EMERGING TECHNOLOGICAL AND OPERATIONAL CAPABILITIES FOR SPACE WARFARE

PART THREE OF "GRAY ZONES WITHIN THE ARCTIC SPACE DOMAIN"

Peyton Newsome

21 NOVEMBER 2025

New capabilities are transforming the Arctic into a more transparent and data-rich operating environment, yet they also heighten the region's dependence on vulnerable space-based communications and command systems. The challenging Arctic environment requires new forms of resilience, where allied cooperation has become essential to sustaining persistent surveillance and ensuring shared situational awareness across the High North**. This brief examines how emerging space technologies and operational capabilities are reshaping the strategic landscape of Arctic security, particularly within the gray-zone**. By integrating emerging technologies with modernized early warning architectures, improved SATCOM resilience, and enhanced allied data cooperation, the United States and its partners can strengthen deterrence in an increasingly contested Arctic space domain.

26-P-0132

CONTEXT

The Arctic remains the frontline of North American aerospace defense, yet the region's early warning architecture lags behind modern threat capabilities. Legacy satellite systems struggle in the Arctic, where geostationary platforms cannot reliably cover areas above roughly 65° north, creating significant gaps in ISR and introducing line-of-sight–related delays and timing issues.[i] The Northern Warning System (NWS), originally designed in the 1980s to replace the Distant Early Warning Line, relies on near-obsolete technology meant for Cold War-era aircraft rather than hypersonic, cruise missile, or unmanned aerial threats.[ii] Its network of radars provides only partial situational awareness, reflecting a fragmented evolution of detection systems rather than an integrated, all-domain network.[iii]

While the Upgraded Early Warning Radar (UEWR) and Pituffik Space Base now contribute advanced space surveillance capabilities, the larger architecture remains siloed. SPACECOM provides space-based awareness, while NORTHCOM and NORAD manage the defense response, creating a structural division that inhibits real-time coordination across air, space, and cyber domains.[iv] The anticipated Golden Dome system aims to unify these sensors under a single command and control structure capable of countering ballistic, hypersonic, and cruise missiles, but its implementation remains incomplete.

Compounding these challenges are infrastructure and environmental constraints. The U.S. Space Force's plan to expand ground-based interceptor silos in Alaska by 50% requires substantial construction in extreme Arctic conditions and additional command and control facilities.[v] Such projects underscore both the importance and fragility of Arctic-based deterrence assets.

SPACE-BASED ISR AND ARCTIC SURVEILLANCE

Emerging space technologies now provide unprecedented capacities to observe and interpret activities across the Arctic's vast and sparsely populated terrain. Synthetic aperture radar satellites can monitor maritime and land movements in any weather, while thermal imaging satellites can detect human or vehicular activity during the polar night.[vi] Together, these tools are turning the Arctic into an increasingly transparent operating environment where concealment is becoming more difficult.

However, this growing transparency introduces new vulnerabilities. Arctic satellite communications (SATCOM) remain limited by narrowband frequencies, constrained data rates, and high latency.[vii] The Enhanced Polar System provides encrypted communications, but the overall network is insufficient for the full spectrum of operational requirements. Aerial and maritime ISR platforms (e.g., P-8 reconnaissance aircraft, unmanned sea drones) offer only partial coverage due to range and endurance limitations.[viii]

This gap makes the Arctic highly dependent on space-based command, control, and communication networks. Initiatives like Joint All Domain Command and Control (JADC2) aim to unify space, cyber, and terrestrial data streams into a single decision-making ecosystem.[ix] Yet, this integration is predicated on assured access to both cyberspace and space, exposing the system to disruption through non-kinetic gray-zone tactics such as jamming, spoofing, or cyber intrusion.

GRAY-ZONE DYNAMICS IN SPACE

In the evolving gray-zone environment, space-based competition is characterized less by destruction than by positioning. Actions such as satellite repositioning, frequency interference, or blocking access to orbital slots can alter the strategic balance without triggering open conflict.[x] This "silent choreography" enables states to cloak military objectives behind civilian or commercial operations, complicating attribution and deterrence.[xi]

Artificial intelligence (AI) has become a critical enabler in this context. The U.S. Space Force's Rapid and Resilient Command and Control (R2C2) program seeks to automate threat detection and orbital management.[xii] Meanwhile, China's AI-driven satellite imagery analysis, said to be for tracking debris, underscores the dual-use nature of space technology, as the same systems can track adversary satellites and assets.[xiii] AI thus enhances both the speed and subtlety of gray-zone maneuvers, identifying patterns or anomalies that may signal covert aggression.

At the same time, low Earth orbit (LEO) constellations, such as Starlink, have demonstrated resilience and redundancy under cyber and electronic warfare conditions, as observed in Ukraine.[xiv] These networks provide both strategic communication channels and potential countermeasures to orbital interference. The rapid proliferation of commercial and military satellites, however, also expands the attack surface for adversaries seeking to exploit vulnerabilities through cyber or electromagnetic means.

