

Detect and Deter: *Drone Threats, Governance Gaps, and the Future of Icelandic Defence*

JUNE 2026





Publisher:

Varða, June 2026

Authors:

Elizabeth H Redmond

Dr. James Patton Rogers

Sólrún H G Proppé

Kristinn Árni L Hróbjartsson

Design:

Sítrus

Efnisyfirlit

Executive Summary	4
Introduction	6
1. The Policy Landscape	8
The European and NATO Frameworks Iceland Operates Within	8
What Europe's Drone Incidents Reveal for Iceland	9
2. The View from the Institutions on the Front Line	13
The Defence Thinking Gap	13
The Response-Authority Gap	14
The Standing-Watch Gap	16
3. Policy Recommendations	18
1. Bridge detection and response through a written counter-UAS coordination protocol	18
2. Strengthen the police as Iceland's standing counter-UAS authority	18
3. Establish a continuously running coordination cell beneath the Coordination and Control Center	19
4. Conclusion	20
Bibliography	21

Executive Summary

In 2025, drone-related incidents across Northern Europe disrupted operations at major airports, including in Denmark and Norway, where unidentified drones entered controlled airspace and forced their closures. Similar reports of drone sightings near Keflavík International Airport triggered law enforcement responses, media reports, political statements, and the convening of the National Security Council. Interviews conducted for this report indicate that the sightings examined were attributable to registered and permissioned operations, nevertheless these incidents brought drone activity into Iceland's security space and highlighted the challenge of detecting, identifying, and interpreting drone activity in real time.

But drones had already become a domestic issue; in 2022, two Icelandic citizens were arrested on terrorism charges in what became Iceland's first domestic terrorism case. At the core of the case was how they sought to exploit easily accessible emerging technologies, including weaponized commercial drones, to carry out multi-site attacks. Although public attention in Iceland has focused primarily on 3D printed firearms uncovered after police searches, the drone component is equally significant for defence analysis. It demonstrates that drone-enabled threats are no longer something that only occurs to others: they are real, can be domestic in origin, as deemed the most likely scenario by interviewees, and are within reach of motivated actors in Iceland. At the same time, such threats are now a familiar feature of the wider European security landscape, where drones are increasingly discussed in the context of Russian hybrid destabilization tactics.

Iceland's geographic isolation, limited infrastructure redundancy, and dependence on a small number of airports, ports, energy facilities, and submarine cable connections mean that even low-scale drone disruptions could generate disproportionately large national consequences.

This report analyses the drone threats Iceland faces and the governance structures designed to address them by 1) drawing on interviews across relevant Icelandic national security institutions, with academics, infrastructure operators, and other stakeholders, and 2) on desk research encompassing domestic legislation, parliamentary and government reports, media sources, and European and NATO policy frameworks.

We conclude that there are three gaps that cut across institutional boundaries in Iceland's ability to detect, respond to, and deter drones: the defense-thinking gap, response authority gap, and the standing watch gap. Each of which must be resolved to safeguard national security.

Key findings:

1. Iceland's institutions currently assess the drone threat through a domestic lens, centered on undereducated recreational pilots and other lone actors. While this is important, the coordinated, state-linked drone activity now documented across Europe falls outside that frame. Updating the threat picture is a prerequisite for the institutional, legal, and coordinative adjustment the three gaps require; identifying which institution should lead on drone defence is the logical first step in this process.

2. Institutions that detect a drone incident cannot act on it, and the institution that can act is not the one watching. Response authority sits exclusively with the police, while detection is distributed across other institutions and infrastructure operators, none of which have authority to engage. This turns every detection into a request, the institutional interval between request and response is the window a capable actor can exploit.

3. National coordination in Iceland is activated rather than continuously running, a structural mismatch with the pace at which drone incidents unfold.. The Coordination and Control Center is activated when an incident crosses a defined threshold, but hybrid drone activity is typically calibrated to remain below it. A continuously running coordination layer beneath the Center would keep critical infrastructure operators and national authorities in contact across the lower-intensity activity where most drone incidents are likely to occur.

4. The three gaps identified above are mutually reinforcing. A detection that cannot be acted upon, occurring in a zone where jurisdictional authority is contested, reported through a coordination architecture that is not continuously running, and assessed against a threat frame that may not recognise the activity as hostile — compounds into a systemic vulnerability that exceeds the sum of its parts. Closing any single gap without addressing the others will not resolve Iceland's exposure.

Introduction

In 2025, drone activity moved from a peripheral concern to a central question in Northern European security. Among the most disruptive incidents were repeated sightings over Copenhagen and Oslo, which forced temporary closures of major airports, halted flights, and stranded passengers for hours. Iceland was not insulated from these developments. Drone sightings near Keflavík International Airport during the same period triggered law enforcement responses and led to the convening of Iceland's National Security Council, the first time for a drone-related incident.¹ Public messaging in Iceland reflected an evolving and, at times, fragmented understanding of the issue. Prime Minister Kristrún Frostadóttir emphasised caution and measured response,² while Foreign Minister Þorgerður Katrín Gunnarsdóttir framed the incidents within a broader European security context, linking them to the changing character of conflict.³ At the institutional level, the authorities framed the issue through the lens of broader "hybrid" or multi-domain threats, while maintaining that nothing at this stage currently indicates an active threat in Iceland.⁴ While the incidents examined in Iceland were later assessed to involve registered and authorised drone operations,⁵ they exposed a fundamental governance challenge: the absence of institutional ability to detect, identify, and interpret drone activity in real time. These incidents brought drone-related risks to Iceland's domestic security agenda and raised broader questions about how the country would respond to more complex or hostile scenarios. Police statistics indicate that the public awareness has shifted accordingly, with reported drone incidents more than doubling between 2024 and 2025.⁶

Drone technologies have in the last years improved significantly, and have become a staple tool for important activities, ranging from construction to media production to law enforcement. This proliferation has had and will continue to have many positive effects. Any counter-drone regime must therefore distinguish hostile and undereducated activity from the bulk of beneficial commercial and civil use, which is precisely the calibration challenge addressed in the following sections.

