ALLAHABAD ACADEMIC PRESS
a publishing company

The Research Frontline - Journal

A Peer-Reviewed Quarterly Journal of Interdisciplinary Inquiry and Research

Journal homepage: https://trfjournal.cdfaindia.org/index.php/trfjournal/en/index

The Arctic's Ghost Signals: GNSS Interference, Hybrid Pressure, and the Security Politics of Critical Infrastructure in the European High North

Manashjyoti Karjee

To cite this article: Karjee M. (2026): The Arctic's Ghost Signals: GNSS Interference, Hybrid Pressure, and the Security Politics of Critical Infrastructure in the European High North, The Research Frontline - Journal (Vol 1, Issue 2, January - March 2026) DOI:https://doi.org/10.66871/trf-j.v1i2.019

To link to this article: https://doi.org/10.66871/trf-j.v1i2.019

Published online: 05 May 2026.

Submit your article to this journal

Vol. 1, Issue 2, January - March 2026

The Research Frontline - Journal (Vol. 1, Issue 2, January - March 2026)
https://doi.org/10.66871/trf-j.v1i2.019

ALLAHABAD ACADEMIC PRESS
a publishing company

The Arctic's Ghost Signals: GNSS Interference, Hybrid Pressure, and the Security Politics of Critical Infrastructure in the European High North

Manashjyoti Karjee[1]

[1]Researcher, Advanced Study Institute of Asia, New Delhi

ABSTRACT

Since 2014, following Russia's annexation of Crimea and renewed uncertainty over NATO cohesion and Greenland's strategic politics, Arctic states have hardened critical infrastructure: ports, radar systems, undersea cables, and energy sites—to reduce vulnerability. Yet the region's vast distances, limited redundancy, and civil-military overlap mean such measures can be perceived as coercive, increasing the risk of countermeasures. This paper examines when infrastructure hardening triggers a security-dilemma spiral and how design choices can limit that risk. It finds spirals are more likely when measures are dual-use, publicly signalled, militarily led, and near sensitive areas, and less likely when states invest in redundancy, maintain civilian governance, and communicate intentions clearly. It concludes with mitigation options, including shared protocols, clearer rules for protection missions, and resilience investments.

ARTICLE HISTORY
Received: 31 January 2026
Accepted: 30 March 2026

KEYWORDS
Artic; security dilemma; critical infrastructure; dual use; escalation

I. Introduction

Global Navigation Satellite System (GNSS) interference in the European Arctic should be read now because it no longer looks like a small technical irregularity in the frigid, polar region. It has come to appear, rather, as a repeated feature of an increasingly security-sensitive region.[90] In northern Norway and across the wider High North, repeated jamming and spoofing incidents have disrupted aviation and have also raised wider worries about the dependability of navigation systems on which remote northern societies heavily rely.[90] These incidents become crucial in a region where infrastructure is thin, alternatives are few, repairs when broken are slow and ordinary movement is closely tied to communication systems, surveillance arrangements, and visible state presence. They are also unfolding in an Arctic that can no longer be described very convincingly as insulated from wider geopolitical rivalry. The region is being shaped more and more by increasing military presence, alliance consolidation, and sharper forms of mistrust after Russia's war against Ukraine.[91] Something that might once have been treated as a local or operational disturbance now carries a wider resonance. GNSS disruption is interesting and important to look at because of where it is happening and the way it is now being read.

The puzzle of this essay comes directly out of that shift. Jamming and spoofing often remain ambiguous. Jamming is blocking or disrupting a GPS/GNSS signal so it cannot be received properly, while spoofing is sending a fake signal to mislead a receiver into showing the wrong position or time. They can disrupt civilian and state functions without producing visible destruction, and they often stay below the threshold at which an incident can be classified easily as an open armed attack.[92]

CONTACT: Manashjyoti Karjee manashjrkarjee@gmail.com

Yet in the Arctic, they still produce serious political and security concerns. Why does that happen? Why do acts that are often deniable, technically complicated, and difficult to attribute still provoke rising anxiety, new protective measures, and a wider language of threat? The answer cannot rest on technical disruption alone. If that were the case, GNSS interference would remain mostly a matter for engineers and regulators. But that is not how these incidents are being read. They are increasingly treated as politically meaningful. They are interpreted against a regional setting in which ambiguity itself has strategic value, and where even limited interference may be understood as coercive pressure, probing, or a test of response thresholds. The puzzle, then, is not only why GNSS disruption occurs, but why it comes to carry such a large security meaning in the contemporary Arctic.

This essay argues that, in the post-exceptionalist Arctic, GNSS disruption is being interpreted less as a mere technical anomaly and more as a form of hybrid interference or threat, to be more precise, directed at critical infrastructures and vital systems in a tense geopolitical setting.[93,94] Once interference is read that way, governments are pushed towards securitisation and hardening their policies to respond: they widen monitoring, restore backup systems, and fold infrastructure protection into broader security politics.[95] The core argument that follows, then, is that the politics of GNSS disruption lies not only in the initiating act but also in the responses it generates and the insecurity those responses can further produce.

The essay develops this argument in five steps. It starts by establishing the empirical problem and showing that repeated GNSS disruption in the European Arctic is real, recurring, and already serious enough to have altered operational expectations. It then turns to the literature on hybrid warfare to explain why ambiguous, deniable, and below-threshold methods have become strategically attractive. From there, it shows why jamming and spoofing fit hybrid warfare logic especially well and why they should be understood as interference with critical infrastructure rather than as isolated technical faults. The essay then places that problem within the wider geopolitics of the Arctic, with attention to the decline of Arctic exceptionalism, the consequences of 2014 and especially 2022, the consolidation of NATO's northern flank, and the sensitivity of the European High North and Svalbard. It ends by examining how repeated interference encourages securitisation and hardening, and why those defensive responses may themselves contribute to a security dilemma. The larger purpose is to show that Arctic critical infrastructure protection has become more than a matter of resilience; it has become a field of political and strategic interaction.

II. Establishing the empirical problem: GNSS disruption in the European Arctic

Across the European Arctic, interference with satellite navigation is now harder to dismiss as occasional technical noise. In northern Norway, above all in the airspace around Kirkenes and across eastern Finnmark, pilots and authorities have been dealing with repeated GPS disruption for several years. In Norway's border region with Russia, warnings to pilots about GPS jamming were already being issued before the present phase of Arctic tension had fully taken shape.10 In January 2025, the problem appeared in a sharper form when pilots reported spoofing during the approach to Kirkenes.3 By July 2025, interference had also been reported in Svalbard airspace.[4] Norway is not the only case here. Finland has had to strengthen alternative radio navigation at three eastern airports because GPS interference kept recurring, and Finnish authorities have also recorded jamming and spoofing affecting vessels at sea. [6,8]

These disruptions recur often enough to have changed how northern authorities deal with them. Reporting on Norwegian aviation disruption shows that jamming in Finnmark was recorded on 18 days in 2021, 122 days in 2022, and 294 days in 2023; by late February 2024, disturbances had already been logged on 44 days that year.[1] That looks like a case of escalation rather than a random chain of mishaps. The problem became so routine that Norway's communications authority stopped asking for ordinary interference reports from Finnmark, which was, really, an acknowledgement that the disturbance had become a chronic operating condition in that part of the country.[2] Airlines serving the region likewise described GPS loss as something repeated in northern flying, not some rare technical -

anomaly.[1] When spoofing started appearing alongside jamming, the operational picture became harder, not easier, to read.[3]

