Proceedings of 5th International Conference CNDCGS'2026
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.81**

The Multi-Domain Arctic and Its Challenges to Intelligence Staffs of Non-Arctic NATO Countries: A Czech Perspective

Radovan VASICEK[1]*, Ondrej KACMARIK[1], Jozef PODOBA[1], Tomas DOBROVOLNY[1], Karel MICHENKA[1]

[1]Department of Intelligence Support, Faculty of Military Leadership, University of Defence, Kounicova 156/65, 662 10 Brno, Czech Republic

*Correspondence: * radovan.vasicek@unob.cz*

Abstract

This article analyses how the evolving Arctic security environment generates new requirements for the intelligence staffs of non-Arctic North Atlantic Treaty Organisation (NATO) armies, using the Czech Army as a case study. Drawing on doctrinal analysis, scenario-based assessment, and a review of intelligence education, it identifies a structural mismatch between land-centric intelligence practice and the Arctic's multi-domain, hybrid, and environmentally extreme operational character. The article concludes that non-Arctic allies require proportionate doctrinal adaptation, differentiated professional education, and a limited but credible Arctic intelligence capability.

KEY WORDS: *Arctic security; military intelligence; hybrid threats; intelligence preparation of the operating environment; multi-domain operations; Czech Republic*

Citation: Vasicek, R., Kacmarik, O., Podoba, J., Dobrovolny, T., Michenka K. The Multi-Domain Arctic and Its Challenges to Intelligence Staffs of Non-Arctic NATO Countries: A Czech Perspective. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. https://doi.org/10.47459/cndcgs.2026.81

1. Introduction

The Arctic has undergone a marked strategic transformation in recent years, evolving from a peripheral region of limited military salience into an area of growing geopolitical and operational importance [1, 2]. Climate change, increased accessibility, renewed great-power competition, and the rising significance of northern sea lines of communication and critical infrastructure have together altered the strategic character of the High North [3, 4]. In consequence, NATO and allied analyses increasingly treat the Arctic not as a distant flank, but as an integral part of a wider deterrence and defence space connecting the North Atlantic, Nordic region, and Arctic approaches [5 ,6, 7, 8, 9, 10].

For intelligence staffs, this shift has significant implications. Future Arctic contingencies are unlikely to present themselves primarily through conventional land-force indicators; rather, they are more likely to emerge through a combination of maritime and undersea anomalies, cyber incidents, electromagnetic interference, infrastructure vulnerabilities, and hostile activity in the information environment [11, 12]. The Arctic should therefore be understood not simply as a cold-weather variant of familiar theatres, but as a distinct multi-domain intelligence problem shaped by environmental extremes, long distances, sparse infrastructure, and hybrid forms of competition [1].

These developments also carry important implications for non-Arctic NATO members [6, 10]. Even landlocked allies such as the Czech Republic may be required to support Alliance operations in the High North through force generation, staff contributions, or participation in multinational intelligence processes. At the same time, much of their professional military education, intelligence culture, and doctrinal practice remains oriented toward temperate, continental, and predominantly land-centric conditions. This creates a structural tension between the requirements of the Arctic theatre and the assumptions that continue to shape many army intelligence institutions outside the region.

This article examines how changes in Arctic security are generating new requirements for the intelligence staffs of non-Arctic NATO armies, using the Czech Army as a case study. It argues that credible support to NATO collective-defence operations in the High North does not require full-spectrum Arctic specialisation, but rather a limited and credible intelligence capability adapted to a multi-domain, hybrid, and environmentally demanding theatre.

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

2. Methodology and Limitations

A qualitative case-study approach is used to examine the implications of the Arctic operating environment for the intelligence staffs of a non-Arctic NATO army, with the Czech Army serving as the principal reference point. The analysis combines a review of NATO, allied, and national policy and doctrinal documents with selected academic and policy literature on Arctic security, hybrid threats, and multi-domain operations. To clarify the practical implications of these trends, it also employs a limited scenario-based perspective and draws selectively on practitioner-oriented material concerning intelligence education and preparation for High North contingencies.

The study is intended as an analytical and policy-oriented contribution rather than as a predictive or statistically representative one. Its findings are necessarily limited by reliance on open sources, the selective use of an illustrative scenario, and the fact that the Czech Republic is examined as a specific type of landlocked, non-Arctic allied contributor rather than as a universally representative case. The aim is therefore not to offer a comprehensive model for all NATO members, but to identify the principal areas in which land-centric intelligence institutions may need to adapt in order to support credible allied operations in the Arctic and sub-Arctic.