Alongside beneficial use, drones have become a domestic issue. In the autumn of 2022, a police investigation originating with the discovery of 3D-printed firearms in Reykjavík evolved into Iceland's first domestic terrorism case. Among the methods the suspects discussed was the acquisition, weaponisation, and deployment of commercial drones in a coordinated multi-site attack. Court records document structured operational thinking around "printing drones," sourcing components from commercial platforms, and deploying multiple drones simultaneously against

¹ Agnar Már Másson. *Tilkynnt um dróna yfir Keflavíkurflugvelli*. Vísir, 29 September 2025.

² Vésteinn Örn Pétursson. *Kallar þjóðaröryggisráð saman*. Vísir, 30 September 2025.

³ Lillý Valgerður Pétursdóttir and Lovísa Arnardóttir. *Þorgerður telur tilefni til að kalla saman þjóðaröryggisráð*. Vísir, 23 September 2025.

⁴ Brynjólfur Þór Guðmundsson. *Ekki búið að boða fund í þjóðaröryggisráði*. RÚV, 26 September 2025.

⁵ According to interviews.

⁶ Icelandic Police, Data Science and Information Division. *Statistics on reports concerning unmanned aircraft operations (drones or UAVs)*. Data provided to Varða on 29 April 2026.

different targets.⁷ Media coverage focused primarily on 3D-printed firearms, with comparatively little attention given to the role of drones in the planning of the attacks. For the purposes of this report, it constitutes the more significant finding as it demonstrates that a drone-enabled threat in Iceland is both realistic and in need of further time-sensitive analysis.

The Reykjavík case is instructive precisely because existing mechanisms functioned as designed, two men were detained before any attack took place, and yet what the investigation revealed was a threat model that Iceland's institutions are not yet structured to address at scale. A successful law enforcement response to a single domestic pilot does not resolve the broader question of how the authorities would manage coordinated, externally directed drone activity now documented across Europe, where detection capabilities are distributed across agencies and response authority is jurisdictionally narrow. Iceland's security architecture was built for a quieter threat environment than the one it now confronts. That gap is the central concern of this report.

The report draws on multiple interviews with leaders and experts from across Icelandic society within policy, regulators, response units and infrastructure operators that have insights or bear responsibility. Iceland does not currently publish a comprehensive national threat assessment, on drones or on any other category, unlike Norway and Denmark, which publish annual consolidated assessments through their police and defence intelligence services. This report is therefore anchored not in a national baseline but in interviews, parliamentary and government reports, and the comparative European record. One consequence is that the drone threat cannot be placed against a prioritised national picture: the report can say what the risk is and why it matters, but not where it ranks among the other threats Iceland faces. The absence of such an assessment is itself a finding, taken up under the defence-thinking gap in Section 2.

⁷ Héraðsdómur Reykjavíkur. *Dómur 12. mars 2024, mál nr. S-6091/2022*. 12 March 2024; Landsréttur. *Dómur fimmtudaginn 6. mars 2025, mál nr. 324/2024*. 6 March 2025; Hæstiréttur. *Mál nr. 28/2025, miðvikudagurinn 11. mars 2026*. 11 March 2026.

1. The Policy Landscape

THE EUROPEAN AND NATO FRAMEWORKS ICELAND OPERATES WITHIN

The European regulatory baseline for civilian drones is established by Regulations (EU) 2019/947 and 2019/945. These regulations create three operational categories (Open, Specific, and Certified) calibrated to risk levels, and impose mandatory operator registration, pilot competence requirements, and technical product standards.⁸ Regulation (EU) 2021/664 builds on this foundation by establishing the U-space framework, a system of dedicated low-altitude airspace zones functioning as a digital known traffic picture for drones. Compliant aircraft continuously broadcast their identity and location in real time, so drones operating outside the system immediately stand out.⁹

Iceland participates through the European Economic Area (EEA) and has transposed the framework into domestic law through the Air traffic Act 80/2022 with drone related regulations further detailed in regulation No. 1360/2024.¹⁰ Flight within 150 metres of sensitive sites is prohibited, and the list of sensitive sites expressly includes Alþingi, Bessastaðir (the Presidential residence), ministries, embassies, police stations, prisons, hospitals, power plants, and substations. Moreover, “Icelandic operators and visitors from outside the EU can register on flydrone.is.”¹¹

Two additional European legislative instruments bear directly on the critical infrastructure dimension of the drone threat as it applies to Iceland. The Critical Entities Resilience (CER) Directive (EU 2022/2557) requires Member States to identify critical infrastructure across energy, transport, health, digital infrastructure, and related sectors, and to ensure that designated entities implement measures that address both physical and cyber risks.¹² In addition, the NIS2 Directive (EU 2022/2555) focuses on the digital dimension of critical infrastructure resilience specifically, imposing stricter cybersecurity risk management and incident reporting obligations on operators of essential services.¹³

⁸ European Aviation Safety Agency, *Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU) 2019/945)*.

⁹ European Aviation Safety Agency, *Easy Access Rules for U-space (Regulation (EU) 2021/664)*.

¹⁰ Samgöngustofa. *Reglur um drónaflug*.

¹¹ Samgöngustofa. *Reglur um drónaflug*.

¹² European Parliament and the Council of the European Union. *Directive (EU) 2022/2557 of 14 December 2022 on the Resilience of Critical Entities*.

¹³ European Parliament and the Council of the European Union. *Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2)*.

At the NATO level, the Integrated Air and Missile Defence policy provides Iceland with an alliance-level doctrinal framework for responding to air threats across the full threat spectrum, explicitly including drone systems.¹⁴ Iceland contributes to collective defence through operation of its national air surveillance system¹⁵ and provision of host-nation support and infrastructure for Allied air policing.¹⁶ Since 2008, NATO allies have rotated fighter detachments through Keflavík Air Base to provide air policing, typically three deployments annually of three to four weeks each.¹⁷ The most recent rotation was led by the Swedish Air Force with six JAS 39 Gripen fighters, marking Sweden's first leadership of an Icelandic Air Policing mission since its NATO accession in March 2024.¹⁸ In February 2026, NATO launched Arctic Sentry, a broader initiative designed to strengthen alliance deterrence and defence across the Arctic and High North, of which Iceland Air Policing constitutes a central element.¹⁹

Finally, Keflavík Airport serves as a critical transatlantic hub, hosting rotational deployments of US Navy P-8A Poseidon maritime patrol aircraft and allied surveillance assets in support of GIUK-gap operations. The US Naval Air Station at Keflavík closed in 2006, current allied military presence is now rotational and expeditionary, sustained by US and NATO infrastructure investment considered vital to US homeland defense and to deter and defend critical maritime chokepoints for transatlantic security.²⁰

Taken together, these European and NATO frameworks provide Iceland with a policy and regulatory foundation for managing drone and wider airspace threats. Yet, how do these function in practice given the rising number of drone incidents across Europe? The following section examines that record and identifies ongoing policy limitations.