The effects are wide because GNSS sits underneath many of the systems on which remote northern societies rely. The clearest and most visible effects have appeared in civilian aviation, especially at smaller northern airports where satellite-assisted navigation matters a great deal in poor weather and difficult terrain.[6] In September 2025, GPS interference contributed to a Widerøe aircraft aborting its landing at Vardø in low visibility.[5] Still, the reach of these disruptions goes well beyond scheduled passenger flights. Finnish research and preparedness authorities have warned that interruptions in satellite positioning can produce extensive social and operational consequences, above all where redundancy is limited, and emergency response depends on reliable navigation and timing.[13] Maritime users are drawn in as well: Finnish authorities have linked jamming and spoofing to navigational disruption in nearby waters.[7,8]

Attribution, though, remains politically sensitive and analytically incomplete. In November 2018, Norway's Defence Ministry stated that jamming affecting civilian aircraft had come from Russian forces on the Kola Peninsula.[11] Later reporting continued to connect much of the interference affecting Finnmark to Russian activity across the border.[1] Even so, when the likely source appears strong, the meaning of a given episode is still not straightforward. It is often difficult to know whether a disruption reflects deliberate coercion, spillover from military training, defensive electronic activity, or some other operational logic.[3] In Svalbard, for instance, the source of the 2025 interference was still described as unknown. Finland has also publicly suspected Russia in cases of jamming and spoofing, while Moscow has denied involvement.[8]

This uncertainty is not a weakness in the case. It is part of why the issue is read politically. GNSS interference usually appears first as signal loss, false positioning, route instability, or cockpit alerts, rather than as dramatic physical destruction.[3,4] Because of that, authorities have to decide what kind of event they are facing before they can fully explain it. That burden of interpretation has already shaped state behaviour. Norway has strengthened monitoring of GPS interference in the High North because the problem has persisted.[12] Finnish preparedness authorities have, in much the same vein, argued that disruption to satellite positioning should be treated as a serious societal vulnerability, not a narrow technical inconvenience.[13] Seen this way, ambiguity does not lessen the weight of these incidents. It raises it, since states must decide under uncertainty whether they are facing a nuisance, hazard, or hostile action.[14]

The empirical conclusion seems fairly plain. The European Arctic is not dealing with a merely hypothetical vulnerability in navigation infrastructure. Northern Norway has already experienced repeated jamming serious enough to alter reporting practices,[1,2] and the problem has spread into newer forms too, including spoofing in Kirkenes and interference in Svalbard airspace.[3,4] Finland's response at eastern airports shows that neighbouring states are now adjusting their infrastructure to live with this pressure,[6] and these incidents have already started to reshape monitoring practices, mitigation efforts, and preparedness thinking in the wider region.[12,13] Before turning to the literature on hybrid warfare, the available evidence already shows that Arctic navigation disruption is a recurring operational problem with regional consequences.[1]

III. Hybrid warfare and why it is attractive

The term hybrid warfare is widely used, though it remains contested, and that makes conceptual precision necessary while dealing with it.[15] At its strongest, the concept refers not to a single tactic but to the coordinated use of different instruments of coercion, including conventional force, irregular methods, information operations, coercive signalling, and other disruptive practices, used in ways meant to reinforce one another politically and operationally.[16] What makes such warfare "hybrid" is not mere variety on its own. It is the deliberate combination of military and non-military means within the same design.[17] More recent scholarship sharpens this point by arguing that hybrid warfare is best -

understood not simply as a doctrinal category, but as a mode of organised coercion that exploits the blurred line between peace and war.[18] Read that way, hybrid warfare is less a departure from politics than a means of pursuing political goals through calibrated, multi-domain pressure without immediately crossing into open conventional conflict.[19]

Hybrid methods have become attractive because they offer a way to compete with stronger adversaries without fighting on terms that would favour them.[20] For actors facing the conventional military superiority of NATO or other advanced powers, hybrid approaches create room to offset weakness through dispersion, deniability, and the selective use of pressure below the threshold that would trigger a decisive response.[21] They leave room for calibration as well. Since the tools involved are often reversible, hard to attribute at once, or ambiguous in legal and political terms, they allow states to impose costs while keeping some freedom to de-escalate, deny, or redefine what they are doing.[22] That makes hybrid methods useful for limited political purposes: probing defences, unsettling civilian confidence, complicating command decisions, and testing the adversary's appetite for retaliation.[23] The attraction of hybrid warfare, then, lies not in battlefield victory alone. It lies in the ability to shape an opponent's choices while avoiding the risks of full-scale war.[24]

Ambiguity is not some accidental by-product of hybrid warfare; it is one of its, if not the most central, advantages.[25] As Mumford and Carlucci argue, ambiguity creates a cognitive impasse in which the target struggles to determine what is happening, who is responsible, and what political objective lies behind the action.[26] That uncertainty slows consensus, complicates attribution, and makes it harder for governments and alliances to decide whether a particular act is criminal, coercive, military, or merely accidental.[27] This is even more true for democratic governments because of transparency and checks and balances in place. The effect becomes stronger when states operate through intermediaries, proxies, auxiliaries, or affiliated actors, because the link between the visible event and the actor ultimately directing it becomes harder to prove quickly or conclusively.[28] Legal ambiguity matters as well. Hybrid methods often make use of the fact that international law and public doctrine draw their clearest lines around overt armed force, leaving more room for manoeuvre in actions that remain deniable, indirect, or difficult to classify.[29] For the attacker, ambiguity buys time, space, and political flexibility. For the defender, it creates hesitation at the very point where clarity is most needed.[30]

Hybrid warfare becomes especially relevant when geopolitical rivalry is intense but open war still appears too costly, dangerous, or escalatory for the actors involved.[31] This situation can very closely define the Arctic geopolitics, divided between the NATO camp and Russia. In those settings, states look for ways to pressure and weaken one another without presenting a single, unmistakable casus belli.[32] The point is not always to win a decisive military encounter. It may instead be to alter the strategic environment bit by bit: to probe red lines, create doubt, erode confidence, and push the adversary into a reactive posture.[33] Here, Kilcullen's idea of liminal manoeuvre is very useful for the paper. He claims that Russia and similar actors have become adept at operating in the threshold space between war and peace, detectability and deniability, where action can be forceful enough to matter but still ambiguous enough to complicate response.[34] Liminal manoeuvre is attractive precisely because it lets the initiator "ride the edge" of escalation, gaining political or operational advantage without fully committing to open war.[35] In periods of sharpened confrontation short of direct conflict, hybrid warfare is not peripheral to strategy. It becomes one of its more practical instruments.[36]

The Arctic is especially open to this sort of pressure because many of the conditions favouring hybrid tactics are already built into the region's physical and political landscape.[37] Critical infrastructure is sparse, distances are long, weather conditions are severe, and redundancy is often limited, so even fairly modest disruption can have outsized effects on mobility, communications, and governance.[38] Arctic security is also marked by a persistent tension between cooperation and rivalry: the region cannot be reduced either to pure exceptionalism or to open confrontation, and that ambiguity itself makes sub-threshold pressure more potent.[39] Recent scholarship on Svalbard and the waters around northern Norway helps show why. The Arctic is a setting in which actors, means, and intentions are not

always immediately apparent, while legal disputes, jurisdictional sensitivities, and dual-use infrastructures open space that hybrid tactics can exploit.[40] In that light, the repeated GNSS jamming and spoofing traced in the previous section fits the literature quite closely: it occurs in a region where ambiguity, infrastructural vulnerability, and geopolitical sensitivity converge.[41]

IV. Why jamming and spoofing fit hybrid warfare logic

Jamming and spoofing should not be treated as ordinary technical breakdowns because they do something rather different from routine malfunctions. A malfunction interrupts a system from within: equipment fails, software glitches, weather distorts reception, or some component simply stops working. Jamming and spoofing, by contrast, are forms of intentional interference aimed at the integrity of navigation itself.[42] Jamming tries to overwhelm or suppress legitimate signals so that the receiver cannot function normally, whereas spoofing works in a more deceptive way: it feeds the receiver false signals that appear authentic and can, as a result, produce incorrect position, navigation, or timing outputs without immediately showing that anything is wrong.[42,43] That distinction matters analytically. A broken system creates a problem of repair. A manipulated system creates a problem of trust. Once navigation can be distorted from outside, the issue is no longer only one of technical reliability. It becomes a matter of adversarial control over the informational environment on which mobility and coordination depend.