Against this backdrop, the study is guided by the following overarching research question: *How should the Czech Army's intelligence concepts, structures and skill sets be adapted to enable credible support to NATO collective-defence operations in the Arctic and sub-Arctic, given the region's multi-domain, hybrid and extreme-environment characteristics?*

3. The Arctic Operating and Threat Environment

The Arctic and sub-Arctic should not be understood as merely colder variants of familiar temperate theatres, but as distinct operating environments in which climate, distance, sparse infrastructure, and environmental volatility directly shape force employment, sustainment, and threat manifestation [1, 3, 5]. At the same time, the region is marked by unusually strong cross-domain interdependence: land operations cannot be assessed in isolation from maritime access, undersea infrastructure, air and missile approaches, cyber systems, the electromagnetic environment (EME), and the information environment [5, 7, 8, 10]. For intelligence staffs, this means that Arctic situational awareness depends less on any single domain than on the ability to interpret how multiple weak indicators interact across a fragile and tightly connected operational system.

3.1 Environmental Specificity

Allied assessments converge on the view that the Arctic imposes qualitatively different constraints on planning, tempo, and sustainment than those embedded in standard NATO land assumptions [1, 5]. Cold, darkness, rapid weather shifts, and the paucity of transport and support infrastructure compress decision-space and increase the operational penalty for misjudging terrain and climatic effects [1, 5]. In such conditions, mobility, access, and supportability are not secondary planning factors but central determinants of what forces can realistically do and how quickly they can do it [13].

For land forces, trafficability is both more fragile and more decisive than in temperate theatres. Snow cover, ice conditions, thawing permafrost, elevation, and limited road and rail networks can rapidly turn apparently usable terrain into an obstacle to manoeuvre, while logistics, maintenance, medical support, and force protection become more vulnerable at an earlier stage of operations. Arctic conditions also affect sensing, communications, and navigation. Polar conditions, weak redundancy, and dependence on long-range technical enablers make communications and positioning both more necessary and more fragile than in many continental settings. For non-Arctic allies, the key implication is that the Arctic changes the meaning of distance, tempo, and access from the outset; treating it as a familiar land theatre with worse weather risks distorting both planning and intelligence assessment [13].

3.2 The Multi-Domain and Hybrid Character

The Arctic threat environment is defined less by any single dominant domain than by the interaction of land, maritime, air, space-enabled, cyber, and information activities [5, 11, 14]. Recent allied and policy analyses emphasize that competition in the High North increasingly takes hybrid form, combining military and non-military instruments in ways calibrated to shape the environment below the threshold of open conflict [3, 4, 11, 15, 16, 23]. From an intelligence perspective, the central consequence is that early warning may emerge first through anomalies in infrastructure, communications, maritime behaviour, cyber activity, or information operations rather than through visible land-force posture alone [6, 7, 12].

3.2.1 Land Domain

On land, Russian forces in the European Arctic continue to anchor a layered posture linked to the defence of the Kola Peninsula, the protection of Northern Fleet assets, and wider regional deterrence signaling [5, 17]. Yet the land domain is shaped not only by regular force presence, but also by dual-use and ambiguously civilian activity [14, 16, 18]. Case material from Svalbard and the Norwegian High North suggests that state-owned companies, controlled tourism, research presence, and local influence mechanisms can affect political and operational conditions well before conventional military escalation occurs [16, 19]. For intelligence staffs, this means that the land picture cannot be reduced to order of battle alone; it must also include civilian vectors that can support access, influence, or shaping activity.

3.2.2 Maritime and Undersea Domain

The maritime and undersea domain is a central organising axis of Arctic competition [10, 20]. Russian strategy links military posture, bastion defence, economic interests, and claims connected to the Northern Sea Route, while growing traffic and infrastructure density increase both opportunity and vulnerability in northern waters [2, 17, 18, 20]. Hybrid-threat analyses stress that ports, offshore facilities, seabed cables, satellite ground stations, and maritime traffic systems constitute critical vulnerability nodes, and incidents in the wider European maritime space show how commercial or research activity can be used for surveillance, mapping, interference, or sabotage under plausible deniability [3, 11, 21, 26]. For NATO and non-Arctic contributors alike, maritime domain awareness, undersea infrastructure security, and attribution capacity are therefore core intelligence problems rather than specialist peripheral concerns [9, 11, 20, 21, 26].

