Knowledge is Power: The Politics of Arctic Data Infrastructure and Dual-Use Monitoring Systems

Kathryn Urban

Climate change is reshaping the Arctic's physical environment and driving expansion of monitoring in the region. Satellites, among other monitoring technologies, gather critical data to track sea ice retreat, ecosystem change, and infrastructure vulnerability. These systems underpin Arctic scientific knowledge and inform climate policy decisions. Yet because the costs of environmental monitoring infrastructure are borne primarily by national governments, the same infrastructure that collects climate data also supports military activities in the Arctic. This article examines the dual-use role of Arctic data collection across both environmental knowledge systems and the full spectrum of military intelligence and operations, from strategic assessment to tactical and operational decision-making. Recent scholarship highlights trade-offs between transparency and capability in emerging monitoring technologies. This article builds on that work by shifting focus from individual tools to data-gathering infrastructures that shape how Arctic realities are observed, interpreted, and governed. Climate-driven demand for persistent environmental observation has produced institutional convergence between environmental knowledge systems and military domain awareness architectures. This convergence suggests that states may unintentionally alter regional security dynamics by increasing monitoring for the sake of scientific knowledge or environmental stewardship rather than through deliberate militarization. The argument is developed through a qualitative discourse examination of U.S.-Canadian North American Aerospace Defense Command (NORAD) modernization and the accompanying data-collection efforts. Drawing on defense strategies and political statements, the analysis traces how climate change is framed as a monitoring challenge and how new sensing capabilities are integrated with military systems.

Introduction

The Arctic is warming at nearly four times the global average rate, with consequences that extend beyond ecology. Retreating sea ice is transforming the region from a naturally protected area into an accessible maritime domain, attracting interest from scientific researchers hoping to understand climate change and from military planners seeking to exploit the new environment. This surge of interest in the High North has led to growing demands for Arctic observation data from military and scientific communities. Arctic states are investing in persistent sensing architectures capable of delivering comprehensive awareness of conditions across the circumpolar region. This article argues that these investments have produced an underappreciated strategic risk: the institutional

Kathryn Urban, PhD Candidate, Massachusetts Institute of Technology (MIT)

convergence of environmental monitoring and military intelligence, surveillance, and reconnaissance (ISR) in Arctic data-gathering infrastructure, and the escalatory dynamics that convergence enables.

The problem is structural. Satellite remote sensing is the primary means of collecting environmental data in the Arctic as well of military domain awareness. The physical requirements of persistent Arctic observation are identical whether the end product is scientific or strategic. Furthermore, the expense of Arctic observation means that states are primarily responsible for fielding the infrastructure that serves both purposes. This drives a problem of indistinguishability. A state that expands its Arctic monitoring infrastructure for environmental stewardship reasons cannot credibly signal that it is not simultaneously expanding its ISR capacity. This risks setting up a security dilemma in which states interpret their neighbors' expanded monitoring through the lens of their own security interests, setting off regional militarization and arms racing. We are already seeing such escalation in Russia's characterization of Western satellite ground stations as dual-use facilities in violation of arms control commitments, targeting undersea environmental monitoring cables capable of simultaneously tracking submarine activity, and denouncing NATO's monitoring missions in the Arctic.

This article examines these dynamics through a structured discourse analysis of official strategy documents, centered on the U.S. and Canada and extended illustratively to Russia and the European Union (EU). The primary case study is the joint U.S.-Canadian effort to modernize the North American Aerospace Defense Command (NORAD), which provides detailed evidence of how climate-driven demands for environmental monitoring are being institutionally integrated with military domain awareness systems. Illustrative cases of Russia's Arctic domain awareness architecture and the EU Copernicus program are examined to probe whether the same convergence plausibly operates beyond the North American context. The argument contributes to scholarship on dual-use monitoring and transparency-security trade-offs (Coe and Vaynman, 2020; Vaynman, 2021; Vaynman and Volpe, 2023) and to the literature on Arctic security and militarization (Boulègue, 2019; Johnson, 2021; Rumer et al., 2021), identifying the specific causal pathway from environmental monitoring investment to security dilemma dynamics.

Background on Dual-Use Monitoring in the Arctic

The Arctic's rapid warming makes it a priority region for climate researchers. However, the difficulty of reaching the region and increased risk to life and equipment due to severe weather makes remote sensing the only viable means of collecting sustained data on Arctic environmental conditions (Druckenmiller et al., 2025). A range of satellite-mounted instruments generate continuous records of greenhouse gas concentrations, sea surface temperatures, sea ice thickness, and weather patterns. But while the scientific community is demanding more robust data on the region to address imminent climate trends, supply has not kept up. The data-gathering infrastructure for the Arctic region is uniquely plagued by problems of consistency and detail. Geostationary-Earth orbit (GEO) satellites can watch a fixed area continuously, but GEO satellite coverage degrades above the Arctic Circle due to the Earth's curvature (Fish, 2024; Cherry and Delamere, 2025; Druckenmiller et al., 2025). High-Earth Orbit (HEO) or Medium-Earth Orbit (MEO) satellites following elliptical orbits do cross these latitudes and can survey vast areas, but only at coarse resolutions of around 100 meters, too imprecise to monitor specific activity or localized change (Fish, 2024). Finer imaging requires Low-Earth Orbit (LEO) satellites on near-

polar tracks. But because these capabilities do not keep pace with Earth's rotation as GEO satellites do, there may be a span of days or weeks between observations of a given point on Earth. Especially given that severe weather and the polar night can interfere with electronic sensors and imaging (Uppal, 2021; Lucas et al., 2023; Cherry and Delamere, 2025; Druckenmiller et al., 2025), irregular data collection hampers observers' ability to extract regular trends – whether climactic or strategic. It also challenges efforts to track localized conditions or account for the effects of sudden disturbances.