These tactics fit hybrid warfare especially well because they combine low visibility with meaningful operational effect. They are comparatively inexpensive, difficult to attribute immediately, scalable in intensity, and often reversible once the signal environment changes.[42,45] Most importantly, they generate disruption without producing the kind of dramatic physical destruction that would make classification easy. An airport approach becomes unstable, a vessel loses confidence in its position, a timing-dependent system behaves unpredictably, or an operator is forced to abort or reroute. The insecurity produced is real, but it does not arrive in a form that automatically triggers the political clarity associated with missile strikes or kinetic sabotage. That is exactly why these methods sit so easily within hybrid logic. They allow an actor to interfere, unsettle, and impose costs while still keeping room for denial, reinterpretation, and diplomatic evasion. Jamming and spoofing are useful, then, not because they destroy infrastructure outright, but because they make infrastructure unreliable at politically sensitive moments.

In contested spaces, that kind of interference becomes strategically useful for reasons that go beyond simple disruption. It can expose where a target depends most heavily on fragile systems, reveal how quickly authorities can detect anomalies, and show whether civilian operators, regulators, and military actors respond in coordinated or fragmented ways.[44] Jamming and spoofing can also work as tests of threshold: they pressure the adversary to decide what counts as nuisance, what counts as coercion, and what counts as a hostile act worth answering. Kilcullen's idea of liminal manoeuvre is helpful here because it sharpens the point. The value of operating in the threshold space between peace and war lies in being forceful enough to shape behaviour while still remaining ambiguous enough to complicate response.[44] GNSS interference does exactly this. It can probe, signal, and unsettle without giving up deniability. Over time, repeated interference can also wear away confidence in the ordinary systems that make everyday movement possible. That matters because, once daily navigation becomes uncertain, the target is pushed to devote more resources to monitoring, redundancy, and protection, even where the attacker never crosses into open confrontation.

Taken together, these features show why GNSS interference matters politically in the European Arctic. In a remote but strategically sensitive region, interference with navigation systems affects access, surveillance, emergency response, logistics, and state presence rather than being a stand-alone technical function.[46,47] What begins as a disturbance in positioning or timing, therefore, becomes part of a wider struggle over confidence, vulnerability, and the interpretation of intent.[46] The next section develops that point by treating navigation systems as critical and geopolitical infrastructure.

V. Critical infrastructure and why it is political in the Arctic

Critical infrastructure is usually understood as the set of systems and assets whose disruption would seriously impair the basic functioning of society, the continuity of government, economic life, and national security.[48] But that definition needs to be read more broadly than as a simple checklist of sectors. As Collier and Lakoff suggest, modern societies rely on interconnected "vital systems" whose failure can quickly spill across domains that are normally treated as separate, such as transport, energy, communication, finance, and emergency response.[49] Critical infrastructure matters, then, not only because it keeps daily life going, but because it underpins the state's capacity to govern crisis, maintain order, and sustain collective life under strain. In that sense, critical infrastructure is not merely important equipment. It is the material basis on which social and political order rests.

Once the infrastructure is understood that way, its political character comes into view more clearly. Infrastructure is never just inert background support. As Brian Larkin argues, infrastructures organise circulation: they shape how goods, people, information, power, and authority move across space.[50] They privilege some routes, actors, and forms of dependence over others. To build infrastructure is to make choices about connection, vulnerability, access, and control; to secure it is to decide what forms of life and authority are to be protected first. This is why infrastructure protection cannot be reduced to engineering alone. It is also a matter of governing interdependence. Decisions about redundancy, backup systems, ownership, surveillance, and protection all distribute power. Put a bit differently, infrastructure is political not only when it fails, but already in the way it structures everyday order and marks out what counts as a tolerable risk.

Seen from that angle, navigation and positioning systems plainly belong within the category of critical infrastructure. GNSS does not simply help users find where they are. It supports aviation approaches, maritime movement, logistics, search and rescue, timing-dependent communications, and a wide range of civilian and state functions that rely on accurate position and time.[51] In the Arctic, that role is even more pronounced because space-based navigation, communication, and observation are often prerequisites for movement, coordination, and connectivity across remote environments.[52] That means interference with GNSS is not only a technical inconvenience for pilots or vessels. It affects a foundational layer of how movement is organised and trusted. When positioning becomes unreliable, the problem reaches into the operational routines through which authorities, firms, and communities hold space together.

Critical infrastructure matters more sharply in the Arctic because the region intensifies both dependence and vulnerability. Distances are long, settlements are dispersed, weather conditions are severe, and redundancy is often limited. When infrastructure fails in a dense metropolitan setting, alternatives may exist nearby. In the Arctic, those alternatives are often fewer, slower, and more expensive to mobilise. Research on circumpolar infrastructure shows that Arctic systems are already under pressure from environmental exposure, permafrost change, and high replacement costs.[53] At the same time, scholarship on Arctic connectivity stresses that infrastructure in the region cannot be treated as a generic technical issue, because remote communities depend on connective systems that are tailored, and often somewhat fragile, to sustain ordinary life and wider economic links.[54] This makes infrastructure failure more consequential and infrastructure protection more politically charged. The Arctic does not simply contain infrastructure; much of Arctic social and political life is made possible only through infrastructure that is unusually exposed and difficult to replace.

In the Arctic, moreover, infrastructure is never only civilian. Ports, airports, undersea cables, satellite links, radar systems, navigation networks, and energy installations are also tied to sovereignty, monitoring, strategic access, and military mobility. As Østhagen argues, Arctic security dynamics are driven less by a single self-contained "Arctic region" than by the way broader strategic competition, especially involving Russia and NATO, is refracted through northern spaces and infrastructures.[55] This is especially visible around Svalbard and the European High North, where ordinary governance arrangements intersect with disputes over jurisdiction, access, and security significance.[56] Svalbard is

useful here because its infrastructure does more than serve residents or tourists. They also express Norwegian presence, make administration possible in a legally sensitive territory, and shape how other actors read sovereignty in practice.[57] Infrastructure in the Arctic is therefore geopolitical: it helps states occupy, govern, monitor, and signal in places where physical presence and logistical reach are themselves politically meaningful.

Once navigation systems are understood as critical and geopolitical infrastructure, repeated GNSS interference is best read as a challenge to the reliability of the systems through which authority and presence are exercised in the High North.[52,56] The disruption happens at the level of signal, but its effects travel upward into governance, preparedness, and threat perception. This is why GNSS interference fits so closely into a hybrid framework: it targets the material conditions of order without necessarily crossing the threshold of overt physical attack.

For that reason, protecting critical infrastructure in the Arctic is not simply a matter of resilience in the narrow sense of recovery and adaptation. It is also a question of power. To harden infrastructure is to decide who monitors it, who owns it, who may access it, what risks justify exceptional coordination, and how civilian systems should be linked to security institutions. In contested northern spaces, those choices take on additional meaning because they can be read as efforts not only to protect daily life but also to consolidate strategic position. Protection, then, is never politically innocent. That is what makes critical infrastructure such an important bridge in the essay between hybrid disruption and the politics of response.