3.2.3 Air, Space and Electromagnetic Environment

The Arctic air domain matters both as an operating space and as an avenue for signaling, long-range strike, and interference directed at Europe and North America [18]. Repeated Global Navigation Satellite System (GNSS) jamming and spoofing, limited diversion options, harsh weather margins, and the effects of high-latitude electromagnetic phenomena all make aerospace warning and airspace management especially sensitive to both hostile action and natural disruption [15]. In the Arctic, geomagnetic activity, solar storms, ionospheric irregularities, and auroral effects can degrade navigation, sensing, and communications even in the absence of deliberate interference, thereby complicating the distinction between environmental friction and hostile action. These challenges are reinforced by the region's dependence on space-enabled communications, navigation, and surveillance, all of which are particularly exposed to high-latitude limitations, electromagnetic disturbance, and infrastructure fragility [10, 21, 22]. For intelligence staffs, the practical implication is that interruptions in positioning, communications, or sensing may be operationally significant even when attribution remains uncertain, and must therefore be interpreted in conjunction with activity in other domains.

3.2.4 Cyber and information environment

Cyber and information activities in the Arctic are closely tied to infrastructure, governance, and social resilience [15]. Because many northern communities and installations depend on limited digital nodes and weakly redundant communications systems, even modest cyber disruption can produce disproportionate operational and political effects. At the same time, Russian and Chinese information activity seeks to shape narratives about militarisation, legality, sovereignty, local grievances, and the legitimacy of allied presence in the region [11, 23, 24, 25]. In practice, cyber and information operations support wider hybrid competition by obscuring intent, amplifying uncertainty, and complicating attribution [3, 11, 24]. For intelligence staffs, they must therefore be treated not as separate specialist categories but as integral parts of multi-domain warning and assessment.

3.3 Cross-domain interaction

The defining feature of the Arctic operating environment is the way in which these domains interact [1]. Environmental severity, long distances, and sparse infrastructure force military and civilian activity alike to rely on a thin network of high-value nodes: a limited number of ports, airfields, cables, depots, communications links, and small population centres. As a result, disturbances in one domain can rapidly generate consequences in others. A cable incident at sea, sustained GNSS disruption, cyber interference against transport or public administration, or coordinated information activity around a legal dispute can all have effects that cascade into logistics, governance, command and control (C2), and force protection [20, 21].

For intelligence staffs, this means that Arctic warning depends not simply on collecting more data, but on recognising patterns across domains before they become visible through conventional military indicators alone. The Arctic is therefore best understood as a multi-domain and hybrid intelligence problem in which the analytical challenge lies in connecting weak signals across a tightly coupled and environmentally fragile theatre [18].

4. Hybrid-Armed Arctic Contingency and Its Implications for Battalion and Brigade Intelligence Sections

A plausible contingency in the European High North is less likely to take the form of a large-scale surprise attack than of a calibrated hybrid-armed crisis centred, for example, on Svalbard and extending across northern Norway, Finland, and Sweden [9, 10, 12, 17, 19]. In such a scenario, pressure would likely develop through a combination of legal contestation, hostile information activity, cyber interference, electromagnetic disruption, anomalous maritime behaviour, and threats to critical infrastructure rather than through an immediate transition to overt conventional conflict [15, 19, 23, 24]. For the purposes of this analysis, it is assumed that the Czech Republic contributes forces to a NATO Forward Land Force (FLF) deployment in northern Finland or Sweden [5, 7, 8, 9, 27].

For battalion and brigade intelligence sections (S-2), the main difficulty in such a contingency would lie not in the absence of indicators, but in their dispersion across domains, agencies, and levels of command [22, 28]. Rather than tracking a clearly developing land threat, S-2 staffs would need to work with fragmented reporting on maritime anomalies, infrastructure incidents, GNSS disruption, cyber events, suspicious civilian activity, and shifts in the information space, often without immediate clarity as to whether these form part of a coordinated hostile campaign. Their task would therefore be less to produce a complete independent picture than to recognise potentially significant patterns early, report them in a disciplined manner, and relate them to a broader warning framework maintained at higher echelons.

For intelligence staffs deployed to such a theatre, the challenge would be qualitatively different from that encountered in temperate land operations. Standard intelligence preparation of the operating environment (IPOE) remains relevant, but it must be adapted to conditions in which terrain, infrastructure, weather, communications, and sensor performance are less predictable, and in which adversary activity may be deliberately designed to remain below the threshold of clear attribution [29]. Mobility estimates, likely avenues of approach, sustainment assessments, and threat templates cannot simply be transferred from continental assumptions to the Arctic battlespace without distortion [13].

These difficulties are compounded by the fact that many of the most consequential indicators in an Arctic contingency lie beyond the organic collection and analytical reach of a land-centric tactical staff [11, 26, 28]. Effective support to battalion and brigade commanders would therefore depend on a credible operational-level joint intelligence preparation of the operating environment (JIPOE), prepared in advance by joint headquarters intelligence staffs (J-2) able to integrate maritime, undersea, cyber, air, space, infrastructure, and information-environment factors into a single theatre picture [22, 30]. Without that higher-level framework, local incidents risk appearing disconnected even when they form part of a coordinated hostile campaign.