Environmental data-gathering requires precise orbit patterns and high-resolution instruments. As such, most climate scientists cannot realistically field their own satellite or piggyback on commercial satellites. Space-based monitoring also requires in situ facilities for servicing and calibration. There is a severe dearth of such civilian infrastructure in the Arctic (Gabarró et al., 2023). All these challenges mean that climate scientists rely on state-operated satellites to collect climate data. Programs are embedded in the U.S. National Aeronautics and Space Administration (NASA) and National Oceanic and Atmospheric Administration (NOAA), the Canadian Space Agency, the European Space Agency's (ESA) Copernicus program, and the China Aerospace Science and Technology Corporation (CASC), among others (Urban, 2024).

Because the same governments funding environmental monitoring also fund military domain awareness and because the physical requirements of both missions are identical at Arctic latitudes, the architecture that serves climate science cannot be separated from that which serves intelligence collection. In the U.S., indistinguishability comes from parallel civilian and military satellites. The Defense Meteorological Satellite Program (DMSP), for example, operates complementary to NOAA's polar-orbiting satellite, collecting environmental data to plan and conduct U.S. military operations while also contributing incidentally-collected climate data to scientific consumers (Van Deelen, 2025). In other states, environmental and security data is formally integrated into the same satellite infrastructure. EU and Chinese program follow this integration logic, with a single set of raw data being collected by satellites then broken out to civilian and military agencies for analysis ("Copernicus Maritime Surveillance - EMSA - European Maritime Safety Agency," n.d.; Vandakova, 2026). Civilian data collection across Arctic states also relies on military bases as in situ installations for space assets.

Transparency versus Security in Space-Based Monitoring

From the initial development and deployment of reconnaissance satellites in the 1960s, the U.S. and USSR recognized that exclusive unilateral monitoring created distinct escalation risks (Gaddis, 1989: 195–209). This illustrates the pervasive problem of space-based data-collection: Even if states agree to permit discrete monitoring for cooperative purposes, mistrust persists due to architecture indistinguishability. Recent arms-control scholarship has given this long-held intuition a theoretical footing.

Coe and Vaynman (2020: 343) named and formalized the transparency-security trade-off, in which states seek to balance a monitoring architecture that is transparent enough to enable agreed-upon observation but not so transparent as to reveal information the state would prefer to keep secret. The severity of the trade-off may be partially ameliorated by open security establishments and reconnaissance technologies with demonstrable control over information collection (Vaynman, 2021: 35–36). However, dual-use capabilities carry the greatest risk for misinterpretation. Vaynman and Volpe (2023) locate this risk along two dimensions: distinguishability, the ease with which an

observer can tell a military use from a civilian one, and integration, the degree to which a capability is embedded in both military and civilian institutions. Capabilities that rate high on both are the hardest to govern, since neither side can verify the other's intentions without surrendering information it needs to protect (Vaynman and Volpe, 2023: 605–611). Major satellite architectures are therefore a key flashpoint for great power competition in space and counterspace capabilities (Burdette, 2025), despite the extensive civilian applications of these assets.

These dynamics are not merely theoretical in the Arctic. Space-based monitoring capabilities already feature in security competition among Arctic states, particularly between the U.S. and Russia, suggesting that these states are primed for competition or misunderstanding. The shortest route for a strategic air or missile attack between these states is over the North Pole. Washington and Moscow have entrenched early warning radar in the region since the Cold War. With the Arctic reemerging as a locus of great power competition, the U.S. and Russia are investing in polar satellite coverage for domain awareness, ISR, and military communications (Boulègue, 2019: 21–33; Brewer et al., 2021: 6). There have also been documented clashes between the two powers in outer space, notably Russia tailing U.S. spy satellites in 2020 (Hennigan, 2020) and Russia's 2021 test of anti-satellite weapons (Gabbatt, 2021).

The scholarship reviewed here has advanced understanding of how dual-use capabilities generate security risks. Yet it has done so at the level of individual technologies rather than the data-gathering infrastructures within which those technologies are embedded. A technology-level analysis can identify the dual-use risks of a given monitoring capability. It cannot account for how institutional choices about who funds, operates, and has access to the resulting data shape the security implications of that dual-use character. This paper takes up the question of whether and how this climate-driven demand reshapes the dual-use dilemma in the Arctic operating context.

Research Methods

This paper uses discursive analysis of official strategy documents to evaluate how states frame their Arctic monitoring architecture and how adversaries respond to the real or perceived risk of intelligence gathering through scientific or dual-use data collection. This analysis focuses on what public documents reveal about institutional design choices. Because the operational details of state intelligence architecture are not available in the public domain, this analysis cannot establish the full extent to which environmental data collected through state monitoring programs is processed, retained, or acted upon by military agents. What public-facing documents can establish is that states make deliberate choices that produce convergent sensing architectures and that adversaries respond to those systems with escalatory behavior.

The primary case study is NORAD modernization in the North American Arctic. As the only binational military command in the Arctic, NORAD merges the forces of two sovereign states into a single, shared sensing architecture. This shared command is particularly noteworthy in light of the two states' divergent primary motivations for the region: Canadian Arctic discourse leads with climate threats as the driver of policy while U.S. discourse leads with geopolitical competition and treats climate as an amplifier. This divergence makes NORAD a hard case for the paper's central claim. If convergence between environmental monitoring and military ISR were the product of deliberate design, two governments beginning from different rationales would not be expected to arrive at institutionally identical infrastructure. The NORAD case thus offers analytic leverage that

a single-state case cannot provide by holding constant the sensing environment while varying political rationale, isolating structure from intent.

The NORAD case includes nine strategy documents released by the U.S., Canada, or jointly from 2021 to 2024. These represent the full set of formal strategy and policy documents on NORAD modernization. The Arctic postures of both states have shifted since 2024, as Canada's Carney government has accelerated Arctic defense build-outs (Glesby, 2025) while in the U.S., the second Trump administration has stripped climate language from national security discourse (Sikorsky, 2025). Neither change unsettles this paper's core argument. Because the convergence of sensing infrastructure identified here is structural rather than political, the underlying indistinguishability of dual-use architecture and its escalatory logic remain intact.