WHAT EUROPE'S DRONE INCIDENTS REVEAL FOR ICELAND

The drone threats recently observed across Europe could exploit Iceland's most serious and unchangeable vulnerability, its geography. As an island nation, Iceland depends on a small number of entry points for the flow of goods and people, so disruptions at airports or ports would carry consequences far greater than in countries with more redundancy. Similar dynamics apply to energy, as Iceland produces the overwhelming majority of its power domestically. This means that an attack on energy infrastructure could cascade through the economy in ways unlikely in nations with diverse energy sources. The forms of drone activity now emerging across Europe, around airports, ports, and energy facilities, map directly onto the three sectors where Iceland has the least capacity to absorb disruption.

¹⁴ NATO. *NATO Integrated Air and Missile Defence Policy*. 13 February 2025.

¹⁵ NATO Allied Air Command. *Iceland's Role in NATO Integrated Air and Missile Defence System*. 2016.

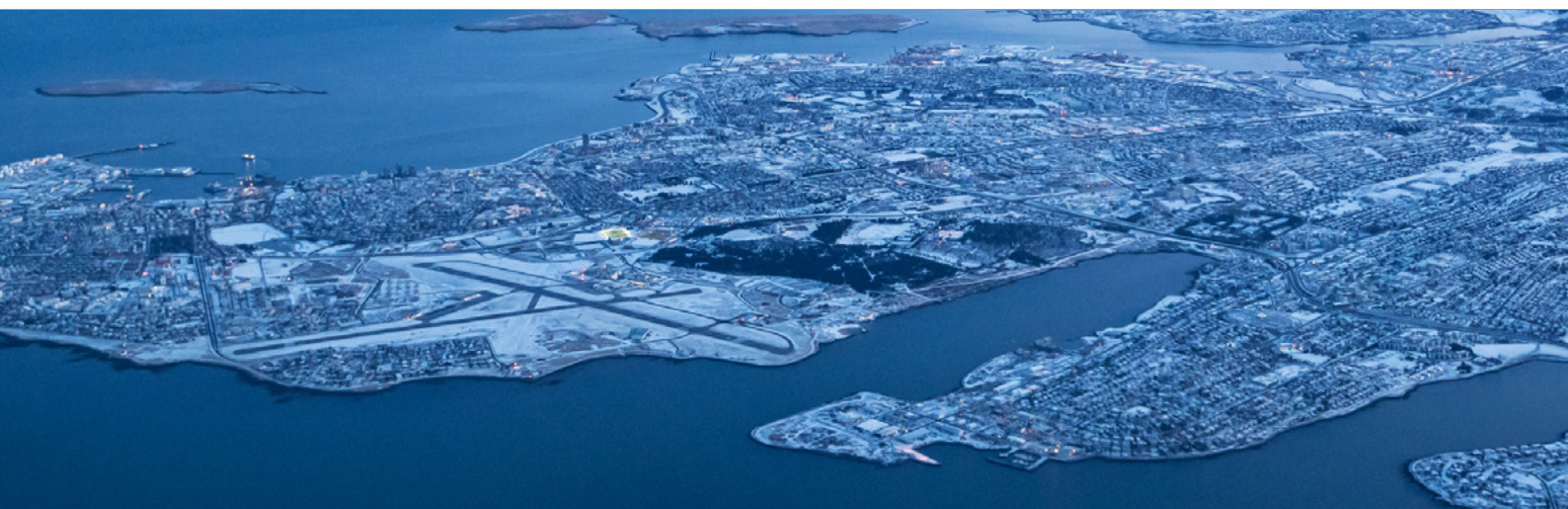
¹⁶ NATO. *NATO Secretary General Welcomes Icelandic Prime Minister to NATO Headquarters*. 28 May 2025.

¹⁷ NATO Allied Air Command. *Norway Ready for Third Deployment of F-35 to Iceland*. 11 January 2023.

¹⁸ RÚV. *Svíþjóð sér í fyrsta sinn um loftrýmisgæslu á Íslandi*. 12 February 2026.

¹⁹ NATO. *Arctic Security*. Updated 16 February 2026.

²⁰ NATO Allied Air Command. *Iceland's Role in NATO Integrated Air and Missile Defence System*. 2016.



AIRPORTS

The most consequential drone incidents documented across the European Union have involved airspace incursions at major airports, causing hours-long facility closures and significant economic loss. In September 2025, Copenhagen Airport, which served over 32 million passengers that year, was forced to close for four hours when two large drones were observed in its airspace. The Danish authorities concluded that the drones were operated by a “capable actor,”²¹ which differentiated this event from those caused by undereducated recreational drone pilots. Approximately 109 flights were cancelled and 51 redirected,²² and Danish authorities characterised the incursions as “the most serious attack yet on its critical infrastructure.”²³ Around the same time, Oslo Airport was forced to close for three hours due to a separate drone sighting. It is estimated that the Copenhagen and Oslo closures caused €5–10 million and €0.5 and €1.2 million in losses, respectively.²⁴ For Iceland, a nation where aviation supports over a quarter of the GDP,²⁵ drone incursions around airports can produce losses well beyond those seen in Copenhagen or Oslo, since Keflavík handles nearly all of the country’s international traffic and the limited capacity of Iceland’s other airports could not absorb all redirected flights during high season.

²¹ Bloomberg. *Copenhagen Airport Closed as Police Investigate Drone Activity*. 22 September 2025; CNN. *Travel Disruption for Thousands After Mystery Drones Closed Two of Scandinavia’s Busiest Airports*. 23 September 2025.

²² Flightradar24 (@flightradar24). “Summary of last night’s drone chaos in Scandinavia.” X (formerly Twitter), 23 September 2025.