A further challenge lies in the weakness and unevenness of intelligence, surveillance, and reconnaissance (ISR) coverage in the High North, where darkness, snow, ice fog, communications constraints, electromagnetic effects, and extreme cold degrade collection and complicate interpretation [31]. In addition to affecting sensors and connectivity, low temperatures can reduce the endurance and reliability of ISR platforms and personnel, including dismounted reconnaissance teams and battery-powered uncrewed aerial systems, thereby narrowing effective collection windows [28]. Tactical intelligence staffs must therefore distinguish carefully between gaps caused by hostile interference, those produced by environmental conditions, and those arising from the intrinsic limits of allied Arctic surveillance architecture. This increases the importance of disciplined reporting, baseline awareness, calibrated confidence levels, and close interaction with higher-echelon intelligence staffs responsible for collection management and theatre fusion.

Multinational interoperability adds another layer of difficulty [6, 30]. Forward-deployed formations in the High North are likely to rely heavily on host-nation data, allied ISR, and multinational intelligence-sharing arrangements, yet releasability restrictions, bandwidth constraints, and uneven procedural familiarity can fragment the picture available to tactical staffs [28]. For non-Arctic contributors such as the Czech Republic, intelligence adaptation must therefore be understood as a multi-echelon problem: battalion and brigade S-2s require Arctic-specific preparation, but their effectiveness will depend equally on whether operational and joint-level staffs can connect tactical observations to a broader multi-domain warning framework.

5. The Czech Case: Intelligence Challenges for a Central European Landlocked Contributor

The general challenges outlined above are particularly acute in the Czech case. For much of the past decade, the Arctic occupied only a marginal place in Czech strategic and defence planning, and in the Long Term Perspective for Defence 2030 it was treated less as a potential theatre of allied engagement than as an explicit exception to expected force employment. The document states both that the Czech Armed Forces can deploy in all climatic zones *"except the Arctic areas"* [32] and that they must be able to perform their tasks without geographical restrictions *"except the Arctic areas and in unusual environments"* [32]. That earlier framing is increasingly difficult to sustain, however, as more recent Czech strategy documents place greater emphasis on alliance defence, extra-territorial security interests, and the wider consequences of Russian aggression for European security, including the Arctic [33]. An exception to this otherwise limited Czech experience in the wider High North is the Czech Air Force's repeated participation in NATO

Air Policing in Iceland, which has provided limited operational familiarity with northern conditions and theatre-specific allied procedures.

From an intelligence perspective, the central issue for the Czech Republic is not simply whether land forces can operate in snow and cold, but whether Czech intelligence structures can support collective-defence operations in a theatre where many of the most important indicators emerge outside the traditional land domain [22, 34]. If the Czech Army were required to contribute forces to a NATO deployment in northern Finland or Sweden, effective intelligence support would depend not only on tactical S-2 adaptation, but also on the ability of operational-level staffs to interpret and contribute to theatre-wide JIPOE, warning, collection planning, and multinational intelligence fusion.

This creates a specific challenge for a landlocked ally whose intelligence institutions have historically been land-centric. Czech intelligence culture, doctrine, and education have been shaped primarily by continental land operations, with growing attention to cyber and hybrid threats, but with much less systematic emphasis on maritime awareness, undersea infrastructure, Arctic communications fragility, and host-nation or allied reporting ecosystems relevant to the High North. In an Arctic contingency, however, these areas are not supplementary but integral to the warning problem. The Czech case therefore illustrates a broader institutional issue facing non-Arctic NATO armies: land-centric intelligence structures may remain competent within their traditional frame while still being insufficiently prepared for a theatre in which operationally significant indicators often emerge first elsewhere [8].

At the same time, the Czech case does not imply a need for full-spectrum Arctic specialisation. The Czech Armed Forces Development Concept 2035 points toward broader multi-domain capability development and recognises the importance of participation in multinational command structures and information-sharing arrangements, including in areas where the Czech Republic is structurally dependent on allied frameworks [35]. For the Czech Army, the practical implication is that adaptation should be approached as a multi-echelon task. Battalion and brigade S-2 sections would require only limited but targeted Arctic-oriented competence, whereas a smaller cadre of officers would need deeper preparation for service in division, corps, national joint headquarters, and NATO intelligence structures, where Arctic warning and JIPOE are assembled and where a single multi-domain analytical picture is translated into tactically relevant support. In this sense, Czech credibility in the High North will depend less on becoming an Arctic specialist force than on building a proportionate intelligence capability able to connect tactical reporting with a wider allied multi-domain picture.