VI. Situating the problem in Arctic geopolitics

For much of the post-Cold War period, the Arctic was often described in the language of exceptionalism: a region where practical cooperation, scientific exchange, and institutional restraint could continue even when relations between Russia and the West were tense elsewhere.[58] That description was never fully apolitical, but it did capture something real about the regional order that emerged around the Arctic Council, the Barents framework, and a broader norm of keeping Arctic cooperation apart from wider confrontation.[59] That order has narrowed quite sharply now. The Arctic can no longer really be treated as insulated from global rivalry. Cooperation has not disappeared altogether, no, but it has become thinner, more selective, and more fragile, while strategic competition has become more openly visible in military planning, alliance thinking, and public threat perception.[59,60]

The turning point did not begin in 2022. Russia's annexation of Crimea in 2014, and the worsening of Russia-West relations that followed, began reshaping the Arctic security environment much earlier.[60] After 2014, it became harder to sustain the idea that the High North could remain politically detached from the wider European security order. Western states had increasingly to think about Russian military modernisation, Arctic force posture, and the possibility that Moscow was using the language of "low tension" while steadily improving its relative position in the region.[60] In that sense, 2014 mattered because it weakened trust before institutions had formally broken down. It altered the background assumptions through which Arctic developments were being interpreted, even while many cooperative arrangements remained formally in place.[60,65]

Russia's full-scale invasion of Ukraine in February 2022 changed the Arctic more deeply because it broke not only trust but also the institutional habits that had sustained Arctic governance. On 3 March 2022, the seven Western Arctic states announced that they were temporarily pausing participation in Arctic Council meetings under Russia's chairship.[61] On 8 June 2022, those same states announced only a limited resumption of work in projects that did not involve Russian participation.[62] The Barents Euro-Arctic cooperation framework was also suspended in March 2022.63 What followed was not the complete disappearance of Arctic cooperation, but its fragmentation. What had once been treated as a fairly durable regional exception now had to operate under the shadow of war, sanctions, and an openly divided political order.[61,62,63]

The allied side of the regional balance changed as well. Finland became a NATO member on 4 April 2023, and Sweden followed on 7 March 2024.[64] Those two accessions did more than add new members. They consolidated NATO's northern flank, changed the strategic geography of the Nordic-Baltic space, and gave the alliance a much more integrated position in the European Arctic.[64] This matters for the argument because incidents in the High North are no longer read against the older background of Nordic military non-alignment. They are, more and more, interpreted within a more explicitly allied frame. For NATO states, this raises the salience of deterrence and infrastructure protection. For Russia, it sharpens the sense that the northern theatre forms part of a broader confrontation with the alliance.[64,65]

Russia is central to this discussion not because every Arctic incident can be mechanically attributed to Moscow, but because Russia possesses both the capability and the strategic incentive to use ambiguous tools in contested northern spaces.[60] The problem is not simply one of military inventory, though that matters. It is also a strategic logic. As Finnish analysts have argued, Russia benefited from Western attachment to Arctic exceptionalism while systematically improving its own military and hybrid position in the region.[60] Pavel Baev makes a similar point from a strategic angle: in the Arctic theatre, the level of direct threat to Russian core interests is relatively low, while Russia's capacity to threaten NATO interests from a position of relative regional strength is high.[66] Under those conditions, below-threshold and deniable methods become especially attractive, because they allow Moscow to signal, probe, deter, and unsettle without openly escalating to war.[60,66]

The European High North is especially sensitive because it lies at the intersection of Russia's strategic nuclear posture, NATO's northern access routes, and the everyday governance of a sparsely connected Arctic frontier. The Kola Peninsula remains the core of Russia's Northern Fleet and hosts submarines, strategic bombers, cruise-missile capabilities, and other assets central to Russian deterrence.[65,66] The Barents Sea is not just another maritime space. It forms part of the protective "bastion" around sea-based nuclear forces and a zone through which questions of surveillance, anti-access, and allied reinforcement are filtered.[66] Northern Norway and Finnmark matter here because they face that military complex directly, while also serving as spaces through which NATO presence, monitoring, and political signalling become visible. This is why the European Arctic is so difficult to stabilise rhetorically: local infrastructure, regional mobility, and great-power deterrence are layered on top of one another.[65,66]

Svalbard sharpens these tensions further because it is not merely a remote Arctic locality; it is a legally unusual and politically symbolic space. Norway has sovereignty over the archipelago, but that sovereignty is exercised under the constraints of the 1920 Svalbard Treaty, which combines Norwegian authority with non-discrimination obligations and restrictions related to military use.[67,68] As Østhagen shows, Svalbard's sensitivity lies less in a single "dispute" than in a cluster of overlapping issues: challenges to Norwegian policies on land, disagreement over the treaty's application to maritime zones, and the possibility that the archipelago could acquire military significance in a broader confrontation with Russia.[67] That combination makes Svalbard unusually vulnerable to symbolic contestation. Acts are rarely read only in local terms; they are quickly folded into larger arguments about sovereignty, access, and strategic intent.[67,68]

Under these conditions, ambiguous GNSS interference is much more likely to be interpreted through the language of competition, probing, and grey-zone pressure than it would be in a lower-tension regional order. The same disruption that might once have been bracketed as a technical nuisance or military spillover now appears inside a much more suspicious interpretive environment. The reason is not hard to see: the Arctic is no longer read as a sheltered arena of cooperation, and the European High North is already saturated with concerns about deterrence, infrastructure vulnerability, and hybrid tactics.[60,65] This does not mean that every episode proves a coordinated coercive campaign. What it means is that the geopolitical setting has changed the burden of interpretation. Ambiguous interference now resonates politically much faster because it occurs where trust is weak, signalling matters, and even modest disruptions can be read as strategic tests.[60,65,67]

The geopolitical conclusion, then, is that GNSS disruption in the European Arctic now unfolds in a regional order shaped by NATO-Russia rivalry, institutional rupture, and shrinking trust.[59,61,64] In that setting, even modest interference is read against wider concerns about sovereignty, deterrence, and strategic access.[59,65,67] This altered interpretive environment is what makes the politics of response so important in the next section.

VII. Securitisation, hardening, and the politics of response

To securitise GNSS disruption is not simply to say that it matters. It is to recast it as a threat serious enough to justify heightened attention, quicker coordination, and measures that go beyond routine technical management.[69] In practical terms, securitisation takes place when officials stop treating interference as an isolated operational inconvenience and start presenting it as part of a wider problem of national preparedness, critical infrastructure vulnerability, and hostile pressure.[70] With that shift, the issue moves out of the register of maintenance and troubleshooting and into the register of security governance. The technical dimension does not disappear, exactly. It is absorbed into a broader claim: signal interference threatens functions in which the state cannot afford to lose confidence. Once that happens, the response is no longer left only to engineers, air traffic personnel, or telecom regulators. It becomes a matter for ministries, security agencies, alliance consultation, and exceptional protective planning.

States are pushed in that direction here because purely technocratic management is no longer adequate to the scale and meaning of the problem. Repeated disturbances in Finnmark became so routine that the Norwegian Communications Authority stopped asking for ordinary reports from that region, which is itself a sign that the issue had grown beyond normal incident handling.[71] In Finland, officials have linked GPS interference to a wider pattern of hostile activity associated with Russia, alongside sabotage, cyber pressure, and other disruptive acts.[72] At the same time, Finnish preparedness authorities have warned that large-scale disruption to satellite positioning would produce broad societal, economic, and security consequences, especially because critical functions depend more and more on GNSS.[73] Together, repeated disruption, infrastructural dependence, and geopolitical suspicion push governments to treat the issue as part of a wider threat environment rather than as a series of disconnected malfunctions.