Each of the strategy documents evaluated in this case are coded according to six parameters of monitoring architecture ambiguity and institutional convergence in environmental and ISR data collection:

1. Climate as a Threat Enabler (CTE): Climate change is framed not primarily as an environmental crisis, but as a condition that creates or amplifies traditional military security threats.
2. Monitoring as a Shared Solution (MSS): A single monitoring and/or data collection capability is proposed, justified, or described as serving environmental and military purposes simultaneously or interchangeably.
3. Organizational and Institutional Integration (OII): Military organizations explicitly assume responsibility for environmental monitoring functions or civilian environmental agencies are folded into military planning and command architectures.
4. Data Indistinguishability (DI): The text acknowledges or implies that data collected for environmental or scientific purposes is available to, used by, or structurally identical to data serving military ISR functions.
5. Urgency-Access Coupling (UAC): Climate-driven increased physical access to the Arctic is framed as inseparable from expanded military monitoring demands.
6. Adversarial Dual-Use Recognition (ADR): Adversaries are engaging in dual-use monitoring activities and reciprocally perceive Western monitoring as serving intelligence functions.

These six parameters operationalize the key mechanisms of the transparency-security and dual-use scholarship. The idea of military-civilian distinguishability is the direct basis for the DI parameter and underlies MSS while the integration mechanism underscores OII and sets up the reciprocal suspicion dilemma captured by ADR. The remaining two parameters, CTE and UAC, extend this framework to the Arctic region specifically. Three additional features of this framework bear on how its results should be read. First, the six parameters are not variables, but different facets of institutional convergence. A passage coupling climate-driven access to military demand, for example, will often also frame monitoring as a shared solution. Overlap among the parameters is evidence of convergence, not a measurement flaw. Second, the parameters are not indexed and no single parameter or threshold count is treated as necessary or sufficient. The analytical weight rests instead on saturation across the corpus. Third, the coding distinguishes explicit and implicit textual evidence. Explicit coding (marked ++ in Table 1) indicates that a document directly names the

dual-use function, openly assigns environmental monitoring responsibilities to military actors, or acknowledges simultaneous activity. Implicit coding (marked + in Table 1) indicates that the dual-use function is present in the structure of the document, but not directly stated. For instance, environmental monitoring language is used to justify military procurement without the civilian function being named. This implicit language may be a deliberate rhetorical choice in public-facing documents. It may also demonstrate that convergence is occurring in institutional design without officials necessarily being aware of that fact. The inferences drawn from the textual analysis are therefore interpretive. The pattern of coded language warrants the claim that environmental and military monitoring functions are being institutionally fused, not a claim about the frequency or magnitude of that fusion.

NORAD Modernization Case

NORAD is a joint U.S.-Canadian military command established during the Cold War to provide warning for aerial and maritime threats and to secure aerospace control for continental defense. Because a ballistic missile launched from Russia or China would follow a polar trajectory, NORAD's early warning systems have always been oriented toward the Arctic. The backbone of this system is the North Warning System (NWS), a chain of radar installations stretching from Labrador to Alaska. As the NWS approaches the end of its operational lifespan, the U.S. and Canada have committed to a comprehensive modernization effort, allocating $38.6 billion (Department of National Defence, 2023). This investment reflects not only the obsolescence of Cold War-era infrastructure but also new adversary capabilities, the growing importance of the Arctic region to adversary military planning, and the physical transformation of the region due to climate change (O'Shaughnessy and Fesler, 2020; Johnson, 2021; Karako, 2025). As NORAD prepares to expand situational awareness for defense and deterrence, policy analysts are calling for equal attention to civilian data-gathering purposes (Charron, 2020). This case study analyzes relevant strategy documents to assess the salience of dual-use data incentives and risks in state planning for NORAD modernization.

NORAD is a binational command with shared infrastructure and a unified chain of authority and both states have committed to modernization investments. The case treats U.S. and Canadian strategy documents as a single institutional case for the purposes of this analysis.

An Architecture of Ambiguity

Nine U.S., Canadian, and bilateral strategy documents released between 2021 and 2024 make up the core of this case study, with the content of each assessed along the six parameters of monitoring architecture ambiguity (see Table 1). This analysis reveals a consistent pattern: civilian and military sensing are framed as a single problem requiring unified solutions, administered within a shared command architecture, and indistinguishable in terms of the physical infrastructure deployed to serve both purposes. This section presents each code in turn, drawing on representative passages to demonstrate the pattern.

Table 1. NORAD Modernization Strategy Documents Coded for Dual-Use Language

	CTE	MSS	OII	DI	UAC	ADR
Joint Statement on NORAD Modernization (2021)	++	++	+	+		
NORAD-USNORTHCOM Strategy (2021)	+	++	++	++	+	
USNORTHCOM and NORAD Posture Statement (2021)	+	++	++		+	++
Canada's NORAD Modernization Plan (2022)	+	++	++		+	
US National Strategy for the Arctic Region (2022)	++	++	+		++	++
Canada Arctic Foreign Policy (2024)	++	+	+	++	+	++
Canada's "Our North, Strong and Free" Strategy (2024)	++	++	+	+	++	+
DoD Arctic Strategy (2024)	++	++	++	++	++	++
DoD Climate Adaptation Plan (2024)	+	++	+	+		

++ = strong/explicit passage; + = present but implicit or secondary passage

Climate as Threat Enabler

Across the case documents, states consistently frame climate change not as an environmental challenge distinct from security concerns, but as a co-equal driver of the same strategic imperatives that motivate military investments. This framing of Climate as Threat Enabler (CTE) is clearly articulated in the Joint Statement on NORAD Modernization (2021), which identifies "growing strategic competition, rapid advancements in technology, and ongoing changes in our climate" as comparable forces "eroding" North America's geographic protection. The grammatical coordination is significant because it points to state discourse of climate change not as subordinate

to or derivative of geopolitical challenges, but as an independent cause of the same strategic exposure. The same formulation appears in Canada's NORAD Modernization Plan (2022), demonstrating that the NORAD-specific framing was carried forward into national implementation documents.