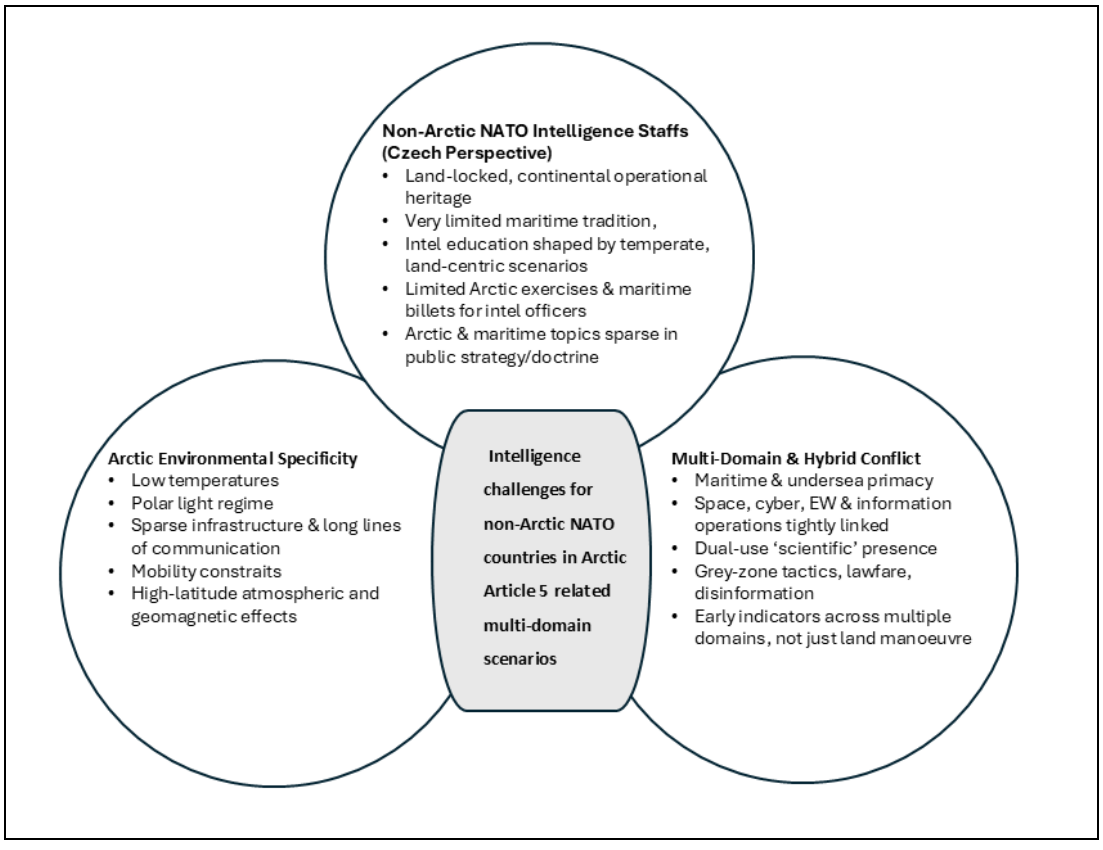

Fig.1. Interplay of the three challenge dimensions confronting intelligence staffs of non-Arctic NATO armies in an Arctic Article 5 contingency

6. Implications for Doctrine, Education, and Roles

For the Czech Army, the Arctic problem should be understood not primarily as a matter of climatic adaptation, but as a requirement to adjust intelligence practice to a distinct multi-domain operating environment. The most efficient doctrinal response is therefore selective adaptation rather than wholesale revision. Recently introduced IPOE and JIPOE procedures remain usable, but they should be supplemented with Arctic-relevant indicators, environmental and mobility factors, infrastructure-related warning criteria, and examples of cross-domain escalation specific to the High North [13]. Such adaptation should apply not only to battalion and brigade S-2 sections, but also to J-2 staffs responsible for operational-level warning, collection planning, and intelligence fusion.

Educational adaptation should follow a differentiated rather than uniform model [22]. A common baseline of Arctic literacy is needed across the intelligence community, including the operational effects of extreme climate, sparse infrastructure, communications fragility, hybrid activity, and multinational interoperability in the High North. Beyond that shared foundation, however, learning objectives should diverge by echelon and function. [23] Tactical intelligence officers require applied competence in Arctic IPOE, local warning, and anomaly reporting, whereas operational- and joint-level officers require stronger preparation in multi-domain synthesis, allied ISR architectures, theatre-wide warning, and multinational intelligence integration.