Once GNSS interference is interpreted as a security issue, the range of response widens quickly. One response is redundancy: in eastern Finland, airports have reintroduced and upgraded radio-navigation equipment so that aircraft can land without relying exclusively on satellite guidance.[76] Another is monitoring and detection: Norway has expanded its measurement and analysis capacity in the High North and decided to open a Norwegian Communications Authority office in Tromsø to shorten response times to Finnmark and Svalbard.[74] The same authority has also tested an AI model designed to distinguish deliberate jamming from other kinds of signal error, which suggests that detection itself is becoming part of preparedness.[75] A third response is institutional coordination. At the allied level, NATO has created a Critical Undersea Infrastructure Coordination Cell and later expanded civilian-military cooperation, information sharing, and preparedness around vulnerable infrastructure more generally.[77,78] Even if not all these measures focus only on GNSS, they show the same hardening logic: build backup, improve sensing, thicken coordination, and reduce the space in which ambiguous disruption can succeed cheaply.

These measures are not purely technical because they redistribute authority and alter the governing architecture around infrastructure. When monitoring is intensified, telecom regulators do not simply gather better data; they become more closely tied to security policy. When fallback systems are restored, infrastructure operators are deciding which vulnerabilities are politically intolerable and worth funding against.[73,76] When NATO builds coordination mechanisms around critical infrastructure, the issue is inserted into a wider framework of allied deterrence, military awareness, and strategic response.[77,78] The Norwegian case makes this especially plain. The planned Tromsø presence is justified not only in terms of convenience, but in terms of the changed security-policy situation in Northern Norway and the need for faster reaction in strategically important areas such as Eastern Finnmark and Svalbard.[74] Hardening, therefore, changes who is authorised to watch, classify, coordinate, and respond.

How does infrastructure protection become part of broader deterrence signalling?

Protection measures function as signals too. They tell adversaries, allies, and domestic audiences that the state is alert to below-threshold pressure, capable of adaptation, and willing to treat ambiguous

interference as strategically relevant.[79] Reintroducing fallback systems, improving sensing, widening information sharing, and visibly strengthening the state's presence in the High North communicates that interference will be monitored and politically noticed.[74,77,78] Once protection becomes legible in that way, the question is no longer only whether systems are safer, but how other actors read the measures. That takes the essay directly to the security dilemma.

VIII. The security dilemma: when defensive protection produces further insecurity

The central dilemma in this essay is that measures adopted for protection do not carry one fixed meaning only. In classical security-dilemma terms, states often take steps to increase their own security that are defensive in intention but threatening in effect, because others cannot be sure how those measures will be used or where they might lead.[80] Jervis's original point remains directly relevant here: even actors motivated mainly by security can still generate fear in others when the means of defence are difficult to distinguish from the means of coercion.[80] That insight matters for infrastructure protection because many of the measures associated with resilience, such as tighter monitoring, expanded surveillance, more integrated civil-military coordination, hardened access control, or closer alliance involvement, may also be read as preparation for denial, control, and strategic consolidation.[81] Defensive protection, then, is not politically transparent. Once infrastructure becomes entangled with competition, protection itself can start to look like posture.

This logic applies especially sharply in the European Arctic because the region is already saturated with mistrust, military sensitivity, and symbolic over-reading. As Friis shows, the European Arctic now has to be understood as a space of mutual deterrence signalling in which both Russia and NATO watch each other's moves closely, even when day-to-day activity remains more measured than alarmist rhetoric sometimes suggests.[82] That means relatively modest steps can acquire strategic meaning out of proportion to their immediate technical purpose. A new monitoring node in Northern Norway, a more integrated allied role in infrastructure security, or a more visible pattern of resilience exercises may be read in Moscow not simply as prudent protection but as part of a broader tightening of NATO's northern posture.[82,83] The same dynamic works in reverse, too. Russian activity that may be explained domestically as defensive or routine is likely to be interpreted on the allied side through the lens of coercion and probing. In a theatre shaped by proximity to the Kola complex, alliance boundaries, and strategic maritime access, the political meaning of protective acts does not really stay local.

Ambiguity, moreover, does not disappear when states move from diagnosis to response. It shifts to another level. One side may see backup systems, expanded sensing, and closer coordination as clearly defensive steps meant to stabilise vulnerable infrastructure. The other may see those same measures as evidence of a more ambitious effort to consolidate presence or deepen alliance integration.[81,82] The response phase is therefore analytically as important as the disruption phase. In the Arctic, where legal complexity, symbolic signalling, and strategic geography overlap, countermeasures can become part of the same interpretive struggle as the incidents they were supposed to address.[84,85]

Once that happens, hardening can begin to reproduce the very insecurity it is meant to manage. If one side interprets recurring GNSS interference as a sign that it must thicken surveillance, widen coordination, and protect critical systems more visibly, the other side may respond not with reassurance but with counter-monitoring, rhetorical escalation, or added pressure designed to test whether the new posture has changed anything important.[80,81] In the Arctic, this process seems more likely to be incremental than dramatic: repeated rounds of disruption and hardening can gradually make the region more tense, more heavily monitored, and more politically brittle even when neither side publicly declares expansionist intent.[82.83]

That does not mean the dilemma is unmanageable. Classical security-dilemma theory has long suggested that spirals can be softened when states make their defensive intentions more legible and when postures are designed in ways less easily mistaken for offensive preparation.[80,81] In the Arctic context, that suggests several practical lessons. First, communication channels still matter, especially

in the European High North, where misunderstandings can spread quickly from local incidents into wider strategic interpretation. Second, some defensive measures may need clearer public framing so that they are seen as resilience-oriented rather than as a concealed extension of military posture. Third, legal and institutional clarity matters because ambiguity over jurisdiction, infrastructure status, and permissible activity can intensify suspicion unnecessarily.[84,85] None of these steps will eliminate rivalry. They may, though, reduce the likelihood that every protective response is automatically folded into a more dangerous story of encroachment and escalation.

The broader theoretical implication, then, is that Arctic critical infrastructure protection should not be analysed only as a resilience policy. It should be understood as a field of strategic interaction shaped by signalling, interpretation, and the security dilemma.[82,83] In this setting, even backup systems and monitoring upgrades acquire political meaning beyond their immediate function.[80,81] That is why the paper's central claim matters beyond GNSS too: in the contemporary Arctic, the protection of critical infrastructure is itself part of the region's security politics.

IX. Conclusion

This essay has shown that GNSS disruption in the European Arctic is a recurring problem with clear political significance.[86] Because navigation systems underpin mobility, emergency response, surveillance, and state presence in a sparse and strategically sensitive region, repeated jamming and spoofing fit the logic of hybrid warfare: they are ambiguous, deniable, and disruptive without necessarily crossing into open attack.[87,88] In the contemporary Arctic, those incidents are interpreted within a geopolitical environment marked by the erosion of Arctic exceptionalism, intensified NATO-Russia rivalry, and declining institutional trust, which in turn encourages securitisation and hardening.[89]

The importance of this argument goes beyond GNSS interference alone. Low-visibility acts can reshape regional security not only through the immediate disruption they cause, but through the precautionary responses and interpretive struggles they set in motion.[88,89] Managing Arctic hybrid threats, therefore, requires not resilience alone, but also careful signalling and institutional clarity so that efforts to reduce vulnerability do not deepen suspicion more than they must.