Canada's Arctic Foreign Policy (2024: 2) extends this logic, asserting that "threats to Canada's security are no longer bound by geography; climate change is accelerating rapidly; and non-Arctic states, including China, are also seeking greater influence in the governance of the Arctic." Here, climate change, geographic exposure, and geopolitical competition are presented as a unified threat complex rather than separate policy domains. The U.S. National Strategy for the Arctic Region (NSAR) (2022: 5-6) articulates the same dynamic from the other direction, noting that climate change "creates a cascade of difficulties, as well as some new possibilities" and that "the Arctic's growing strategic importance has intensified competition." Physical environmental change and strategic competition are causally linked through a shared mechanism of increased access.

The U.S. Department of Defense (DoD) Climate Adaptation Plan (2024: 1) inverts this logic, framing environmental change as strategic opportunity: "As changes in the physical environment create the opportunity for well-prepared forces to secure a competitive advantage, deter aggression, and protect the United States and its interests." Whether threat or opportunity, the logic is the same: environmental change is a strategic condition for military forces, not a civilian policy domain.

Monitoring as Shared Solution

If CTE language establishes why climate and security are treated as unified problems, Monitoring as Shared Solution (MSS) language establishes how by proposing and justifying sensing architectures that serve both environmental and military functions simultaneously. This code appears in every document analyzed and is explicit in all documents except for Canada's Arctic Foreign Policy (2024), making it the most consistent indicator of institutional convergence in the corpus.

The most explicit MSS language appears in the NSAR's (2022: 9) Strategic Objective 1.1, which states that the U.S. will "invest in modernized domain awareness to detect and track potential airborne and maritime threats and improve sensing and observational capabilities, including for sea ice, ship traffic, and weather." Within a single strategic objective under a national security pillar, sea ice observation and threat detection are listed as parallel outputs of the same sensing investment, justified by the same rationale, and to be administered by the same command structure. Environmental monitoring is not assigned to civilian agencies — it is explicitly named as a security function. The DoD Arctic Strategy (2024: 10) similarly directs the department to "advance analysis to better sense, model, and predict the meteorological, atmospheric, and oceanographic environment within the Arctic," including "naval oceanography, ice research, coupled atmospheric and ocean modeling, and ionospheric modeling" through "partnerships with other Federal entities." Scientific research tasks are here framed as military capability requirements, with civilian agencies repositioned as partners contributing to a defense mission rather than independent operators.

The NORAD-USNORTHCOM Strategy describes the intended architecture as "a layered sensing grid that provides persistent battlespace awareness from the seabed to space and cyberspace" and calls for the "inclusion of non-DoD/DND capabilities" to extend its reach (VanHerck, 2021a: 7).

Canada's NORAD Modernization Plan (2022) reflects the same approach, listing "undersea surveillance," "cloud-enabled command, control, communications, and computers intelligence, surveillance and reconnaissance," and "enabling defence research and development in the Arctic" as undifferentiated technology investment priorities within the same procurement plan.

Organizational and Institutional Integration

Organizational and Institutional Integration (OII) language moves beyond sensing architecture to describe how military institutions are positioned as the organizational home of environmental monitoring functions and data aggregation. The clearest expression of this is the DoD Arctic Strategy's (2024: 10) direction that the Department of Defense assume responsibility for environmental data and modeling as military requirements. Climate science is not to be conducted in parallel with military activities. It is to be conducted by military-funded and military-directed organizations. This represents a significant expansion of the security sector's institutional footprint into domains previously occupied by civilian scientific agencies. The NSAR (2022: 9) reinforces this pattern by committing to environmental functions: "We will improve Arctic observing, mapping, and charting; weather, water, and sea ice forecasting; subseasonal and seasonal prediction; emergency preparedness posture; and satellite coverage." The assignment of these functions to the Security pillar is an institutional choice that places environmental data governance within a security framework.

Canada's Arctic Foreign Policy (2024: 19) frames situational awareness as "bridging the intelligence gap" while the DoD Climate Adaptation Plan (2024: 5) mandates that all military resource allocation decisions incorporate climate considerations, embedding environmental data governance within military institutional authority. The NORAD-USNORTHCOM Strategy calls for Joint All-Domain Command and Control to dissolve institutional barriers between civilian environmental data producers and military consumers, making all sensing data available to military decision-makers in real time (VanHerck, 2021a: 7). The language of strategy documents consistently positions civilian agencies as downstream beneficiaries of military-led investments rather than co-equal partners in environmental monitoring.

Data Indistinguishability

Data Indistinguishability (DI) language documents discursive acknowledgements of the challenges of differentiating environmental and military monitoring. The DoD Arctic Strategy (2024: 7) provides the clearest statement of the problem: "Monitoring involves robust intelligence collection in concert with other departments, agencies, Allies, and partners to provide early indications and warning to manage risk. This includes monitoring the activities of our adversaries as well as the physical changes to the operating environment." In a single definition of "monitoring," this text presents adversary surveillance and physical environmental observation as undifferentiated activities without differentiated outputs for scientific or intelligence purposes.

The DoD Climate Adaptation Plan (2024: 7) makes the operational workflow explicit. In considering environmental risk questions, the document illustrates how tactical military decision-making draws on environmental data related to weather conditions, sea levels, and aerial visibility. It calls for practitioners to use "sensing, satellite, 1-10 day weather forecast models" to collect needed information, the same tools that compose the civilian climate monitoring record. This implies that an external observer would not be able to separate out the processes for collecting

scientific climate data from those used to gather data to inform a lethal force decision because both the collection instruments and the raw data that they produce are identical.

