DOPSR 26-P-0126

GOVERNANCE OF SPACE WARFARE FOR ARCTIC SECURITY

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

Peyton Newsome

21 November 2025

Satellites are indispensable to Arctic operations, underpinning navigation, communications, monitoring, and intelligence. This dependence makes the region uniquely vulnerable to gray zone space warfare, including cyberattacks, jamming, spoofing, and the weaponization of dual-use technologies. **This brief examines how governance gaps in space law create vulnerabilities for Arctic operations, where the interdependence of civilian and military systems coupled with legal ambiguity creates risks of escalation, strategic vulnerability, and severe consequences for Arctic communities and industries**. It recommends strengthening space governance through improved transparency and situational awareness, integrating space and cyber regulations, clarifying state accountability for commercial actors, and promoting confidence-building measures among Arctic and spacefaring nations.

CONTEXT

Modern militaries are increasingly dependent on satellites for communications, navigation, and intelligence. Nowhere is this dependence more acute than in the Arctic, a region where extreme conditions and sparse terrestrial infrastructure make space systems indispensable for both civilian and military activity. Ground stations in the Arctic provide strategic locations for satellite control and data transmission, supporting command-and-control, unmanned intelligence, surveillance, and reconnaissance (ISR) missions, and connectivity for deployed forces.[i] Yet, this reliance also exposes the Arctic to the risks of gray zone space warfare: hostile actions below the threshold of armed conflict, including electronic interference, cyber attacks, and the weaponization of dual-use technologies. **Governance structures that regulate space activities play a crucial role in shaping how such threats impact Arctic security and stability**.

GRAY ZONE WARFARE IN SPACE

Gray zone warfare is typically associated with ambiguity and involves actions that blur the line between peace and open conflict. In the space domain, this often involves non-kinetic activities: jamming and spoofing of satellite signals, cyber operations against ground stations, information warfare, or the use of directed energy to temporarily disable sensors.[ii] These actions exploit vulnerabilities without crossing the threshold of an "armed attack" as defined in international law, complicating attribution and response. As space-based systems increasingly support Arctic operations, such gray zone tactics directly threaten the reliability of communications, ISR, and navigation critical to the region's militaries, industries, and communities. These vulnerabilities in Arctic space operations highlight the urgent need to examine the existing legal and regulatory frameworks that govern space activities and their capacity to address gray zone threats.

SPACE GOVERNANCE FRAMEWORKS

The legal foundation for space governance is the **1967 Outer Space Treaty (OST)**, which, along with subsequent agreements such as the Rescue Agreement, Registration Convention, and Liability Convention, establishes the principles of state responsibility, peaceful use, and prohibition of weapons of mass destruction in orbit.[iii] However, the OST leaves key terms undefined: "peaceful purposes" is vague, Article IV restricts only nuclear and weapons of mass destruction (WMD) deployments, and no vertical boundary between airspace and outer space has been codified. The absence of a defined airspace-space boundary creates jurisdictional confusion as technology increasingly spans both domains, with different stakeholders holding conflicting preferences: militaries fear altitude restrictions on surveillance operations, commercial operators seek regulatory flexibility for suborbital activities, and developing nations worry that fixed boundaries could worsen inequitable access to space.[iv]

Recent developments, such as the April 2024 UN Security Council resolution affirming OST obligations,[v] demonstrate renewed attention to space security, but gaps remain. Governance structures are ill-suited to address gray zone activities: jamming, cyber intrusions, or dual-use technology weaponization fall into legal ambiguity.

GOVERNANCE GAPS AND CHALLENGES

1. **Attribution and Visibility**: Gray zone activities thrive on deniability. Improving space situational awareness (SSA) and transparency mechanisms, such as prenotification, enhanced registration, and operator communication, could help illuminate harmful actions.[vi]
2. **Dual-Use and Commercial Involvement**: The prevalence of dual-use technology complicates governance. Commercial satellites provide global internet and Arctic connectivity but can also be leveraged for military advantage. This raises questions of accountability when private firms are targeted or implicated in conflict.[vii] States remain legally responsible for all activities under their jurisdiction, including commercial operators, yet there is little clarity on liability if these actors are drawn into conflict.
3. **Legal Ambiguities**: The undefined boundary between airspace and outer space complicates sovereignty and jurisdiction. The OST suffers from vague terminology, leaving fundamental concepts like "due regard" and "peaceful use" undefined despite broad agreement on their importance, while maintaining the principle that states retain jurisdiction over their space activities without claiming sovereignty over space itself. This is compounded by siloed efforts, with little integration between space and cyber governance despite the significant overlap.[viii]
4. **Norm-Building Efforts**: UN initiatives, including the Open-Ended Working Group (OEWG), seek to establish norms of responsible behavior, but consensus is slow.

IMPLICATIONS FOR THE ARCTIC

Governance shortcomings have direct consequences for Arctic security:

- **Strategic Vulnerability**: Reliance on satellites for Arctic communications and ISR makes ground stations and orbital assets attractive targets for gray zone operations. Disruptions could undermine regional deterrence and crisis management.
- **Risk of Escalation**: Without clear governance, ambiguous attacks may provoke disproportionate responses, heightening the risk of militarization and conflict in the Arctic.
- **Civilian Impacts**: Local communities, shipping industries, and scientific research depend on satellite services for navigation, internet, and climate monitoring. Gray zone interference could have far-reaching humanitarian and environmental effects.[ix]
- **Great Power Competition**: China, Russia, and non-Arctic states increasingly view the Arctic as a strategic frontier. Exploiting governance gaps in space could offer them a low-cost means of exerting pressure in the region.