²³ Al Jazeera. *Denmark Reports ‘Hybrid Attack’ as Drones Shutter Major Airport*. 25 September 2025; Euronews. *Fact-checking Europe’s ‘Drone Problem’*. 20 November 2025.

²⁴ David Schwartz. *The Hidden Cost of Drone Incursions: Why Airports Need Counter-UAS*. D-Fend Solutions, 30 September 2025.

²⁵ International Air Transport Association (IATA). *The Value of Air Transport to Iceland*.



PORTS

Port infrastructure represents a second structural vulnerability. Icelandic ports underlie two of the nation's most important industries: tourism and fisheries, and account for over 90% of imports.^{26, 27, 28} Recent drone incursions over European ports have prompted investments in new security for these vital economic nodes, illustrated by the decision to install c-UAS air defense systems in Belgium's Port of Antwerp after a series of drone disruptions in 2025.²⁹ Germany also recorded suspicious drone activity over ports and naval infrastructure; in September 2025, two drones were "spotted flying over the ThyssenKrupp naval shipyard," followed by reports of "a formation led by a large drone, accompanied by several smaller ones," over the Kiel Fjord, home to the Port of Kiel.³⁰ Port infrastructure is specialised and costly, and gantry cranes "can cost tens of millions of dollars each," and if damaged can have "replacement lead times stretching up to two years."³¹ For Iceland, where maritime trade sustains both the import-export economy and the tourism sector, a single damaged crane or temporarily closed harbour would carry disproportionate economic consequences.

²⁶ International Trade Administration. *Iceland Country Commercial Guide: Market Overview*. 1 April 2026.

²⁷ Statistics Iceland (Hagstofa Íslands). *Innflutningur eftir vöruflokkum SITC 3 Rev. 4, 2010–2025*.

²⁸ Statistics Iceland (Hagstofa Íslands). *Vöruflutningar um hafnir 2001–2024*.

²⁹ Britbrief. *Europe's Second Largest Port to Deploy Air-Defence System After Drone Incursions*. 26 February 2026.

³⁰ Kateryna Hodunova. *Unidentified Drones May Have Spied on Critical Infrastructure in Germany*, *Media Reports*. The Kyiv Independent, 1 October 2025.

³¹ Marsh. *Port and Terminal Risks: Understanding Allisions, Costs, and Supply Chain Impacts*. 1 June 2026.



ENERGY INFRASTRUCTURE

Iceland ranks among the highest in the world both energy production and energy consumption per capita,³² with approximately 85% of its energy domestically produced.³³ Its energy infrastructure, particularly hydrothermal power plants, is therefore disproportionately and structurally exposed in ways that import-dependent or interconnected grid states are not. There have been several recent reports of drone sightings around power plants in Europe, like over a hydroelectric power plant in Rovaniemi, Finland in August 2025.³⁴ In some cases, like that of the Doel Nuclear Power Plant in Belgium, authorities have claimed that the drone activity is “coordinated and sophisticated, not the work of hobbyists.”³⁵

Drone disruptions of this kind, documented across multiple critical infrastructure sectors, have been characterised acts of “hybrid warfare” by the President of the European Commission, usually linked to Russian state activity.³⁶ The non-attributable nature of drones makes them an attractive vector, particularly because the threat any single sighting poses is difficult to assess in real time. A quadcopter observed near an airport could be the work of an inattentive hobbyist drifting into restricted airspace, or it could be collecting geospatial intelligence on behalf of an adversary. Either way, sites of importance must investigate out of an abundance of caution, which is precisely what makes drones such an operationally effective instrument below the threshold of conventional military engagement. The resulting social and economic disruption can rival that of a traditional kinetic attack, without carrying the same threat of retaliation.

A recurring challenge identified throughout this research is the difficulty of distinguishing between benign, negligent, criminal, and hostile drone activity in real time. This ambiguity is itself strategically useful to hostile actors operating below the threshold of conventional conflict, and it complicates both proportional response and public communication.

³² Hannah Ritchie, Pablo Rosado, and Max Roser. *Energy Production and Consumption*. Our World in Data, first published July 2020, updated January 2024.

³³ Government of Iceland. *Energy*.

³⁴ Mezha. *Drone Incident Over Finnish Hydroelectric Plant Highlights Growing Security Concerns in Europe*. 27 September 2025.

³⁵ Miriam McNabb. *Unidentified Drone Incursions at Belgium Nuclear Plant Highlight Growing Critical Infrastructure Threat*. DroneLife, 10 November 2025.

³⁶ Reuters. *Russia's Suspected 'Hybrid War' Puts European Air Defences to the Test*. 5 November 2025.

2. The View from *the Institutions* on the Front Line

Icelandic institutions operating on the frontline of drone detection and defenses, academics, infrastructure operators, and other experts with insights into drone-related threats informed this assessment. The threats these institutions are likely to face are not state-on-state kinetic attacks like those Ukraine is experiencing, but low-cost, low-attribution activities like those listed in the previous section.

The central problem is not the existence of drones themselves, but rather the mismatch between the speed, ambiguity, and low attribution of modern drone activity and the slower, event-triggered coordination structures currently responsible for responding to it. Iceland's institutions are not failing within their existing mandates; rather, the threat environment has evolved faster than the governance architecture built to manage it.

Beyond the more overt drone terror attack scenario making headlines in Iceland, drones are most likely to be used to probe institutional blind spots or to cause disruption to normal activity through airspace incursions. Given this, we have identified three gaps that could be exploited by a hostile actor: 1) the defence-thinking gap, 2) the response-authority gap, and 3) the standing-watch gap.

THE DEFENCE THINKING GAP

Iceland's position as a state without a standing military, located at the intersection of north Atlantic strategic corridors, has shaped an institutional and political culture that treats security as a matter of foreign policy cooperation rather than a domestic capability. The two traditional pillars of Icelandic defence are the NATO alliance and the 1951 Bilateral Defence Agreement with the United States, both of which orient the country outward.³⁷ The past decade has seen this orientation begin to shift on national defence, marked most notably by the creation of the National Security Council in 2016,^{38,39} but the reorientation remains recent and still consolidating. Interviewees described Iceland as "finding its place" in national security, a departure from a past in which "even discussing security" was "a taboo." As this reorientation is still underway, the institutional, legal, and technological adjustments needed to address the drone threat will likely arrive piecemeal, advancing institution

³⁷ Government of Iceland. *National Security*.