The Joint Statement on NORAD Modernization (2021) addresses the data architecture from the command perspective, emphasizing the need to "fuse and integrate data from all-domain sensors into a common, comprehensive operating picture." Within the Arctic context, all-domain sensors include the same satellites, oceanographic buoys, and atmospheric monitoring instruments used for climate science.

Urgency-Access Coupling

Urgency-Access Coupling (UAC) language is present across the documents in a consistent logical structure, setting up sea ice retreat (an environmental phenomenon) and strategic competition (a military phenomenon) as co-constitutive challenges that produce the same requirement for enhanced domain awareness.

Canada's "Our North, Strong and Free" (ONSF) strategy document (2024: v) articulates the coupling most directly: "Our Arctic is warming at four times the global average, opening the region to the world…By 2050, the Arctic Ocean could become the most efficient shipping route between Europe and East Asia. We are seeing greater Russian activity in our air approaches, and a growing number of Chinese vessels and surveillance platforms are mapping and collecting data about the region." The passage moves seamlessly from an environmental trend (global warming) to economic implications (shipping routes) to security responses (adversary surveillance) – three distinct domains connected by the single causal logic of increased access to the region. The NORAD-USNORTHCOM Strategy makes the coupling even more explicit: "Diminished sea ice and competition over resources present overlapping challenges in this strategically significant region" (VanHerck, 2021a: 5). The word "overlapping" is telling here: these are not separate challenges requiring separate responses but a single, integrated problem requiring an integrated monitoring solution.

Adversarial Dual-Use Recognition

Adversarial Dual-Use Recognition (ADR) is perhaps the most analytically consequential code because it demonstrates that Western officials are themselves aware of the dual-use challenge of data infrastructure and are concerned about ostensibly environmental efforts run by adversaries that could also facilitate intelligence collection. Canada's Arctic Foreign Policy (2024: 8) provides the definitional anchor for this code, explicitly characterizing "China's regular deployment of dual-use — having both research and military application — research vessels and surveillance platforms to collect data" as a security threat. The document's own definition of "dual-use" as ascribed to Canada's adversary describes with precision the very same architecture present in North American monitoring investments. The NSAR (2022) and ONSF (2024) apply the logic to Chinese scientific expeditions and Russian surveillance platforms, respectively.

Adversary Perception and the Escalation Dynamic

The preceding analysis established that U.S. and Canadian officials design and justify North American monitoring architecture in terms that render environmental and military functions indistinguishable. The escalation risk that this paper identifies, however, depends on a second claim: that adversaries perceive Western monitoring activities as militarily threatening and respond accordingly. Russian and Chinese documents do not explicitly characterize Western environmental

monitoring as intelligence collection, but behavioral evidence suggests the interpretive framework is operative across all major Arctic actors.

Russia's responses to specific Western monitoring deployments provide clear behavioral evidence. In November 2021, Russia's Ministry of Foreign Affairs characterized the Svalbard Satellite (SvalSat) ground station as a "dual-use" facility in violation of the Svalbard Treaty's demilitarization provisions (van der Wal, 2025). SvalSat's primary function is downloading data from polar-orbiting environmental and scientific satellites operated by NASA, NOAA, and the U.S. Geological Survey. Yet its position in an elliptical polar orbit receiving architecture also makes it useful for military missions. Open-source evidence confirms that the U.S. used space-based data received by SvalSat to plan and execute operations in Iraq and Afghanistan (van der Wal, 2025). As one SvalSat operator acknowledged, "all the satellite-based information that comes to us is dual-use…if the military will have it, they get it" (Scoles, 2025). Russian officials have also framed NATO activity in the Arctic as escalatory. The alliance primarily conducts sensing and monitoring operations with at least some dual-use components (e.g., search-and-rescue) rather than weapons deployments. But the commander of Russia's Northern Fleet characterized NATO and U.S. activities in the region as "definitely" provocative (Devyatkin, 2025) while Russian Foreign Minister Sergey Lavrov stated in September 2024 that "Russia is fully ready for a conflict with NATO in the Arctic. We see NATO stepping up drills related to possible crises in the Arctic" (Gray, 2026).

Russian views on Chinese activity in the Arctic also acknowledge the indistinguishability problem. Russia's Federal Security Service (FSB), in an internal planning document authenticated by six Western intelligence agencies, characterized Chinese scientific and commercial research activities in the Arctic as a form of espionage. FSB directed officers to "intercept the threat and prevent the transfer of important strategic information" to Chinese civilians engaged in such activities (Judah et al., 2025). The DoD applied identical reasoning to Chinese Arctic expeditions, arguing that scientific research in the region served as a cover for military activities (Kahraman, 2025). Both Russia and the U.S. treat the environmental research activities of a third party as intelligence collection — demonstrating that the dual-use interpretive framework is not a Western construct applied only to adversaries but a structural feature of how all major powers read monitoring activities in the Arctic. Just as Moscow applied this framework to be skeptical of Chinese Arctic research, so too did it turn the same logic on NORAD, treating its environmental sensing networks as intelligence platforms – as the SvalSat case confirms.

Behavioral evidence further confirms that this is not merely a discursive posture but one that produces real responses to perceived intelligence threats. In 2021, the Lofoten Vesterålen (LoVe) undersea observatory in northern Norway, which monitored ocean emissions and fish stocks alongside detection of Russian Northern Fleet submarines, suffered extensive cable damage that hampered its observations. Western intelligence reports attributed the damage to Russian vessels active in the area (Kertysova and Gricius, 2023: 16). In 2023, the U.S. publicized the activities of fifty Russian trawlers reported to be collecting intelligence on classified U.S. seabed infrastructure alongside their stated mission of environmental data-gathering (Gray, 2026). Both cases illustrate the reflexive character of the dynamic: Russia targets Western environmental monitoring infrastructure that it perceives as dual-use, while simultaneously conducting intelligence operations under environmental cover — the same behavior it attributes to, and protests in, others.