Citations

1. Thomas Nilsen, "Russian Jamming Is Now Messing Up GPS Signals for Norwegian Aviation Practically Every Day," ArcticToday, February 26, 2024, https://www.arctictoday.com/russian-jamming-is-now-messing-up-gps-signals-for-norwegian-aviation-practically-every-day/. Accessed March 7, 2026.
2. Trine Jonassen, "Stops Registering GPS Disruptions in Finnmark, Northern Norway," High North News, September 27, 2024, https://en.highnorthnews.com/politics/stops-registering-gps-disruptions-in-finnmark-northern-norway/212107. Accessed March 4, 2026.
3. Thomas Nilsen, "Russia Intensifies Electronic Warfare against Norway: 'We Were Spoofed on Approaching Kirkenes Today,'" ArcticToday, January 20, 2025, https://www.arctictoday.com/russia-intensifies-electronic-warfare-against-norway-we-were-spoofed-on-approaching-kirkenes-today/. Accessed March 12, 2026.
4. Thomas Nilsen, "Someone Is Messing with GPS Signals in Svalbard Airspace," ArcticToday, July 21, 2025, https://www.arctictoday.com/someone-is-messing-with-gps-signals-in-svalbard-airspace-2/. Accessed March 11, 2026.
5. Thomas Nilsen, "Widerøe Plane Forced to Abort Landing at Vardø Airport due to GPS Interference," The Barents Observer, September 16, 2025, https://www.thebarentsobserver.com/security/wideroe-plane-forced-to-abort-landing-at-vardo-airport-due-to-gps-interference/437146. Accessed March 11, 2026.
6. Anne Kauranen, "Three Finnish Airports Mitigate Russian GPS Interference with Radio Navigation," Reuters, November 7, 2024, https://www.reuters.com/business/aerospace-defense/three-finnish-airports-mitigate-russian-gps-interference-with-radio-navigation-2024-11-07/. Accessed March 8, 2026.

7. “Finnish Coast Guard Reports GPS Interference and ‘Shadow Fleets’ in Baltic Sea,” Yle News, October 31, 2024, https://yle.fi/a/74-20121555. Accessed March 7, 2026.
8. Anne Kauranen, “Finland Detects Satellite Navigation Jamming and Spoofing in Baltic Sea,” Reuters, October 31, 2024, https://www.reuters.com/world/europe/finland-detects-satellite-navigation-jamming-spoofing-baltic-sea-2024-10-31/. Accessed March 6, 2026.
9. Thomas Nilsen, “More Russian GPS Jamming than Ever across Border to Norway,” The Barents Observer, July 9, 2022, https://www.thebarentsobserver.com/security/more-russian-gps-jamming-than-ever-across-border-to-norway/161843. Accessed March 17, 2026.
10. Thomas Nilsen, “Pilots Again Warned of GPS Jamming in Norway’s Border Region to Russia,” The Barents Observer, January 10, 2019, https://www.thebarentsobserver.com/security/pilots-again-warned-of-gps-jamming-in-norways-border-region-to-russia/157025. Accessed March 5, 2026.
11. Thomas Nilsen, “GPS Jamming Came from Kola, Defense Ministry in Norway Confirms,” The Barents Observer, November 13, 2018, https://www.thebarentsobserver.com/security/gps-jamming-came-from-kola-defense-ministry-in-norway-confirms/155625. Accessed March 4, 2026.
12. Astri Edvardsen, “Strengthens the Monitoring of GPS Interference in the High North,” High North News, August 27, 2025, https://en.highnorthnews.com/politics/strengthens-the-monitoring-of-gps-interference-in-the-high-north/179931. Accessed March 6, 2026.
13. “Disruptions in Satellite Positioning Can Cause Extensive Damage to Society – Preparedness Should Be Strengthened by Increasing Research,” National Land Survey of Finland, June 11, 2025, https://www.maanmittauslaitos.fi/en/topical_issues/disruptions-satellite-positioning-can-cause-extensive-damage-society-preparedness. Accessed March 10, 2026.
14. Astri Edvardsen, “Northern Norway Is Likely Facing a More Serious Hybrid Threat Situation, Says Professor,” High North News, October 29, 2024, https://en.highnorthnews.com/politics/northern-norway-is-likely-facing-a-more-serious-hybrid-threat-situation-says-professor/223634. Accessed March 11, 2026.
15. Bettina Renz, “Russia and ‘Hybrid Warfare’,” Contemporary Politics 22, no. 3 (2016): 283–300, https://doi.org/10.1080/13569775.2016.1201316. Accessed March 4, 2026.
16. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Arlington, VA: Potomac Institute for Policy Studies, 2007).
17. Ibid.
18. Andrew Mumford, “Understanding Hybrid Warfare,” Cambridge Review of International Affairs 33, no. 6 (2020): 824–27, https://doi.org/10.1080/09557571.2020.1837737. Accessed March 10, 2026.
19. Andrew Mumford and Pascal Carlucci, “Hybrid Warfare: The Continuation of Ambiguity by Other Means,” European Journal of International Security 8, no. 2 (2023): 192–206, https://doi.org/10.1017/eis.2022.19. Accessed March 17, 2026.
20. David Kilcullen, The Dragons and the Snakes: How the Rest Learned to Fight the West (Oxford: Oxford University Press, 2020).
21. Ibid.
22. Mumford and Carlucci, “Hybrid Warfare.”
23. Kilcullen, The Dragons and the Snakes.
24. Mumford and Carlucci, “Hybrid Warfare.”
25. Ibid.

26. Ibid.
27. Renz, “Russia and ‘Hybrid Warfare’.”
28. Vladimir Rauta, “Towards a Typology of Non-State Actors in ‘Hybrid Warfare’: Proxy, Auxiliary, Surrogate and Affiliated Forces,” Cambridge Review of International Affairs 33, no. 6 (2020): 868–87, https://doi.org/10.1080/09557571.2019.1656600. Accessed March 11, 2026.
29. Hitoshi Nasu, “Challenges of Hybrid Warfare to the Implementation of International Humanitarian Law in the Asia-Pacific,” in Asia-Pacific Perspectives on International Humanitarian Law, ed. Suzannah Linton, Tim McCormack, and Sandesh Sivakumaran (Cambridge: Cambridge University Press, 2019), https://doi.org/10.1017/9781108667203.014. Accessed March 18, 2026.
30. Mumford and Carlucci, “Hybrid Warfare.”
31. Ibid.
32. Kilcullen, The Dragons and the Snakes.
33. Mumford and Carlucci, “Hybrid Warfare.”
34. Kilcullen, The Dragons and the Snakes.
35. Ibid.
36. Mumford and Carlucci, “Hybrid Warfare.”
37. Luis Suter, Dmitry Streletskiy, and Nikolay Shiklomanov, “Assessment of the Cost of Climate Change Impacts on Critical Infrastructure in the Circumpolar Arctic,” Polar Geography 42, no. 4 (2019): 267–86, https://doi.org/10.1080/1088937X.2019.1686082. Accessed March 12, 2026.
38. Ibid.
39. Andreas Østhagen, “The Arctic Security Region: Misconceptions and Contradictions,” Polar Geography 44, no. 1 (2021): 55–74, https://doi.org/10.1080/1088937X.2021.1881645. Accessed March 4, 2026.
40. Cecilie Juul Stensrud and Andreas Østhagen, “Hybrid Warfare at Sea? Russia, Svalbard and the Arctic,” Scandinavian Journal of Military Studies 7, no. 1 (2024): 111–30, https://doi.org/10.31374/sjms.233; Alaa Al-Aridi, “Legal Complexities of Hybrid Threats in the Arctic Region,” Teisė 112 (2019): 107–23, https://doi.org/10.15388/Teise.2019.112.6. Accessed March 9, 2026.
41. Stensrud and Østhagen, “Hybrid Warfare at Sea?”; Østhagen, “The Arctic Security Region.”
42. Lianxiao Meng, Lin Yang, Wu Yang, and Long Zhang, “A Survey of GNSS Spoofing and Anti-Spoofing Technology,” Remote Sensing 14, no. 19 (2022): 4826, https://doi.org/10.3390/rs14194826. Accessed March 17, 2026.
43. Yang Liu, Sihai Li, Qiangwen Fu, and Zhenbo Liu, “Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System,” Sensors 18, no. 5 (2018): 1433, https://doi.org/10.3390/s18051433. Accessed March 14, 2026.
44. David Kilcullen, “Liminal Warfare,” in The Dragons and the Snakes: How the Rest Learned to Fight the West (New York: Oxford University Press, 2020), 115–66, https://doi.org/10.1093/oso/9780190265687.003.0006. Accessed March 12, 2026.
45. Andrew Mumford and Pascal Carlucci, “Hybrid Warfare: The Continuation of Ambiguity by Other Means,” European Journal of International Security 8, no. 2 (2023): 192–206, https://doi.org/10.1017/eis.2022.19. Accessed March 8, 2026.