The personnel implication is that the Czech Republic does not need full-spectrum Arctic specialisation, but rather a limited and credible cadre structure aligned with likely alliance roles [7]. Most battalion and brigade S-2 personnel require only targeted pre-deployment and staff-training preparation, while a smaller group of officers should be deliberately prepared for service in division, corps, joint, and NATO intelligence structures, where Arctic assessments are assembled and translated into operational guidance. In this sense, Arctic competence should be treated as an element of interoperability and force credibility rather than as an isolated specialist niche [6, 8].

Table 1. Practical division of labor rather than a hierarchy of prestige.

Tier	Echelon / Role	Primary Focus	Knowledge Requirements	Training Pathway
1	**Battalion / Brigade S-2**	Applied Arctic IPOE, local warning, hybrid anomaly detection	Environmental effects, terrain cycles, infrastructure vulnerabilities, basic maritime and air-domain literacy, host-nation reporting context	Short Arctic IPOE module; pre-deployment package; tabletop exercises with multi-domain injects
2	**Division / Corps G-2 or National Joint HQ J-2**	Operational-level JIPOE, multi-domain synthesis, theatre warning	Hybrid escalation pathways, allied ISR architecture, collection gaps in the High North, maritime and undersea intelligence interfaces, multinational fusion procedures	Advanced modules; participation in Arctic-focused NATO exercises; short exchanges with Nordic or maritime headquarters
3	**NATO or Allied Joint Intelligence Staffs**	Alliance-level Arctic intelligence integration and policy support	Russian Arctic posture, Chinese dual-use activity, infrastructure security, Arctic information environment, NATO command and intelligence arrangements	Pre-assignment familiarisation; specialist courses; structured post-tour knowledge transfer into Czech institutions

This model, depicted in Table 1, reflects a practical division of labour rather than a hierarchy of prestige. Tier 1 personnel need tools for immediate use in their area of operations rather than deep strategic expertise; Tier 2 officers must be able to connect Czech contributions to broader operational assessment; and Tier 3 officers should function as knowledge brokers who translate alliance-level Arctic intelligence into realistic training, planning, and doctrinal implications for Czech forces. Such differentiation is especially important for a small, landlocked ally, because it allows scarce personnel and educational resources to be concentrated where they can have the greatest operational effect.

The broader implication is that Arctic competence should be treated as an element of interoperability, not as an optional stand-alone specialty. For the Czech Army, a proportionate Arctic intelligence capability would not require major institutional transformation, but it would require continuity: recurring training, deliberate personnel management, modest doctrinal adjustment, and systematic use of allied expertise. If developed in this way, Czech adaptation would remain aligned with national scale and geography while still enabling a credible contribution to NATO deterrence and defence in the High North.

7. Conclusions

The Arctic should not be understood by non-Arctic NATO armies as a remote or exceptional theatre, but as an increasingly relevant part of the Alliance's wider deterrence and defence space. For intelligence staffs, the central challenge is that Arctic warning and assessment depend on a multi-domain logic in which environmental conditions,

maritime and undersea activity, cyber interference, communications fragility, and information operations may be more decisive than traditional land-force indicators alone.

For the Czech Army, this creates a structural mismatch between historically land-centric intelligence practice and the requirements of a theatre in which effective support depends on operational- and joint-level fusion as much as on tactical reporting. The appropriate response is therefore not full-spectrum Arctic specialisation, but proportionate adaptation: selective doctrinal revision, differentiated professional education, and the deliberate preparation of a limited cadre able to contribute credibly to allied Arctic intelligence processes.

In this sense, Arctic intelligence readiness should be treated less as a question of geography than of interoperability and alliance credibility. For non-Arctic allies such as the Czech Republic, the aim is not to replicate the capabilities of Arctic states, but to ensure that national intelligence staffs can recognise, interpret, and connect the multi-domain indicators on which credible allied warning in the High North increasingly depends.