NORAD Case Discussion

The nine documents analyzed in the NORAD case span four years and two governments, yet all six codes appear across the full corpus. This saturation is itself analytically significant. It demonstrates that the convergence between environmental monitoring and military ISR is not a feature of any particular document's rhetorical strategy or any single official's framing choices, but a property of the entire policy architecture within which NORAD modernization is planned and justified.

Two features of this pattern merit specific attention because they bear on the paper's claim about inadvertent rather than deliberate convergence. First, the national asymmetry in primary framing identified above cuts against a deliberate design interpretation. As the case selection anticipated, Canada's climate-led discourse and the U.S.'s competition-led discourse are distinct motivations, yet they generate identical sensing requirements, procurement logic, and institutional arrangements across the shared NORAD command architecture. That two governments working from different rationales nonetheless built identical infrastructure suggests that convergence is a structural feature of shared monitoring rather than coordinated intent to militarize it. Second, the ADR evidence creates a reflexive problem that the documents themselves do not acknowledge. Canadian and U.S. officials acknowledge the dual-use threat of adversary scientific activities simultaneously serving military functions. But while NORAD strategy documents recognize this logic and apply it outwards, they do not (publicly) apply it inward. The behavioral evidence suggests that adversaries observe the indistinguishability of Western monitoring infrastructure, responding to it as they would to intelligence platforms. The strategic consequence is a security dilemma rooted not in weapons acquisition or force posture changes, but in data-gathering infrastructure.

Beyond NORAD: Two Illustrative Cases

The NORAD case provides systematically coded evidence of institutional convergence between environmental monitoring and military domain awareness in a specific bilateral context. This section turns to two further cases to consider whether the same convergence is visible elsewhere in the region. These cases are analytically useful because the three actors are so different: a binational military command (NORAD), a centralized nation-state (Russia), and a civilian-led supranational program (EU Copernicus). They diverge in institutional form, political context, and stated purpose. If the same convergence is observed across all three, it is therefore likely to be a structural feature of Arctic monitoring rather than an artifact of any one arrangement.

As with the North American states, Russia has invested in Arctic monitoring infrastructure to track new strategic opportunities and vulnerabilities in the High North. Russia's 2020 Arctic Strategy commits to monitoring across both civilian socioeconomic objectives and military security ones, and scholars have highlighted the resulting indistinguishability between Moscow's civilian and military monitoring infrastructure (Boulègue, 2019: 14; Boulègue and Kertysova, 2020). Russia launched the Arktika-M satellite constellation in 2021 with the stated scientific objectives of hydrometeorological observation of the Arctic Ocean. The application of the collected data, however, spans both civilian and military functions: information on sea ice conditions is used in route planning for both civilian ships and military vessels, enabling both search-and-rescue efforts and near-real-time tracking of enemy ships (Humpert, 2022; Kabachynskyi, 2025). Russia's own Deputy Prime Minister, Yury Trutnev, commented on the dual-use task spectrum of the Arktika-M satellites and the state's objective of creating an "Arctic orbital satellite group" (Humpert, 2022).

This convergence also extends to ground infrastructure. Russia has rebuilt and expanded Soviet-era Arctic bases, constructing military stations that support polar satellites for security missions and domain awareness as well as civilian meteorological research. But despite scientific applications, the projects were constructed under military authority using off-the-shelf military hardware (Boulègue, 2019: 14). This drawing of civilian scientific research into the security domain binds Arctic monitoring systems into a common command authority and physical structure.

The EU Copernicus Program is a space-based monitoring institution designed with security and environmental objectives as dual facets of its founding mandate. The Arctic is a priority region for Copernicus on both scientific and strategic grounds. But while Copernicus is funded through EU budget mechanisms rather than defense appropriations and is managed by civilian agencies, the data from satellites tasked with environmental monitoring is also used for ISR functions (European Space Agency, n.d.). The convergence in Copernicus' monitoring and institutional architectures is most clearly visible in the Maritime Surveillance Service, in which satellite-collected information on sea ice and ocean conditions exists as a single raw data package and civilian and military functions become apparent only in dissemination (European Maritime Safety Agency, n.d.). The space-based and ground station architecture is identical but the end-use products can be either civilian environmental studies or classified intelligence reports (European Maritime Safety Agency, 2019, p. 2). Similarly undifferentiated data collection across military and civilian spheres is a hallmark of other Copernicus missions, including the forthcoming ROSE-L mission much-lauded by climate researchers (European Space Agency, n.d.).

The two illustrative cases indicate that convergence is not confined to the North American context. Furthermore, they suggest that the mechanism of convergence varies with institutional context even as the outcome remains constant. In the NORAD case, a binational military command absorbs civilian environmental functions as it expands its sensing architecture to meet climate-driven domain awareness requirements. In the Russian case, the direction of absorption runs opposite: a centralized state deploys military institutions to perform civilian environmental functions because those institutions are better resourced and enjoy superior logistical reach in the remote Arctic (Davis and Holland, 2020). Copernicus is the hardest case of the three, given its civilian mandate, civilian funding, open-data principles, and absence of military command authority. Yet convergence appears even there, not through either institution absorbing the other but through the accumulation of secondary users, as open environmental data is drawn into restricted security applications by the operational needs of member states. The result is a tiered access structure that renders the same data simultaneously open science and restricted intelligence. Three different institutional starting points thus produce the same structural result: monitoring infrastructure that external observers cannot classify as either environmental or military.

Conclusion

This article has argued that the structural indistinguishability of environmental monitoring and military ISR in the Arctic is not an incidental feature of specific technologies or state objectives, but a property of the dual pressures of climate-driven monitoring demand and intensifying geopolitical competition. The NORAD modernization case provides the most detailed evidence. Analysis of strategy documents reveals a consistent pattern of state discourse on Arctic monitoring that centers climate change and security competition as parallel drivers of investment requirements and produces institutional solutions that give military organizations institutional authority over

many civilian scientific functions. These decisions result in indistinguishability of both monitoring architectures and the resulting raw data, leading adversaries to characterize monitoring installations as military targets and respond with escalatory behavior. The illustrative Russian and European cases suggest that this pattern is not unique to North America, even given their diverging institutional characteristics.