³⁸ Government of Iceland. *National Security*.

³⁹ Silja Bára Ómarsdóttir and Guðbjörg Ríkey Th. Hauksdóttir, "In and of the Arctic: Security in Iceland," Belfer Center for Science and International Affairs, November 6, 2025.

by institution rather than through a single coordinated effort. Interviewees also identified institutional culture, organisational tradition, and differing perceptions of responsibility as barriers to adaptation in a system where drone defence historically fell between civilian, policing, and defence-oriented mandates.

Icelandic institutions are still developing the conceptual frameworks needed to assess the drone threat in its current form, and interviewee assessments reflect a consistently low threat perception. The present institutional concern is described as “overstimulation” and an oversuggestion of drones as a threat, with interviewees noting that Iceland is far away from conflict zones. Interviewees suggest that a drone incident would most likely involve an undereducated but permissioned drone pilot or, at worst, a “lone wolf” rather than a hostile foreign actor. Both framings reflect the threat picture as it has historically appeared in Iceland. They are however poorly suited to the coordinated, state-linked drone activity now documented across Europe, and updating institutional threat assessments accordingly is a necessary condition for the governance reforms that follow. This updating is also currently invisible: Iceland publishes no comprehensive national threat assessment, whether on drones or on the other security challenges it faces, so the threat pictures held inside individual institutions are neither legible to one another nor to the wider public, and any revision that does occur happens behind institutional walls rather than against a shared, prioritised baseline.

A second dimension of the defence-thinking gap concerns not how the threat is understood but who bears institutional responsibility for thinking about it. Drone policy is described as something that “someone needs to ask for,” and that “defence doesn’t get attention generally” but infrastructure operators seem to be somewhat aware, describing internal drone discussions happening “over the coffee table” and drone detection projects as “on the roadmap.”

Interviewees acknowledged that Iceland cannot lean on others for drone defense, recognizing the need for domestic institutional capacity alongside its longstanding NATO commitments. Identifying which institution should lead on drone defence is a logical next step in the broader evolution of Icelandic defence thinking underway since 2016.

THE RESPONSE-AUTHORITY GAP

Response authority for drone incidents in Iceland sits exclusively with the police, while detection is distributed across agencies and critical infrastructure operators. All institutions interviewed located response authority with the police, and police officers interviewed opposed any expanded legal framework on the grounds that it would require large-scale revision of existing statutes and structures. The response authority gap is that the institutions with situational awareness on a developing incident hold no authority to act on it, converting every detection into a request rather than a response. The Copenhagen and Oslo incidents showed that drone incursions at critical infrastructure are not brief events but sustained ones, with capable actors keeping airspace contested for hours. For Iceland, where a detecting institution must wait for the police to arrive and assess

before any response can be initiated, that sustained character of such incidents is precisely what makes the request-and-response structure inadequate. The hard-to-assess nature of drone sightings extends this further, since each request carries an investigative judgment that only the police are positioned to make.

The police are correct that opening up that authority would require significant statutory revision. Icelandic law is reasonably clear at the extremes but ambiguous in the operational space between them. Article 14 of the Police Act authorises officers to use force in the course of their duties, constrained by a proportionality requirement.⁴⁰ Where an immediate, identifiable threat is present, the police, in practice the Special Intervention Unit of the National Police Commissioner (Sérsvait ríkislögreglustjóra) as the only routinely armed police unit in Iceland⁴¹, has both the legal basis and the operational training to act. The gap opens immediately below that threshold. Counter-drone responses that fall short of kinetic engagement, such as signal jamming, GPS spoofing, or takeover of the control link, are precisely the techniques most relevant to the kind of low-cost, low-attribution drone activity Iceland is most likely to face, and they sit in a legal grey zone almost everywhere in Europe. The European Commission's February 2026 Action Plan on Drone and Counter-Drone Security observes that active mitigation measures such as jamming, spoofing, or kinetic intervention "remain restricted to military and specialised police units due to strict spectrum-interference and aviation-safety rules," and that critical-infrastructure operators "typically lack legal authority to neutralise a threatening drone."⁴² The Action Plan commits the Commission to encourage Member States to develop legal frameworks enabling such operators to take effective remedial measures, including takedowns, and names Iceland among close partners with whom this work will be coordinated.⁴³

The chain of command above the officer level is itself incomplete in statute. Institutions that detect unexpected drone traffic describe their role as surveillance and, once detected, a police problem; but the Police Act tells an officer what they may do in the moment, not what ministers, the National Police Commissioner, or the Director General of the Coast Guard should do in a non-imminent but escalating situation: whether to authorise a non-kinetic response, who executes it, or what threshold of evidence is required. In declared civil-protection emergencies, the chain is clear: the Civil Protection Act places operational command with the National Commissioner of Police under the responsible minister, with defined roles for the response agencies. The gap is in the wide band below that threshold. Iceland's National Security Council (Þjóðaröryggisráð), established in 2016, was created as a coordinating forum for precisely that kind of cross-institutional question, but it operates at the policy level — its capacity remains consultative rather than operational, and it does not issue tactical orders.⁴⁴

⁴⁰ Alþingi. *Lögreglulög nr. 90/1996 (Police Act)*.

⁴¹ Wikipedia. *Sérsvait ríkislögreglustjóra*.

⁴² European Commission. *Action Plan on Drone and Counter-Drone Security, COM(2026) 81 final*. 11 February 2026.

⁴³ European Commission. *Action Plan on Drone and Counter-Drone Security, COM(2026) 81 final*. 11 February 2026.

⁴⁴ Alþingi. *Lög um þjóðaröryggisráð nr. 98/2016*.