References

1. **NATO Strategic Foresight Branch.** Regional Perspectives Report: The Arctic and High North. Norfolk: HQ SACT, 2021. Available at: https://shorturl.at/WWyQ6 (accessed on 4 April 2026).
2. **Conley, H. A., et al**. A New Era of Arctic Geopolitics: Russia–PRC Strategic Alignment Is Driving Unprecedented Regional Collaboration. GMF Report, 2024. 12 p.
3. **Vandakova, D.** Overview of the Arctic Security. Bloomsbury Intelligence & Security Institute, 2023. Available online: https://shorturl.at/Oa7mg (accessed on 20 March 2026)
4. **Vlček, T., Chovančík, M., Uhlířová, K., Jirušek, M.** Strained Relations in the High North: Steps-to-War Analysis of Conflict Potential in the Arctic. *Europe-Asia Studies*, 76(3), 2024, p. 289–313. DOI: 10.1080/09668136.2023.2292471. Available online: https://shorturl.at/bKW4E (accessed on 10 April 2026).
5. **NATO.** Arctic security. NATO Topic Page, 15 February 2026. Available online: https://shorturl.at/OaolF (accessed on 4 April 2026).
6. **Gricius, G.** NATO in the Arctic. North American and Arctic Defense and Security Network, 7 June 2024. 5 p.
7. **Black, J., et al.** NATO Enlargement Amidst Russia's War in Ukraine. RAND Europe, 2024. 32 p.
8. **NATO.** Secretary General Annual Report 2025. Brussels: NATO, 2026. – 76 p. Available online: https://shorturl.at/VVj2x (accessed on 8 February 2026).
9. **Wieslander, A., Rácz, A.** How Sweden and Finland's Membership in NATO Affects the High North. Atlantic Council Issue Brief, 4 November 2024. – 9 p. Available online: https://shorturl.at/Fe7mk (accessed on 14 March 2026).
10. **Gricius, G., Glesby, N.** NATO and the Arctic in the 2020s. Arctic Yearbook, 2025, 12 p.
11. **Schalin, J., Arts, S.** *Bracing for a Cold Front: Assessing Russian and Chinese Strategic Objectives and Hybrid Threat Capabilities in the Arctic.* Hybrid CoE Paper 28. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, January 2026. 44 p. Available online: https://www.hybridcoe.fi/publications/bracing-for-a-cold-front-assessing-russian-and-chinese-strategic-objectives-and-hybrid-threat-capabilities-in-the-arctic/ (accessed on 15 March 2026).
12. **Østhagen, A.** The Arctic after Russia's Invasion of Ukraine: The Increased Risk of Conflict and Hybrid Threats. Hybrid CoE Paper 18, 2023. 20 p.
13. **Everett, M.** Intelligence Preparation of the Operational Environment in the Subarctic. Military Intelligence Professional Bulletin, July–December 2024, p. 1–5. Available online: https://www.lineofdeparture.army.mil/Portals/144/PDF/Journals/Intelligence/2024/E_IPOE_v2.pdf (accessed on 7 February 2026).
14. **Bouffard, T. J., Grau, L. W., Bartles, C. K., Boulègue, M**. Russian Arctic Land Forces and Defense Trends Redefined by NATO and Ukraine. Parameters, 55(3), 2025. p. 51–66. Available online: https://press.armywarcollege.edu/parameters/vol55/iss3/6/ (accessed on 8 March 2026)
15. **Kertysova, K., Gricius, G.** *Countering Russia's Hybrid Threats in the Arctic.* London: European Leadership Network, August 2023. Available online: https://europeanleadershipnetwork.org/report/countering-russias-hybrid-threats-in-the-arctic/ (accessed on 25 March 2026).
16. **Hoogensen Gjørv, G.** Security and Geopolitics in the Arctic: The Increase of Hybrid Threat Activities in the Norwegian High North. *Hybrid CoE Working Paper* 30. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, March 2024. – 27 p. Available online: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-30-security-and-geopolitics-in-the-arctic-the-increase-of-hybrid-threat-activities-in-the-norwegian-high-north/ (accessed on 21 March 2026)
17. **Obradovic, L.** Russian Strategic Culture and Deterrence in the Arctic. *Space and Defense*, 16(1), 2025, Article 4. DOI: 10.32873/uno.dc.sd.16.01.1304. Available online: https://digitalcommons.unomaha.edu/spaceanddefense/vol16/iss1/4/ (accessed on 8 March 2026)
18. **Borozna, E.** The Evolution of Russia's Arctic Strategy after the War in Ukraine. *Arctic Yearbook*, 2025, 26 p. Available online: https://arcticyearbook.com/images/yearbook/2025/Scholarly_Papers/5SP_AY2025_Borozna.pdf (accessed on 24 April 2026).