The security dilemma documented here is distinctive in a respect that has direct implications for governance responses. Most security dilemmas are amenable to transparency measures or confidence-building protocols because the underlying problem is misattribution of a capability's purpose. Environmental-military convergence in Arctic monitoring infrastructure does not generate misattribution. Russian characterization of SvalSat as a dual-use facility was not a misreading of the architecture's purpose, but an accurate skepticism of infrastructure that served both purposes. Western characterization of Chinese research vessels as intelligence platforms was not paranoia, but a correct identification of dual-use operations. The key distinction is that the adversaries in these dynamics do not misperceive each other's intentions, but face hardware that simultaneously performs military and scientific functions. This means that the standard toolkit of confidence-building measures is structurally inadequate to the problem – trust cannot be built around an ambiguity that is real rather than perceived. The challenge is therefore not to correct misperceptions but to design institutions that can manage a situation in which environmental stewardship and military intelligence cannot be separated.

This has practical implications for how Arctic governance institutions and bilateral security arrangements address monitoring infrastructure. The existing arms control and confidence-building architecture for the Arctic was not designed with data-gathering infrastructure in mind. As monitoring investments accelerate across all major Arctic actors, the absence of any agreed-upon framework for distinguishing environmental from military sensing creates accumulating risks of miscalculation. Existing incidents of infrastructure sabotage and scientific activities as espionage are early expressions of a dynamic that will intensify as monitoring architectures grow denser and more capable.

Future research should examine whether the escalatory potential identified here can be mitigated through institutional design. Possible avenues include data-sharing arrangements that create verifiable separation between environmental and ISR outputs, multilateral frameworks for registering Arctic monitoring infrastructure analogous to space object registration regimes, and confidence-building measures tailored to dual-use sensing architecture. Whether any of these mechanisms can resolve an indistinguishability problem that is structural rather than perceptual is an open question. But the alternative, allowing monitoring infrastructure to accumulate without governance, risks precisely the inadvertent escalation this article has traced.

References

Boulègue, M. (2019). *Russia's Military Posture in the Arctic*. Chatham House. https://www.chathamhouse.org/2019/06/russias-military-posture-arctic

Boulègue, M., & Kertysova, K. (2020). *Arctic Development Reflects Russia's Thorny Civil-Military Relations | Wilson Center*. Wilson Center. https://www.wilsoncenter.org/blog-post/arctic-development-reflects-russias-thorny-civil-military-relations

Brewer, E., Hersman, R., & Simon, M. (2021). *Deep Dive Debrief: Strategic Stability and Competition in the Arctic*. Center for Strategic and International Studies. https://www.csis.org/analysis/deep-dive-debrief-strategic-stability-and-competition-arctic

Charron, A. (2020, September 7). Beyond the North Warning System. *War on the Rocks*. https://warontherocks.com/2020/09/beyond-the-north-warning-system/

Cherry, J., & Delamere, J. (2025). *2024 Alaska Next Generation Workshop Report*. NOAA. https://repository.library.noaa.gov/view/noaa/71362

Coe, A. J., & Vaynman, J. (2020). Why Arms Control Is So Rare. *American Political Science Review*, *114*(2), 342–355. https://doi.org/10.1017/S000305541900073X

Department of National Defence. (2023, March 24). *NORAD modernization project timelines*. https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/norad-modernization-project-timelines.html

Department of National Defence. (2024). *Our North, Strong and Free: A Renewed Vision for Canada's Defence*. Canadian Department of National Defence.

Devyatkin, P. (2025, September 11). The rising US-NATO-Russia security dilemma in the Arctic. *Responsible Statecraft*. https://responsiblestatecraft.org/arctic-nato-russia-2673981485/

Druckenmiller, M., Thoman, R., & Moon, T. (2025). *Arctic Report Card 2025*. NOAA. https://arctic.noaa.gov/report-card/report-card-2025/

European Maritime Safety Agency. (n.d.). *Copernicus Maritime Surveillance*. Retrieved April 9, 2026, from https://www.emsa.europa.eu/copernicus.html

European Maritime Safety Agency. (2019). *Copernicus Maritime Surveillance: Service Overview*. European Maritime Safety Agency.

European Space Agency. (n.d.). *Copernicus Sentinel Expansion missions*. Retrieved April 9, 2026, from https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Copernicus_Sentinel_Expansion_missions

Fish, T. (2024, May 29). Increasing coverage: Overcoming Arctic challenges. *European Security & Defence*. https://euro-sd.com/2024/05/articles/technology/38351/increasing-coverage-overcoming-arctic-challenges/

Gabarró, C., Hughes, N., Wilkinson, J., Bertino, L., Bracher, A., Diehl, T., Dierking, W., Gonzalez-Gambau, V., Lavergne, T., Madurell, T., Malnes, E., & Wagner, P. M. (2023). Improving satellite-based monitoring of the polar regions: Identification of research and capacity gaps. *Frontiers in Remote Sensing*, *4*. https://www.frontiersin.org/articles/10.3389/frsen.2023.952091

Gabbatt, A. (2021, November 15). US accuses Russia of 'dangerous' behavior after anti-satellite weapons test. *The Guardian*. https://www.theguardian.com/science/2021/nov/15/us-investigating-debris-event-space-reports-russia-anti-satellite-weapon-test

Gaddis, J. L. (1989). *The Long Peace: Inquiries Into the History of the Cold War* (First Edition). Oxford University Press.

Glesby, N. (2025). *Canada's Arctic Over-the-Horizon Radar: Early-Warning for the Defence of North America?* [Policy Primer]. North American and Arctic Defence and Security Network.

Global Affairs Canada. (2024). *Canada's Arctic Foreign Policy*. Global Affairs Canada.