The interplay between the Coast Guard and the Special Unit illustrates the same jurisdictional gap from a different angle. The Coast Guard is the operative law-enforcement authority at sea, and under act 52/2006 its crews are statutorily empowered to exercise police authority when executing or assisting with law enforcement.⁴⁵ In practice the scope of that authority for armed effects is less clearly defined than the statute alone suggests. Interviewees identified the boundaries and interplay between the two institutions as an area requiring clarification, particularly on weapons authority and decision-making in armed responses, and neither Act spells out the threshold at which a maritime incident requiring force would shift from Coast Guard authority into a Special Unit operation. In a drone context that jurisdictional seam becomes operationally significant: if a UAV loiters over a Coast Guard vessel, a fishing trawler, or a cable-laying ship in the Icelandic EEZ, it is unclear from the statutes alone whether the Coast Guard could authorise a counter-drone response on its own.

THE STANDING-WATCH GAP

Even with response authority clarified, Iceland would still face a separate gap in operational tempo. The current model treats drone incidents as discrete events that activate a coordination structure when they occur, rather than as a continuous category of activity warranting a continuously running watch — much in the way ordinary crime is handled, with reports investigated in sequence rather than monitored as a stream. Iceland's Coordination and Control Center (SST) is an established crisis operations centre, but is stood up on an event-triggered basis, when response leaders judge it necessary or when a civil protection committee or response agency requests it.⁴⁶ What is missing is the operational layer beneath this threshold: a continuously running coordination function that keeps airport, port, energy, telecommunications, and submarine cable operators in real-time contact with each other and with national authorities for incidents that fall below the activation threshold, where most hybrid drone activity is likely to sit.

The same gap surfaces inside the existing chain of command. Detection and response capabilities of the police are not publicly shared, so even between the institutions that detect and the institutions that respond there is no shared operational picture, only a sequence of handoffs. Treating drones as a reporting matter rather than a monitoring one means that each sighting is investigated in isolation, with no running record against which to compare it.

Two independent reviews have identified this gap and reached convergent conclusions. The September 2025 cross-party parliamentary working group report on Iceland's defence and security policy called for the establishment of a 24/7 Security Operations Centre ("sólarhringsvöktun (e. Security Operation Center) að erlendra fyrirmynd")) and for strengthened integration of remote and real-time monitoring of critical infrastructure, including ports, airports, submarine cables, and energy facilities.⁴⁷ The November 2025 IISS independent review of the policy reached the

⁴⁵ Alþingi. *Lög um Landhelgisgæslu Íslands nr. 52/2006*.

⁴⁶ Alþingi. *Lög um almannavarnir nr. 82/2008*.

⁴⁷ Stjórnarráð Íslands. *Inntak og áherslur stefnu í varnar- og öryggismálum: Inntak og áherslur stefnu í varnar- og öryggismálum. Skýrsla samráðshóps þingmanna 2025*, 12 September 2025.

same recommendation independently and proposed that the SOC be structured as a public-private partnership drawing in critical-infrastructure operators and technology firms.⁴⁸ A SOC scoped to that operator landscape is also the natural national node for ingest of distributed drone detection by those same operators, providing the continuous shared picture that the existing event-triggered structure cannot, and tying the cyber and physical sides of the hybrid threat into a single running operational layer rather than two parallel ones.

Iceland already demonstrates the institutional capacity for continuous watch-keeping in one domain. The Icelandic Air Defence System runs on a 24/7 basis as part of NATO Integrated Air and Missile Defence, feeding the Combined Air Operations Centre at Uedem and contributing to round-the-clock alliance air-picture compilation.⁴⁹ The country therefore knows how to staff, sustain, and integrate a continuously running surveillance function when the requirement is recognised. The standing-watch gap is consequently not a capacity problem but a scoping one: extending continuous watchkeeping to the hybrid drone threat would build on an existing posture rather than introduce a new one.

Taken together, the three gaps compound. A defence-thinking culture that still treats drones as an exceptional rather than a routine concern produces a single-authority structure with statutory ambiguity below the kinetic threshold, which in turn is operated through processes that activate on demand rather than run continuously. Iceland's response to a drone incident therefore depends on processes that are stood up rather than running, at exactly the moments when a running process is what the threat requires.

⁴⁸ Charlie Edwards. *Iceland's Security and Defence Policy: An Independent Review of the Government's Strategy*. International Institute for Strategic Studies (IISS), 20 November 2025.

⁴⁹ NATO Allied Air Command. *Iceland's Role in NATO Integrated Air and Missile Defence System*. 2016.

3. Policy

Recommendations

The recommendations that follow are derived from the three gaps identified in the preceding analysis, supplemented by issues that surfaced through institutional interviews. They are designed to work within Iceland's existing institutional architecture rather than to redraw it; none require creation of new institutions or a reallocation of responsibilities between the Coast Guard, the police, or the other civil authorities.

1. BRIDGE DETECTION AND RESPONSE THROUGH A WRITTEN COUNTER-UAS COORDINATION PROTOCOL.

Response authority sits exclusively with the police, while detection capacity is distributed across Isavia, Faxaport, the Coast Guard, and other infrastructure operators with no statutory authority to engage. Each detection therefore becomes a request, and the institutional interval between request and response is the window a capable actor can exploit.

This should be addressed by establishing a written counter-UAS protocol binding the police, critical-infrastructure operators, and other actors able to detect drone activity. The protocol should specify detection-sharing standards, handoff procedures, and pre-authorised actions inside the request-and-response window, so that distributed detection capacity converts directly into coordinated response.

2. STRENGTHEN THE POLICE AS ICELAND'S STANDING COUNTER-UAS AUTHORITY.

The Special Unit is the only Icelandic institution with both statutory authority and operational training to engage drones, but its current resourcing assumes drone incidents as occasional rather than as a recurring category of activity. Icelandic law is also silent or ambiguous on non-kinetic responses, for example jamming, spoofing, control-link takeover, that fall short of kinetic force and are precisely the techniques most relevant to low-cost, low-attribution drone activity.

To address, the government should provide standing budget lines for adequate manning, equipment refresh and recurrent training, recognising the speed at which commercial drone platforms evolve, and pair this with legislative work to clarify police authority to use non-kinetic counter-UAS techniques in the operational space below the kinetic-force threshold.

3. ESTABLISH A CONTINUOUSLY RUNNING COORDINATION CELL BENEATH THE COORDINATION AND CONTROL CENTER.

The SST is event-triggered, but hybrid drone activity is calibrated to remain below activation thresholds — the standing-watch gap. Iceland therefore has no continuously running operational layer keeping airport, port, energy, telecommunications, and submarine-cable operators in contact with national authorities across the lower-intensity activity where most drone incidents are likely to sit.