46. Cecilie Juul Stensrud and Andreas Østhagen, “Hybrid Warfare at Sea? Russia, Svalbard and the Arctic,” Scandinavian Journal of Military Studies 7, no. 1 (2024): 111–30, https://doi.org/10.31374/sjms.233. Accessed March 10, 2026.
47. Andreas Østhagen, “The Arctic Security Region: Misconceptions and Contradictions,” Polar Geography 44, no. 1 (2021): 55–74, https://doi.org/10.1080/1088937X.2021.1881645. Accessed March 14, 2026.
48. OECD, Protection of “Critical Infrastructure” and the Role of Investment Policies Relating to National Security, OECD Working Papers on International Investment, no. 2008/01 (Paris: OECD Publishing, 2008), https://doi.org/10.1787/7d159744-en. Accessed March 7, 2026.
49. Stephen J. Collier and Andrew Lakoff, “Vital Systems Security: Reflexive Biopolitics and the Government of Emergency,” Theory, Culture & Society 32, no. 2 (2015): 19–51, https://doi.org/10.1177/0263276413510050. Accessed March 6, 2026.
50. Brian Larkin, “The Politics and Poetics of Infrastructure,” Annual Review of Anthropology 42 (2013): 327–43, https://doi.org/10.1146/annurev-anthro-092412-155522. Accessed March 16, 2026.
51. Lianxiao Meng, Lin Yang, Wu Yang, and Long Zhang, “A Survey of GNSS Spoofing and Anti-Spoofing Technology,” Remote Sensing 14, no. 19 (2022): 4826, https://doi.org/10.3390/rs14194826. Accessed March 7, 2026.
52. Rasmus Gjedssø Bertelsen, “Space Science & Technology in the Arctic: Promises of Cooperation and Development amid New Security Challenges,” IFAC-PapersOnLine 54, no. 13 (2021): 19–22, https://doi.org/10.1016/j.ifacol.2021.10.411. Accessed March 15, 2026.
53. Luis Suter, Dmitry Streletskiy, and Nikolay Shiklomanov, “Assessment of the Cost of Climate Change Impacts on Critical Infrastructure in the Circumpolar Arctic,” Polar Geography 42, no. 4 (2019): 267–86, https://doi.org/10.1080/1088937X.2019.1686082. Accessed March 15, 2026.
54. Mette Simonsen Abildgaard, Carina Ren, Israel Leyva-Mayorga, Cedomir Stefanovic, Beatriz Soret, and Petar Popovski, “Arctic Connectivity: A Frugal Approach to Infrastructural Development,” Arctic 75, no. 1 (2022): 72–85, https://doi.org/10.14430/arctic74869. Accessed March 12, 2026.
55. Andreas Østhagen, “The Arctic Security Region: Misconceptions and Contradictions,” Polar Geography 44, no. 1 (2021): 55–74, https://doi.org/10.1080/1088937X.2021.1881645. Accessed March 5, 2026.
56. Cecilie Juul Stensrud and Andreas Østhagen, “Hybrid Warfare at Sea? Russia, Svalbard and the Arctic,” Scandinavian Journal of Military Studies 7, no. 1 (2024): 111–30, https://doi.org/10.31374/sjms.233. Accessed March 18, 2026.
57. Adam Grydehøj, Anne Grydehøj, and Maria Ackrén, “The Globalization of the Arctic: Negotiating Sovereignty and Building Communities in Svalbard, Norway,” Island Studies Journal 7, no. 1 (2012): 99–118, https://doi.org/10.24043/isj.264. Accessed March 7, 2026.
58. Heather Exner-Pirot and Robert W. Murray, “Regional Order in the Arctic: Negotiated Exceptionalism,” Politik 20, no. 3 (2017), https://doi.org/10.7146/politik.v20i3.97153. Accessed March 16, 2026.
59. Pavel Devyatkin, “Arctic Exceptionalism: A Narrative of Cooperation and Conflict from Gorbachev to Medvedev and Putin,” The Polar Journal 13, no. 2 (2023): 336–57, https://doi.org/10.1080/2154896X.2023.2258658. Accessed March 6, 2026.

60. Harri Mikkola, Samu Paukkunen, and Pekka Toveri, Russian Aggression and the European Arctic: Avoiding the Trap of Arctic Exceptionalism, FIIA Briefing Paper 359 (Helsinki: Finnish Institute of International Affairs, 2023), https://www.fiia.fi/wp-content/uploads/2023/04/bp359_russian-aggression-and-the-european-arctic_harri-mikkola-samu-paukkunen-pekka-toveri.pdf. Accessed March 13, 2026.

61. "Joint Statement on Arctic Council Cooperation following Russia's Invasion of Ukraine," Government Offices of Sweden, March 3, 2022, https://www.government.se/statements/2022/03/joint-statement-on-arctic-council-cooperation-following-russias-invasion-of-ukraine/. Accessed March 15, 2026.

62. "Joint Statement on the Limited Resumption of Arctic Council Cooperation," Government Offices of Sweden, June 8, 2022, https://www.government.se/statements/2022/06/joint-statement-on-the-limited-resumption-of-arctic-council-cooperation/. Accessed March 10, 2026.

63. "Statement of Finland, Denmark, Iceland, Norway, Sweden, and the European Union regarding the Barents Euro-Arctic Cooperation," Government Offices of Sweden, March 9, 2022, https://www.government.se/statements/2022/03/statement-regarding-the-barents-euro-arctic-cooperation/. Accessed March 6, 2026.

64. NATO, "Relations with Finland," NATO Topic Page, https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-finland. Accessed March 5, 2026.

65. Karsten Friis, "Arctic Spillover? Military Signalling in the European Arctic Before and After the Full-Scale Invasion of Ukraine," Scandinavian Journal of Military Studies 8, no. 1 (2025): 240–55, https://doi.org/10.31374/sjms.375. Accessed March 11, 2026.

66. Pavel K. Baev, "Russian Strategic Guidelines and Threat Assessments for the Arctic," Security Insights no. 26 (Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies, 2019), https://www.marshallcenter.org/sites/default/files/files/2019-09/SecurityInsights_26_Baev_March2019.pdf. Accessed March 13, 2026.

67. Andreas Østhagen, "The Myths of Svalbard Geopolitics: An Arctic Case Study," Marine Policy 167 (2024): 106183, https://doi.org/10.1016/j.marpol.2024.106183. Accessed March 6, 2026.

68. "The Svalbard Treaty," Stortinget, https://www.stortinget.no/en/In-English/About-the-Storting/historical-highlights/the-svalbard-treaty/. Accessed March 11, 2026.

