://defence-industry-space.ec.europa.eu/eu-defence-industry/readiness-roadmap-2030_en.

107 Virginie Malingre and Philippe Jacqué, 'Europe Struggles to Agree on a Common Defence as Russian Hybrid Attacks Intensify', *Le Monde*, 2 October 2025, https://www.lemonde.fr/en/international/article/2025/10/02/europe-struggles-to-agree-on-a-common-defence-as-russian-hybrid-attacks-intensify_6746007_4.html.

108 Ewan Jones, 'German Defence Minister Downplays Concept of "Drone Wall" to Protect Europe', TVP World, 30 September 2025, https://tvpworld.com/89208249/german-defence-minister-skeptical-about-drone-wall-idea.

109 Alice Tidey, 'One Year or Three? And Who will Foot the Bill for the Drone Wall? EU Leaders Appear Split', Euronews, 1 October 2025, https://www.euronews.com/my-europe/2025/10/01/one-year-or-three-and-who-will-foot-the-bill-for-the-drone-wall-eu-leaders-appear-split.

110 Reinis Poznaks, 'Drones and New Systems of Warfare: Adapting the EU to Today's Security Challenges', European Parliament, January 2026, https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782599/EPRS_ATA(2026)782599_EN.pdf.

111 Charlie Edwards and Nate Seidenstein, 'The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure'.

112 Daniel Salisbury, 'Drones Targeting European Nuclear Weapons Infrastructure', IISS, 12 December 2025, https://www.iiss.org/online-analysis/online-analysis/2025/12/drones-targeting-european-nuclear-weapons-infrastructure/.

113 Anna Caprile and Gabija Leclerc, 'Russia's "Shadow Fleet": Bringing the Threat to Light'.

114 Witold Stupnicki, 'Russia's Shadow Fleet Presents a Sustained Hybrid War Threat at Sea', Armed Conflict Location & Event Data, 22 May 2026, https://acleddata.com/report/russias-shadow-fleet-presents-sustained-hybrid-war-threat-sea.

Acknowledgements

We would like to thank Douglas Barrie, Nigel Gould-Davies, John Raine and Matthew Redhead for their valuable comments. We are also grateful to the Hanns Seidel Foundation for supporting the research and a workshop on the subject. The views expressed herein are those of the authors and are not necessarily those of the Hanns Seidel Foundation.

IISS

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington DC 20037 | USA
t. +1 202 659 1490 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GFH Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **e.** iiss-middleeast@iiss.org