To address this, the government should stand up a permanent national coordination cell as the operational layer beneath the SST, maintaining a continuous shared picture across critical-infrastructure operators, the police, and the Coast Guard. The 24/7 air surveillance Iceland already runs for NATO Integrated Air and Missile Defence demonstrates the institutional capacity for continuous watchkeeping; this recommendation extends that posture to the hybrid drone domain and establishes the natural ingest point for the public-private Security Operations Centre proposed by the parliamentary working group and the IISS review.

Implementing these measures will require further technical, organisational, and financial assessment. Establishing continuously running coordination and monitoring functions carries staffing, training, infrastructure, and sustainment costs alongside technological requirements. Counter-UAS systems also vary significantly in capability, operational suitability, legal implications, and cost, particularly in aviation and maritime environments where interference risks must be carefully managed. A dedicated follow-on assessment examining technological options, operational ownership, procurement requirements, and long-term sustainment costs would therefore constitute a logical next step.

4. Conclusion

Drones are not the only threat Iceland faces, but they are the clearest example of how the threat environment is changing. Low-cost, commercially available technologies are making it easier for hostile actors to test systems, disrupt activity, and operate below the threshold that would trigger a NATO response. This is the space between routine policing and collective defence, and it is where Iceland is currently least prepared.

Iceland is broadly aligned with European regulatory frameworks, and NATO provides an important layer of deterrence above them. What sits between the two is where the three gaps outlined in this report are concentrated. Authority is uneven and coordination is still largely reactive rather than continuous. Closing the defence-thinking, response authority, and standing-watch gaps is not about building something new, it is about making what already exists work as a system. None of these recommendations require new institutions or a redrawing of responsibilities between the Coast Guard, the police, or the civil defence authority. What they do require is political will to treat the drone question as a domestic security issue, legislative time to close clear gaps in authority, and targeted funding.

Iceland has been moving since 2016 toward a more formalised approach to national security, but the transition is still underway. The risk is not that the problem is unrecognised. It is that progress continues in parallel across institutions without being brought together. The opportunity is that Iceland is still early enough in this process to shape a system that is proportionate, coordinated, and workable in practice. The shift is the right one. It is just not yet complete.

Bibliography

- Agnar Már Másson. *Tilkynnt um dróna yfir Keflavíkurflugvelli*. Vísir. 29 September 2025.
<https://www.visir.is/g/20252781421d/tilkynnt-um-drona-yfir-keflavikurflugvelli>
- Al Jazeera. *Denmark Reports 'Hybrid Attack' as Drones Shutter Major Airport*. 25 September 2025.
<https://www.aljazeera.com/news/2025/9/25/denmark-shuts-second-airport-in-a-week-more-unidentified-drones-spotted>
- Alþingi. *Lög um almannavarnir nr. 82/2008*. <https://www.althingi.is/lagas/nuna/2008082.html>
- Alþingi. *Lög um Landhelgisgæslu Íslands nr. 52/2006*. <https://www.althingi.is/lagas/nuna/2006052.html>
- Alþingi. *Lög um þjóðaröryggisráð nr. 98/2016*. <https://www.althingi.is/lagas/nuna/2016098.html>
- Alþingi. *Lögreglulög nr. 90/1996*. <https://www.althingi.is/lagas/nuna/1996090.html>
- Bloomberg. *Copenhagen Airport Closed as Police Investigate Drone Activity*. 22 September 2025.
<https://www.bloomberg.com/news/articles/2025-09-22/copenhagen-airport-closed-as-police-investigate-drone-activity>
- Britbrief. *Europe's Second Largest Port to Deploy Air-Defence System After Drone Incursions*. 26 February 2026.
<https://britbrief.co.uk/politics/defence/antwerp-port-to-install-anti-aircraft-system-following-drone-threats.html>
- Brynjólfur Þór Guðmundsson. *Ekki búið að boða fund í þjóðaröryggisráði*. RÚV, 26 September 2025.
<https://www.ruv.is/frettir/innlent/2025-09-26-ekki-buid-ad-boda-fund-i-thjodaroryggisradi-45445>
- Charlie Edwards. *Iceland's Security and Defence Policy: An Independent Review of the Government's Strategy*. International Institute for Strategic Studies (IISS), 20 November 2025. <https://varda.org/2025/12/08/ny-iiss-skyrsla-um-oryggis-og-varnarmalastefnu-islands/>
- CNN. *Travel Disruption for Thousands After Mystery Drones Closed Two of Scandinavia's Busiest Airports*. 23 September 2025.
<https://edition.cnn.com/2025/09/23/europe/copenhagen-oslo-airport-closed-drones-int-latam>
- David Schwartz. *The Hidden Cost of Drone Incursions: Why Airports Need Counter-UAS*. D-Fend Solutions, 30 September 2025.
<https://d-fendsolutions.com/blog/why-airports-need-counter-uas/>
- European Aviation Safety Agency. *Easy Access Rules for U-space (Regulation (EU) 2021/664)*.
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0664>
- European Aviation Safety Agency. *Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU) 2019/945)*.
<https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu>
- European Commission. *Action Plan on Drone and Counter-Drone Security, COM(2026) 81 final*. 11 February 2026.
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52026DC0081>
- European Parliament and the Council of the European Union. *Directive (EU) 2022/2555 of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2)*. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

European Parliament and the Council of the European Union. *Directive (EU) 2022/2557 of 14 December 2022 on the Resilience of Critical Entities*. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>

Euronews. *Fact-checking Europe's 'Drone Problem'*. 20 November 2025. <https://www.euronews.com/my-europe/2025/11/20/fact-checking-europes-drone-problem-why-are-airports-shuttering-over-drone-sightings>

Flightradar24 (@flightradar24). *"Summary of last night's drone chaos in Scandinavia."* X (formerly Twitter), 23 September 2025. <https://x.com/flightradar24/status/1970349807374942332>

Government of Iceland. *Energy*. <https://www.government.is/topics/business-and-industry/energy/>

Government of Iceland. *National Security*. <https://www.government.is/topics/foreign-affairs/national-security/>