RECOMMENDATIONS

Improving the governance of gray zone space warfare requires a multi-pronged approach:

1) **Transparency and Space Situational Awareness**: Enhance data sharing, monitoring, and communication mechanisms to reduce ambiguity.
2) **Integrated Governance**: Break down silos between space and cyber regulation; connect Arctic governance forums, such as the Arctic Council, with space law initiatives.
    a) As new institutions such as Space Commands emerge, evolving cyber threat landscapes may expose critical gaps in mandates and coordination unless cyberdefense and cybersecurity are embedded from inception.[x] The 2024 "Minimum Requirements for Space System Cybersecurity" framework represents a promising step toward establishing unified, mission-specific standards that can guide more coherent, cross-domain governance.[xi]
3) **Clarifying State Accountability**: Establish clearer rules for how states are responsible for commercial actors, including mechanisms for liability and protection of civilian infrastructure.
4) **Confidence-Building Measures**: Promote norms of behavior, information exchange, and direct communication channels among Arctic and spacefaring nations.
    a) Protect strategically important space assets through binding or non-binding agreements, potentially beginning with diplomatic dialogue.
    b) Develop shared definitions of critical space infrastructure to increase predictability and reduce escalation risks by clarifying how different nations prioritize and utilize space systems.
    c) Define particularly provocative or escalatory actions by considering their consequences, including debris generation, radiation effects, duration, and cross-border impacts on other nations.
    d) Strengthen civilian space service resilience through measures like those outlined in the EU's 2023 strategy: building space autonomy, cataloging essential systems, mapping supply chains, and creating coordinated emergency response protocols.[xii]

CONCLUSION

The governance of gray zone space warfare is inseparable from the future of the Arctic. As militaries, industries, and communities in the High North grow more reliant on space-based systems, gaps in international law and governance expose the region to heightened risks. While the Outer Space Treaty provides a legal foundation, it lacks the precision to address non-kinetic gray zone activities, dual-use dilemmas, and the growing role of commercial actors. Strengthening governance through improved visibility, norm-building, and clarifying legalities and accountabilities is critical to ensuring that the Arctic remains a domain of stability rather than a testing ground for escalation.

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] Michael E. Lynch. (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

[ii] Steer, C. (n.d.). *International Humanitarian Law in the "Grey Zone" of Space and Cyber*. Centre for International Governance Innovation. Retrieved September 10, 2025, from https://www.cigionline.org/articles/international-humanitarian-law-in-the-grey-zone-of-space-and-cyber/

[iii] Santos, E. A. (2025, July 4). *International Law and the Regulation of Outer Space*. Diplomacy and Law. https://www.diplomacyandlaw.com/post/international-law-and-the-regulation-of-outer-space; West, J., & Miller, J. (2023). *Clearing the fog: The grey zones of space governance*. *287*. https://www.cigionline.org/articles/international-humanitarian-law-in-the-grey-zone-of-space-and-cyber/

[iv] Santos, E. A. (2025, July 4). *International Law and the Regulation of Outer Space*. Diplomacy and Law. https://www.diplomacyandlaw.com/post/international-law-and-the-regulation-of-outer-space

[v] Connolly, R. (2024, July 19). *Rising tensions over outer space – a new diplomatic hot zone | Lowy Institute*. https://www.lowyinstitute.org/the-interpreter/rising-tensions-over-outer-space-new-diplomatic-hot-zone

[vi] West, J., & Doucet, G. (2022). *A Security Regime for Outer Space: Lessons from Arms Control*. Project Ploughshares. https://ploughshares.ca/wp-content/uploads/2025/05/ArmsControlLessons_OuterSpace_10.22.pdf

[vii] Raju, N. (2024). *Parameters to Assess Escalation Risks in Space*. Stockholm International Peace Research Institute. https://doi.org/10.55163/EDTC6801; Hitchens, T. (2022, September 1). To protect and maybe defend: NRO, SPACECOM ponder commercial satellite defense options. *Breaking Defense*. https://breakingdefense.com/2022/09/to-protect-and-maybe-defend-nro-spacecom-ponder-commercial-satellite-defense-options/

[viii] Aganaba, A. S., Timiebi. (2023, January 29). Formulating, Interpreting and Applying International Law in Space. Centre for International Governance Innovation. https://www.cigionline.org/articles/formulating-interpreting-and-applying-international-law-in-space/

[ix] Raju, N. (2024). Parameters to Assess Escalation Risks in Space. Stockholm International Peace Research Institute. https://doi.org/10.55163/EDTC6801

[x] Poirier, C. (2025). Establishing a governance for cyber operations in outer space: Exploring challenges faced by space and cyber commands. *Acta Astronautica*, *237*, 236–242. https://doi.org/10.1016/j.actaastro.2025.08.048

[xi] Casaril, F., & Galletta, L. (2025). Space cybersecurity governance: Assessing policies and frameworks in view of the future European space legislation. *Journal of Cybersecurity*, *11*(1), tyaf013. https://doi.org/10.1093/cybsec/tyaf013

[xii] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, European Union space strategy for security and defence, Joint Communication to the European Parliament and the Council, JOIN(2023)9, 10 Mar. 2023.