19. **Stensrud, C. J., Østhagen, A.** Hybrid Warfare at Sea? Russia, Svalbard and the Arctic. *Scandinavian Journal of Military Studies*, 7(1), 2024, p. 111–130. DOI: 10.31374/sjms.233.
20. **Bouffard, T. J.** Russian Ambitions to Control Freedom of Navigation and Arctic Access: Refined Data Challenging Moscow's Northern Sea Route Claims. *Arctic Yearbook*, 2025, 21 p. Available online: https://arcticyearbook.com/images/yearbook/2025/Scholarly_Papers/6SP_AY2025_Bouffard.pdf (accessed on 23 March 2026).
21. **Kahraman, A. L.** China's Digital Footprint in the Arctic: The Strategic Role of Satellite and Subsea Cable Infrastructure. *The Arctic Institute*, China Series 2025. Available online: https://www.thearcticinstitute.org/chinas-digital-footprint-arctic-strategic-role-satellite-subsea-cable-infrastructure/ (accessed on 18 March 2026).
22. **Maddox, M., Lea, L.** Polar Perspectives No. 13: The Intelligence Community Must Evolve To Meet the Reality of Arctic Change. Wilson Center Polar Institute, May 2023. Available online: https://shorturl.at/2sBNX (accessed on 7 April 2026).
23. **Rapper, J.** China's Arctic Strategy and Hybrid Warfare: Targeting Governance and Strategic Responses. *The Arctic Institute*, China Series 2025. Available online: https://www.thearcticinstitute.org/chinas-arctic-strategy-hybrid-warfare-targeting-governance-strategic-responses/ (accessed on 18 March 2026).
24. **Landriault, M.** Russian Media Coverage of Arctic Issues: Changes Since the Invasion of Ukraine. *Arctic Yearbook*, 2024, Briefing Note, p. 1–5. Available online: https://arcticyearbook.com/images/yearbook/2024/Briefing_Notes/BN1_Landriault.pdf (accessed on 7 April 2026).
25. **Lackenbauer, P. W., Bouffard, T., Lajeunesse, A.** Russian Information Operations: The Kremlin's Competitive Narratives and Arctic Influence Objectives. *Journal of Peace and War Studies*, 4th Edition, October 2022, p. 161–186. Available online: https://archives.norwich.edu/digital/collection/jpws/id/56/ (accessed on 19 March 2026).
26. **Kaushal, S.** Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure. RUSI Commentary, 24 May 2023. Available online: https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure (accessed on 5 April 2026).
27. **Government of Norway; Government of Sweden; Government of Finland.** Joint Statement on Cold Response 26 and NATO's Forward Land Forces in Finland. 16 March 2026. Available online: https://www.government.se/statements/2026/03/joint-statement-on-cold-response-26-and-natos-forward-land-forces-in-finland-by-the-ministers-of-defence-of-finland-sweden-and-norway (accessed on 12 April 2026).
28. **Deitz, R.** Multinational Intelligence Sharing and Interoperability: Lessons from WFX 24-03 and Avenger Triad 24. Military Intelligence. Line of Departure / U.S. Army Intelligence Center, 2025. Available online: https://www.lineofdeparture.army.mil/Journals/Military-Intelligence/Military-Intelligence-Archive/Continuous-Transformation-Special-Edition/Intelligence-Sharing/ (accessed on 10 April 2026).
29. **Department of the Army.** ATP 2-01.3, Intelligence Preparation of the Operational Environment. Washington, DC: Headquarters, Department of the Army, 23 January 2024 (Change 2). 234 p.
30. **NATO.** NATO Secretary General outlines new activity – Arctic Sentry – ahead of Defence Ministers meeting. NATO News, 11 February 2026. Available online: https://www.nato.int/en/news-and-events/articles/news/2026/02/11/nato-secretary-general-outlines-new-activity-arctic-sentry-ahead-of-defence-ministers-meeting (accessed on 15 March 2026).
31. **Barrie, D., Childs, N., Michel, Y., Sabatino, E., Schreer, B.** Northern Europe, the Arctic and the Baltic: The ISR Gap. International Institute for Strategic Studies, December 2022. Available online: https://www.iiss.org/research-paper/2022/12/northern-europe-the-arctic-and-the-baltic-the-isr-gap/ (accessed on 10 April 2026).
32. **Ministry of Defence of the Czech Republic.** The Long Term Perspective for Defence 2030. Prague: Ministry of Defence of the Czech Republic, 2015. Available online: https://www.mo.gov.cz/images/id_8001_9000/8503/the_long_term_perspective_for_defence_2030.pdf (accessed on 14 April 2026).
33. **Government of the Czech Republic.** Security Strategy of the Czech Republic 2023. Prague, 2023. Available online: https://mzv.gov.cz/file/5161068/Security_Strategy_of_the_Czech_Republic_2023.pdf (accessed on 14 April 2026).
34. **Sukhankin, S., Lackenbauer, P. W.** Looking Beyond China: Non-Western Actors in the Russian Arctic after February 2022. NAADSN Strategic Perspectives, November 2024. Available online: https://www.naadsn.ca/wp-content/uploads/2025/01/24nov-StrategicPerspectives-Russian_non-arctic-states-SS_PWL.pdf (accessed on 15 March 2026)
35. **Ministry of Defence of the Czech Republic.** Koncepce výstavby Armády České republiky 2035 [Czech Armed Forces Development Concept 2035]. Prague: Ministry of Defence of the Czech Republic, 2024. Available online: https://mocr.mo.gov.cz/images/id_40001_50000/46088/KVA__R_2035_Final.pdf (accessed on 14 April 2026).