Given the increasingly dual-use nature of space infrastructure, it is important consider how these systems serve both strategic requirements and community needs. Although polar-orbiting satellites generate immense imagery and environmental data, their value to Arctic communities depends on making that information usable and relevant on the ground. Initiatives like SMARTIce, which integrates Indigenous expertise with satellite measurements through community-based observers, and tools such as IcySea, which provides low-bandwidth ice, weather, and navigation updates for local operators, demonstrate how emerging capabilities can become practical resources for those living and working in the High North.[xv]

NATO, ALLIED COOPERATION, AND THE ARCTIC DIMENSION

NATO countries (and the firms operating within them) control over half of all active satellites currently in orbit.[xvi] NATO's Allied Persistent Surveillance from Space (APSS) initiative integrates national and commercial space assets into a virtual constellation known as Aquila to improve collective intelligence sharing.[xvii] Maintaining a baseline of 50 operational satellites for all-domain autonomy will require extensive cooperation, data-sharing agreements, and AI-enabled automation across allies.[xviii]

NATO has taken significant steps to strengthen allied coordination in the space domain. The NATO Space Centre at Allied Air Command in Ramstein, Germany, works alongside national space agencies to generate interoperable products and services (e.g., satellite imagery, PNT, and early-warning support) for use across the alliance.[xix] In 2023, NATO expanded this effort by establishing a Space Centre of Excellence in Toulouse, France, to advance alliance-wide development, training, and expertise in areas such as space domain awareness, operational space support, and coordination.[xx] A comparable model of collaboration is emerging in the Arctic communications sphere as well, illustrated by the Northlink initiative, in which thirteen members are jointly examining options for a secure, resilient, and reliable multinational satellite communications system for high-latitude operations.[xxi]

Cyber resilience has also emerged as a key priority. Mitigation strategies include advanced cryptography, post-quantum encryption, and AI-based intrusion detection to safeguard space assets from interference.[xxii] For Arctic operations where SATCOM reliability directly underpins deterrence and disaster response, such measures are indispensable.

RECOMMENDATIONS

1. **Modernize Arctic Early Warning and Communications.** Replace the Northern Warning System with an integrated, all-domain detection architecture that fuses radar, space, and cyber data streams under unified command and control (e.g., through Golden Dome or JADC2).

2. **Enhance Space-Based Resilience.** Invest in redundant LEO constellations, encrypted Arctic SATCOM, and cyber-hardened AI analytics to ensure persistent situational awareness under contested conditions.

3. **Expand Allied Coordination through APSS and NORAD Renewal.** Integrate NATO's APSS with North American early warning modernization efforts, leveraging shared satellite data for Arctic monitoring and missile defense.

4. **Leverage Emerging Manufacturing and AI Innovations.** Support research into in-space additive manufacturing and autonomous maintenance systems to enhance satellite longevity and reduce launch dependency. By producing components directly in orbit through techniques like 3D printing, space-based additive manufacturing minimizes the volume of material that has to be launched from Earth, which in turn makes missions lighter and reduces fuel demands.[xxiii]

CONCLUSION

Gray-zone competition in space is reshaping Arctic security by enabling subtle, non-kinetic actions that challenge traditional deterrence without crossing the threshold of open conflict. As AI, cyber capabilities, and orbital systems become increasingly intertwined, maintaining stability in the High North will depend on resilient, integrated detection and decision frameworks that can rapidly identify and respond to ambiguous threats. Ensuring this resilience will require both advanced technological investment and strengthened coordination among allies operating across the Arctic and space domains.

Author's Disclaimer: The views expressed in this Brief are those of the author and do not reflect the official policy or position of the U.S. Department of War or of the U.S. Government.

ENDNOTES

[i] Byers, M. (2024). *Outer Space and the Arctic: Connections, Opportunities, Challenges* (303; CIGI Papers). Centre for International Governance Innovation. https://www.cigionline.org/publications/outer-space-and-the-arctic-connections-opportunities-challenges/

[ii] Tukker, P. (2022, May 10). The DEW Line at 65: Future unclear for the North's aging radar sites. *CBC News*. https://www.cbc.ca/news/canada/north/dew-line-65-years-norad-1.6446875

[iii] Lynch, M. E. (2025). From the Last Frontier to the Final Frontier: The Polar Region and Space Security. *Space and Defense*, *16*(1). https://doi.org/10.32873/uno.dc.sd.16.01.1307

[iv] Lynch, M. E. (2025). From the Last Frontier to the Final Frontier: The Polar Region and Space Security. *Space and Defense*, *16*(1). https://doi.org/10.32873/uno.dc.sd.16.01.1307

[v] U.S. Space Force. (n.d.). *About the United States Space Force*. United States Space Force. https://www.spaceforce.mil/About-Us/FactSheets/Article/2197716/cobra-dane-radar/