69. Barry Buzan, Ole Wæver, and Jaap de Wilde, Security: A New Framework for Analysis (Boulder, CO: Lynne Rienner, 1998).

70. Thierry Balzacq, "The Three Faces of Securitization: Political Agency, Audience and Context," European Journal of International Relations 11, no. 2 (2005): 171–201, https://doi.org/10.1177/1354066105052960. Accessed March 7, 2026.

71. Trine Jonassen, "Stops Registering GPS Disruptions in Finnmark, Northern Norway," High North News, September 27, 2024, https://en.highnorthnews.com/politics/stops-registering-gps-disruptions-in-finnmark-northern-norway/212107. Accessed March 16, 2026.

72. Anne Kauranen, "Finland Warns of Hostile Activities by Russia," Reuters, October 23, 2024, https://www.reuters.com/world/europe/finland-warns-hostile-activities-by-russia-2024-10-23/. Accessed March 12, 2026.

73. “Disruptions in Satellite Positioning Can Cause Extensive Damage to Society – Preparedness Should Be Strengthened by Increasing Research,” National Land Survey of Finland, June 11, 2025, https://www.maanmittauslaitos.fi/en/topical_issues/disruptions-satellite-positioning-can-cause-extensive-damage-society-preparedness. Accessed March 18, 2026.
74. Astri Edvardsen, “Strengthens the Monitoring of GPS Interference in the High North,” High North News, August 27, 2025, https://en.highnorthnews.com/politics/strengthens-the-monitoring-of-gps-interference-in-the-high-north/179931. Accessed March 15, 2026.
75. “Nkom Tester Norsk KI-Modell i Jakten på GPS-Forstyrrelser,” Nkom, September 9, 2024, https://nkom.no/aktuelt/nkom-tester-norsk-ki-modell-i-jakten-pa-gps-forstyrrelser. Accessed March 9, 2026.
76. Anne Kauranen, “Three Finnish Airports Mitigate Russian GPS Interference with Radio Navigation,” Reuters, November 7, 2024, https://www.reuters.com/business/aerospace-defense/three-finnish-airports-mitigate-russian-gps-interference-with-radio-navigation-2024-11-07/. Accessed March 15, 2026.
77. NATO, “NATO Stands Up Undersea Infrastructure Coordination Cell,” February 15, 2023, https://www.nato.int/en/news-and-events/articles/news/2023/02/15/nato-stands-up-undersea-infrastructure-coordination-cell. Accessed March 15, 2026.
78. NATO, “NATO Allies Join Forces to Enhance the Security of Critical Undersea Infrastructure,” December 10, 2024, https://www.nato.int/en/news-and-events/articles/news/2024/12/10/nato-allies-join-forces-to-enhance-the-security-of-critical-undersea-infrastructure. Accessed March 10, 2026.
79. Karsten Friis, “Arctic Spillover? Military Signalling in the European Arctic Before and After the Full-Scale Invasion of Ukraine,” Scandinavian Journal of Military Studies 8, no. 1 (2025): 240–55, https://doi.org/10.31374/sjms.375. Accessed March 12, 2026.
80. Robert Jervis, “Cooperation under the Security Dilemma,” World Politics 30, no. 2 (1978): 167–214.
81. Charles L. Glaser, “The Security Dilemma Revisited,” World Politics 50, no. 1 (1997): 171–201. Accessed March 6, 2026.
82. Karsten Friis, “Arctic Spillover? Military Signalling in the European Arctic Before and After the Full-Scale Invasion of Ukraine,” Scandinavian Journal of Military Studies 8, no. 1 (2025): 240–55, https://doi.org/10.31374/sjms.375. Accessed March 9, 2026.
83. Harri Mikkola, Samu Paukkunen, and Pekka Toveri, Russian Aggression and the European Arctic: Avoiding the Trap of Arctic Exceptionalism, FIIA Briefing Paper 359 (Helsinki: Finnish Institute of International Affairs, 2023).
84. Cecilie Juul Stensrud and Andreas Østhagen, “Hybrid Warfare at Sea? Russia, Svalbard and the Arctic,” Scandinavian Journal of Military Studies 7, no. 1 (2024): 111–30, https://doi.org/10.31374/sjms.233. Accessed March 11, 2026.
85. Andreas Østhagen, “The Myths of Svalbard Geopolitics: An Arctic Case Study,” Marine Policy 167 (2024): 106183, https://doi.org/10.1016/j.marpol.2024.106183. Accessed March 9, 2026.

86. Thomas Nilsen, “Russian Jamming Is Now Messing Up GPS Signals for Norwegian Aviation Practically Every Day,” ArcticToday, February 26, 2024; Trine Jonassen, “Stops Registering GPS Disruptions in Finnmark, Northern Norway,” High North News, September 27, 2024. Accessed March 18, 2026.

87. Stephen J. Collier and Andrew Lakoff, “Vital Systems Security: Reflexive Biopolitics and the Government of Emergency,” Theory, Culture & Society 32, no. 2 (2015): 19–51; Andreas Østhagen, “The Arctic Security Region: Misconceptions and Contradictions,” Polar Geography 44, no. 1 (2021): 55–74. Accessed March 16, 2026.

88. Andrew Mumford and Pascal Carlucci, “Hybrid Warfare: The Continuation of Ambiguity by Other Means,” European Journal of International Security 8, no. 2 (2023): 192–206; David Kilcullen, The Dragons and the Snakes: How the Rest Learned to Fight the West (Oxford: Oxford University Press, 2020). Accessed March 12, 2026.

89. Harri Mikkola, Samu Paukkunen, and Pekka Toveri, Russian Aggression and the European Arctic: Avoiding the Trap of Arctic Exceptionalism, FIIA Briefing Paper 359 (Helsinki: Finnish Institute of International Affairs, 2023); Karsten Friis, “Arctic Spillover? Military Signalling in the European Arctic Before and After the Full-Scale Invasion of Ukraine,” Scandinavian Journal of Military Studies 8, no. 1 (2025): 240–55. Accessed March 11, 2026.

90. Thomas Nilsen, “Russian Jamming Is Now Messing Up GPS Signals for Norwegian Aviation Practically Every Day,” ArcticToday, February 26, 2024, https://www.arctictoday.com/russian-jamming-is-now-messing-up-gps-signals-for-norwegian-aviation-practically-every-day/. Accessed March 14, 2026.

91. Karsten Friis, “Arctic Spillover? Military Signalling in the European Arctic Before and After the Full-Scale Invasion of Ukraine,” Scandinavian Journal of Military Studies 8, no. 1 (2025): 240–55, https://doi.org/10.31374/sjms.375. Accessed March 5, 2026.

92. Andrew Mumford and Pascal Carlucci, “Hybrid Warfare: The Continuation of Ambiguity by Other Means,” European Journal of International Security 8, no. 2 (2023): 192–206, https://doi.org/10.1017/eis.2022.19. Accessed March 11, 2026.

93. Harri Mikkola, Samu Paukkunen, and Pekka Toveri, Russian Aggression and the European Arctic: Avoiding the Trap of Arctic Exceptionalism, FIIA Briefing Paper 359 (Helsinki: Finnish Institute of International Affairs, 2023). Accessed March 5, 2026.

94. Stephen J. Collier and Andrew Lakoff, “Vital Systems Security: Reflexive Biopolitics and the Government of Emergency,” Theory, Culture & Society 32, no. 2 (2015): 19–51, https://doi.org/10.1177/0263276413510050. Accessed March 14, 2026.

95. Robert Jervis, “Cooperation under the Security Dilemma,” World Politics 30, no. 2 (1978): 167–214.