Government of Canada. (2022, April 8). *Annex C: Canada's NORAD Modernization Plan*. Government of Canada. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024/annex-c-canada-norad-modernization-plan.html

Gray, J. (2026). War in the Arctic? *Proceedings*, *152*(1). https://www.usni.org/magazines/proceedings/2026/january/war-arctic

Hennigan, W. J. (2020, February 10). Exclusive: Russian Craft Shadowing U.S. Spy Satellite, Space Force Commander Says. *TIME*. https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/

Humpert, M. (2022, November 4). *Russia Plans to Launch Nine Polar-orbiting Satellites to Monitor the Arctic by 2026*. https://en.highnorthnews.com/business/russia-plans-to-launch-nine-polar-orbiting-satellites-to-monitor-the-arctic-by-2026/225803

Johnson, B. T. (2021). Sensing the Arctic: Situational awareness and the future of northern security. *International Journal (Toronto, Ont.)*, *76*(3), 404–426. https://doi.org/10.1177/00207020211048424

Judah, J., Sonne, P., & Troianovski, A. (2025, June 7). Secret Russian Intelligence Document Shows Deep Suspicion of China. *RSN*. https://www.rsn.org/001/secret-russian-intelligence-document-shows-deep-suspicion-of-china.html

Kabachynskyi, I. (2025, October 30). Russia's New Weather Satellites Over the Arctic Can Also Guide Its Military. *UNITED24 Media*. https://united24media.com/world/russia-is-launching-weather-satellites-over-the-arctic-that-can-also-guide-its-military-12966

Kahraman, A. L. (2025, December 30). China's Digital Footprint in the Arctic: The Strategic Role of Satellite and Subsea Cable Infrastructure. *The Arctic Institute - Center for Circumpolar Security Studies*. https://www.thearcticinstitute.org/chinas-digital-footprint-arctic-strategic-role-satellite-subsea-cable-infrastructure/

Karako, T. (2025, October 9). *North American Aerospace Defense Command (NORAD) Modernization* [Interview]. https://www.csis.org/analysis/north-american-aerospace-defense-command-norad-modernization

Kertysova, K., & Gricius, G. (2023). *Countering Russia's hybrid threats in the Arctic*. European Leadership Network. https://europeanleadershipnetwork.org/report/countering-russias-hybrid-threats-in-the-arctic/

Lucas, S., Johannessen, J. A., Cancet, M., Pettersson, L. H., Esau, I., Rheinlænder, J. W., Ardhuin, F., Chapron, B., Korosov, A., Collard, F., Herlédan, S., Olason, E., Ferrari, R., Fouchet, E., & Donlon, C. (2023). Knowledge Gaps and Impact of Future Satellite Missions to Facilitate Monitoring of Changes in the Arctic Ocean. *Remote Sensing*, *15*(11), 2852. https://doi.org/10.3390/rs15112852

O'Shaughnessy, T. J., & Fesler, P. M. (2020). *Hardening the Shield: A Credible Deterrent & Capable Defense for North America*. The Canada Institute.

Rumer, E., Sokolsky, R., & Stronski, P. (2021). *Russia in the Arctic—A Critical Examination*. https://carnegieendowment.org/research/2021/05/russia-in-the-arctica-critical-examination

Scoles, S. (2025, March 19). A Powerhouse of Global Satellite Infrastructure: Norway? *Undark Magazine*. https://undark.org/2025/03/19/global-satellite-infrastructure-norway/

Sikorsky, E. (2025). *2025 Annual Threat Assessment First in Over A Decade to Omit Climate Change—The Council on Strategic Risks*. Council on Strategic Risks. https://councilonstrategicrisks.org/2025/03/26/2025-annual-threat-assessment-first-in-over-a-decade-to-omit-climate-change/

Strategy for Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035 (Revised) (A. Davis & E. Holland, Trans.). (2020). Russia Maritime Studies Institute.

The White House. (2022). *National Strategy for the Arctic Region*. The White House.

Uppal, R. (2021, November 5). *Geopolitics now encompasses military, economic, technological, to Industry domains—International Defense Security & Technology*. https://idstch.com/geopolitics-now-encompasses-military-economic-technological-to-industry-domains/strategy-policy-governance-cat/geopolitics-strategy-technological-rivalries/

Urban, K. (2024). *Multi-stakeholder Data Access in Space-Based Climate Monitoring* (No. 299). Centre for International Governance Innovation. https://www.cigionline.org/publications/multi-stakeholder-data-access-in-space-based-climate-monitoring/

U.S. Department of Defense. (2024a). *Arctic Strategy*. U.S. Department of Defense.

U.S. Department of Defense. (2024b). *Climate Adaptation Plan*. U.S. Department of Defense.

U.S. Department of War. (2021, August 17). *Joint Statement on NORAD Modernization*. U.S. Department of War. https://www.war.gov/News/Releases/Release/Article/2735041/joint-statement-on-norad-modernization/

Van Deelen, G. (2025, December 16). Amid the Arctic's Hottest Year, Arctic Science Faces a Data Deficiency. *Eos*. https://eos.org/articles/amid-the-arctics-hottest-year-arctic-science-faces-a-data-deficiency

van der Wal, B. (2025, November 27). NATO's Polar Pressure Point: The Svalbard Archipelago and the Russian Challenge. *The Arctic Institute - Center for Circumpolar Security Studies*. https://www.thearcticinstitute.org/natos-polar-pressure-point-svalbard-archipelago-russian-challenge/

Vandakova, D. (2026, February 5). Overview of the Arctic Security. *Bloomsbury Intelligence & Security Institute (BISI)*. https://bisi.org.uk/reports/overview-of-the-arctic-security

VanHerck, G. (2021). *NORAD and USNORTHCOM Strategy*.

Vaynman, J. (2021). Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control. *Texas National Security Review*, *4*(4), 33–56.

Vaynman, J., & Volpe, T. A. (2023). Dual Use Deception: How Technology Shapes Cooperation in International Relations. *International Organization*, *77*(3), 599–632. https://doi.org/10.1017/S0020818323000140