[vi] Byers, M. (2024). *Outer Space and the Arctic: Connections, Opportunities, Challenges* (303; CIGI Papers). Centre for International Governance Innovation. https://www.cigionline.org/publications/outer-space-and-the-arctic-connections-opportunities-challenges/

[vii] Jones, K. L., & Cashin, L. M. (2024). SPACE-ENABLED CAPABILITIES FOR CONNECTING AND COLLABORATING IN THE ARCTIC. *Space Agenda 2025*. https://csps.aerospace.org/sites/default/files/2024-10/04c_Arctic_Jones-Cashin_20241017.pdf

[viii] Chase, T. (2022, January 19). *There's a Race for Arctic-Capable Drones Going On, and the United States is Losing*. Modern War Institute. https://mwi.westpoint.edu/theres-a-race-for-arctic-capable-drones-going-on-and-the-united-states-is-losing/; Brewer, E., Hersman, R., & Simon, M. (2021). Deep Dive Debrief: Strategic Stability and Competition in the Arctic. *CSIS Briefs*. https://www.csis.org/analysis/deep-dive-debrief-strategic-stability-and-competition-arctic

[ix] Barth, T. H. (2024). *Cyberspace and Space Similarities, Differences, and Related National Security Issues*. Institute for Defense Analyses. https://www.ida.org/-/media/feature/publications/c/cy/cyberspace-and-space-similarities-differences-and-related-national-security-issues/3001828.ashx

[x] Sokolski, H. (2022, January 17). A China-US war in space: The after-action report. *Bulletin of the Atomic Scientists*. https://thebulletin.org/premium/2022-01/a-china-us-war-in-space-the-after-action-report/

[xi] Dugger, A. T. (2025, February 14). *Space as a Gray Zone: The Future of Orbital Warfare*. Modern War Institute. https://mwi.westpoint.edu/space-as-a-gray-zone-the-future-of-orbital-warfare/, https://mwi.westpoint.edu/space-as-a-gray-zone-the-future-of-orbital-warfare/

[xii] Hadley, G. (2024, December 12). Space Force Is Testing AI to Automate Ops—And Eyeing More. *Air & Space Forces Magazine*. https://www.airandspaceforces.com/space-force-testing-ai-automate-ops/

[xiii] Husain, A. (2024, August 19). *The Military Applications Of Artificial Intelligence In Space*. Forbes. https://www.forbes.com/sites/amirhusain/2024/08/19/the-military-applications-of-artificial-intelligence-in-space/

[xiv] Ogden, T., Knack, A., Lebret, M., Black, J., & Mavroudis, V. (2024, February 23). *The Role of the Space Domain in the Russia-Ukraine War*. Centre for Emerging Technology and Security. https://cetas.turing.ac.uk/publications/role-space-domain-russia-ukraine-war

[xv] Marsh, D. (2024, November 1). *Ever Forward: The Unique Relationship Between the Arctic and Space*. Wilson Center. https://www.wilsoncenter.org/blog-post/ever-forward-unique-relationship-between-arctic-and-space

[xvi] NATO. (2025, July 30). *NATO's approach to space*. NATO. https://www.nato.int/en/what-we-do/deterrence-and-defence/natos-approach-to-space
[xvii] NATO Communications and Information Agency. (n.d.). *Space*. NATO Communications and Information Agency. https://www.ncia.nato.int/about-us/technology-and-innovation/space
[xviii] Cournoyer, J. (2025). *Securing the space-based assets of NATO members from cyberattacks* (International Security Programme) [Research Paper]. Chatham House. https://www.chathamhouse.org/sites/default/files/2025-05/2025-05-14-nato-space-cyberattacks-cournoyer.pdf
[xix] Allied Air Command Public Affairs Office. (2025). *NATO space domain, a new frontier of security*. Ac.Nato.Int. https://ac.nato.int/archive/2025-2/nato-space-domain--a-new-frontier-of-security.aspx
[xx] Giordano, P. (2024, September 3). NATO's Space Centre of Excellence: A Cornerstone for Alliance Space Initiatives. *NATO's ACT*. https://www.act.nato.int/article/space-coe-2024/
[xxi] *NATO launches five new multinational cooperation initiatives that enhance deterrence and defence*. (2024, October 7). NATO. https://www.nato.int/en/news-and-events/articles/news/2024/10/17/nato-launches-five-new-multinational-cooperation-initiatives-that-enhance-deterrence-and-defence
[xxii] Cournoyer, J. (2025). *Securing the space-based assets of NATO members from cyberattacks* (International Security Programme) [Research Paper]. Chatham House. https://www.chathamhouse.org/2025/05/securing-space-based-assets-nato-members-cyberattacks/03-evolution-space-policies-nato-and
[xxiii] Inside Metal Additive Manufacturing. (2024, March 18). *Impact of Additive Manufacturing on Space Exploration*. Inside Metal Additive Manufacturing. https://insidemetaladditivemanufacturing.com/2024/03/18/impact-of-additive-manufacturing-on-space-exploration/