Hagstofa Íslands. *Innflutningur eftir vöruflokkum SITC 3 Rev. 4, 2010–2025*. https://px.hagstofa.is/pxis/pxweb/is/Efnahagur/Efnahagur__utanrikisverslun__1_voruvidskipti__01_voruskripti/UTA06202.px

Hagstofa Íslands. *Vöruflutningar um hafnir 2001–2024*. https://px.hagstofa.is/pxis/pxweb/is/Umhverfi/Umhverfi__5_samgongur__4_skip/SAM05103.px

Hannah Ritchie, Pablo Rosado, and Max Roser. *Energy Production and Consumption*. Our World in Data, first published July 2020, updated January 2024. <https://ourworldindata.org/energy-production-consumption>

Héraðsdómur Reykjavíkur. *Dómur 12. mars 2024, mál nr. S-6091/2022*. 12 March 2024. <https://island.is/domar/g-e489251d-421f-4d66-8590-c7368b595ade>

Hæstiréttur. *Mál nr. 28/2025, miðvikudagurinn 11. mars 2026*. 11 March 2026. <https://island.is/domar/s-E716C889-AAF7-42FE-93E1-2ED28D8BEE62>

Icelandic Police, Data Science and Information Division. *Statistics on reports concerning unmanned aircraft (drones or UAVs)*. Unpublished data provided to Varða. 29 April 2026.

International Air Transport Association (IATA). *The Value of Air Transport to Iceland*. <https://www.iata.org/en/iata-repository/publications/economic-reports/the-value-of-air-transport-to-iceland/>

International Trade Administration. *Iceland Country Commercial Guide: Market Overview*. 1 April 2026. <https://www.trade.gov/country-commercial-guides/iceland-market-overview>

Kateryna Hodunova. *Unidentified Drones May Have Spied on Critical Infrastructure in Germany, Media Reports*. The Kyiv Independent, 1 October 2025. <https://kyivindependent.com/unidentified-drones-may-have-monitored-critical-infrastructure-in-germany-spiegel-reports/>

Landsréttur. *Dómur fimmtudaginn 6. mars 2025, mál nr. 324/2024*. 6 March 2025. <https://island.is/domar/g-aacfc454-1ca5-445a-bca7-36f99aa92966>

Lillý Valgerður Pétursdóttir and Lovísa Arnardóttir. *Þorgerður telur tilefni til að kalla saman þjóðaröryggisráð*. Vísir, 23 September 2025. <https://www.visir.is/g/20252779361d/thorgerdur-telur-tilefni-til-ad-kalla-saman-thjodaroryggisrad>

Marsh. *Port and Terminal Risks: Understanding Allisions, Costs, and Supply Chain Impacts*. 1 June 2026. <https://www.marsh.com/en/industries/marine/insights/understanding-port-terminal-allisions-costs-supply-chain-impacts.html>

Mezha. *Drone Incident Over Finnish Hydroelectric Plant Highlights Growing Security Concerns in Europe*. 27 September 2025. <https://mezha.net/eng/bukvy/drone-incident-over-finnish-hydroelectric-plant-highlights-growing-security-concerns-in-europe/>

- Miriam McNabb. *Unidentified Drone Incursions at Belgium Nuclear Plant Highlight Growing Critical Infrastructure Threat*. DroneLife. 10 November 2025. <https://dronelife.com/2025/11/10/unidentified-drone-incursions-at-belgium-nuclear-plant-highlight-growing-critical-infrastructure-threat/>
- NATO. *Arctic Security*. Updated 16 February 2026. <https://www.nato.int/en/what-we-do/deterrence-and-defence/arctic-security>
- NATO. *NATO Integrated Air and Missile Defence Policy*. 13 February 2025. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy>
- NATO. *NATO Secretary General Welcomes Icelandic Prime Minister to NATO Headquarters*. 28 May 2025. <https://www.nato.int/en/news-and-events/articles/news/2025/05/28/nato-secretary-general-welcomes-icelandic-prime-minister-to-nato-headquarters>
- NATO Allied Air Command. *Iceland's Role in NATO Integrated Air and Missile Defence System*. 2016. <https://ac.nato.int/archive/2016/icelands-role-in-nato-integrated-air-and-missile-defence-system>
- NATO Allied Air Command. *Norway Ready for Third Deployment of F-35 to Iceland*. 11 January 2023. https://ac.nato.int/archive/2023/NOR_F-35_ISL_3rd
- Reuters. *Russia's Suspected 'Hybrid War' Puts European Air Defences to the Test*. 5 November 2025. <https://www.reuters.com/business/aerospace-defense/russias-suspected-hybrid-war-puts-european-air-defences-test-2025-11-05/>
- RÚV. *Svíþjóð sér í fyrsta sinn um loftrýmisgæslu á Íslandi*. 12 February 2026. <https://www.ruv.is/frettir/innlent/2026-01-21-sviar-i-loftrymisgaeslu-vid-island-i-fyrsta-sinn-464496>
- Samgöngustofa. *Reglur um drónaflug*. <https://island.is/dronareglur>
- Silja Bára Ómarsdóttir and Guðbjörg Ríkey Th. Hauksdóttir. *In and of the Arctic: Security in Iceland*. Belfer Center for Science and International Affairs. 6 November 2025. <https://www.belfercenter.org/research-analysis/and-arctic-security-iceland>
- Stjórnarráð Íslands. *Inntak og áherslur stefnu í varnar- og öryggismálum: Inntak og áherslur stefnu í varnar- og öryggismálum. Skýrsla samráðshóps þingmanna 2025*. 12 September 2025. <https://www.stjornarradid.is/gogn/rit-og-skyrslur/stakt-rit/2025/09/12/Inntak-og-aherslur-stefnu-i-varnar-og-oryggismalum/>
- Vésteinn Örn Pétursson. *Kallar þjóðaröryggisráð saman*. Vísir, 30 September 2025. <https://www.visir.is/g/20252782217d/kallar-thjodaroryggis-rad-saman>
- Wikipedia. *Sérsvait ríkislögreglustjóra*. https://is.wikipedia.org/wiki/S%C3%A9rsveit_r%C3%ADkisl%C3%B6greglustj%C3%B3ra

