Falco, Gregory; Boschetti, Nicolò; Nikas, Ioannis

Working Paper

Undercover infrastructure: Dual-use arctic satellite ground stations

CIGI Papers, No. 291

Provided in Cooperation with:
Centre for International Governance Innovation (CIGI), Waterloo, Ontario

Suggested Citation: Falco, Gregory; Boschetti, Nicolò; Nikas, Ioannis (2024) : Undercover infrastructure: Dual-use arctic satellite ground stations, CIGI Papers, No. 291, Centre for International Governance Innovation (CIGI), Waterloo, ON, Canada

This Version is available at:
https://hdl.handle.net/10419/299988

Centre for International
Governance Innovation

CIGI Papers No. 291 — April 2024

Undercover Infrastructure
Dual-Use Arctic Satellite Ground Stations

Gregory Falco, Nicolò Boschetti and Ioannis Nikas

Centre for International
Governance Innovation

CIGI Papers No. 291 — April 2024

Undercover Infrastructure
Dual-Use Arctic Satellite Ground Stations

Gregory Falco, Nicolò Boschetti and Ioannis Nikas

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Susan Bubak
Publications Editor Lynn Schellenberg
Graphic Designer Abhilasha Dewan

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

About the Authors

Gregory Falco has been at the forefront of space system and critical infrastructure security in both industry and academia for the past decade. He is an assistant professor at Cornell University's Sibley School of Mechanical and Aerospace Engineering and the Systems Engineering Program. He is the director of the Aerospace ADVERSARY (Autonomy, Defense and Vulnerability Exploitation for Resilient, Secure and Assured Risk/Yield) Lab at Cornell University. The ADVERSARY Lab designs and develops future aerospace technology enabling secure, resilient and assured autonomous space infrastructure. He is leading the effort to develop an international technical standard for space cybersecurity as the founding chair of the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA) Space System Cybersecurity Working Group. His research paper titled "Cybersecurity Principles for Space Systems" was highly influential in the development of the US government's Space Policy Directive-5, which shared the same title.

Gregory was the former co-founder and CEO of the blockchain-based industrial control security company NeuroMesh Inc., which was acquired in 2022. He has appeared on the *Forbes* "30 Under 30" list for his inventions and contributions to critical infrastructure cybersecurity, is a Fulbright Scholar, was named a Defense Advanced Research Projects Agency (DARPA) Riser and received DARPA's Young Faculty Award for work on building a zero-trust marketplace ecosystem for space systems. Gregory serves as a member of the US Department of Homeland Security's Space Systems Critical Infrastructure Working Group and has been awarded contracts related to space system security for the Air Force Research Laboratory, US Space Force, the National Aeronautics and Space Administration (NASA) and DARPA. He is also a research affiliate at the Massachusetts Institute of Technology (MIT) Computer Science & Artificial Intelligence Laboratory. Gregory completed his Ph.D. at MIT, his master's degree at Columbia University and his bachelor's degree at Cornell University.

Nicolò Boschetti is a Ph.D. student in aerospace engineering at Cornell University and is an assistant researcher at the Aerospace ADVERSARY Lab at Cornell University's Sibley School of Mechanical and Aerospace Engineering. He received his B.A. in international and diplomatic sciences from the University of Bologna, his M.A. in politics and economics of Eurasia from the Moscow State Institute of International Relations, and his M.S. in systems engineering from Johns Hopkins University. He is the IEEE SA Space System Cybersecurity Working Group secretary. His research focuses on the security and resiliency of space-based networks, with several research papers focusing on satellite ground stations and ground stations as a service.

Ioannis (Yanni) Nikas is an undergraduate student in mechanical engineering at Johns Hopkins University. His research is at the intersection of technology, security and foreign policy.

Acronyms and Abbreviations

DoD	Department of Defense
EGNOS	European Geostationary Navigation Overlay Service
ESA	European Space Agency
GNSS	global navigation satellite system
KSAT	Kongsberg Satellite Services
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NWS	North Warning System
OSCE	Organization for Security and Co-operation in Europe
OST	Outer Space Treaty
SSC	Swedish Space Corporation

Executive Summary

The space sector has undergone a transformation, with private companies now playing a pivotal role in what has been termed "the new space race." This shift has not only led to an increase in space assets and infrastructure but has also brought increased attention to the military use of commercial infrastructure, or dual-use technology. Dual-use technologies, which serve both civilian and military purposes without significant modifications, have a long history, with space technologies being among the most notable examples. The current focus is on the strategic importance of satellite ground stations in the Arctic, given their dual-use capabilities and the complex security and legal implications they entail.

The concept of dual-use technologies in space is not new but has evolved to include a wide range of applications, from satellite communications to Earth observation. These technologies, while beneficial for civilian purposes, also pose significant security risks and regulatory challenges, especially when they become targets in geopolitical conflicts. The Arctic region, with its strategic importance for ground station placement, emerges as a critical area for examining the implications of dual-use space technology. This paper discusses the militarization of space, the role of dual-use technologies in this process and the security profile of satellite ground stations in the Arctic.

Ground stations are integral to space operations, providing the necessary link between space assets and their users on Earth. The Arctic's emergence as a key location for these stations is driven by its geographical advantages for satellite communication, especially in polar orbits. However, this also makes the Arctic a focal point of international power competition, with states seeking to optimize their interests through strategic placement and utilization of ground stations. The dual-use nature of these infrastructures further complicates the security landscape, making them potential targets in conflict scenarios.

The governance of dual-use space technologies, particularly in the Arctic, is fraught with challenges. Existing legal frameworks and international treaties, such as the Outer Space Treaty (OST),[1] provide limited guidance on the regulation of ground segments. The paper discusses the legal implications of dual-use designations, the impact of recent geopolitical events on Arctic governance, and the need for innovative governance constructs to ensure stability and security in the region.

The paper examines the interests of various nation-states in the Arctic, highlighting the strategic motivations behind the deployment of satellite ground stations and the pursuit of satellite-based internet connectivity. It explores the dynamics of international relations in the Arctic, considering the roles of major powers such as the United States, Russia and China, as well as the implications of the involvement of the North Atlantic Treaty Organization (NATO) and the challenges posed by the evolving geopolitical landscape.

The paper concludes with a call for multilateral action to address the governance and security challenges of dual-use space technologies in the Arctic. Recommendations include enhancing regulatory oversight, promoting international cooperation and adopting management practices that ensure the resilience of space-ground infrastructures against potential disruptions. It underscores the importance of dialogue among international actors, the development of updated legal regimes, and the implementation of policy measures that safeguard both civilian and military uses of space technologies. The strategic significance of the Arctic in the space sector demands concerted efforts to ensure the security and stability of dual-use infrastructures, with implications for global security and governance.

Introduction

New space, characterized by emergent commercial space capabilities, defines the current era of the space race. If nation-states were the main actors in space activities during the Cold War until the mid-2000s, private companies are now quickly

1 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967 (entered into force 10 October 1967), online: <www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html>.

assuming dominance over this complex sector. This trend has led to consistent growth of space assets and infrastructure in orbit and on the ground, specifically in the satellite communications domain. Without antennas strategically installed across the planet, satellites would be unable to relay their data to ground operators. In particular, the Arctic has emerged as a region of strategic importance for placing ground stations since the dawn of the twenty-first century.

As a function of the commercial sector's new capabilities, civil governments and defence agencies have progressively outsourced space operations to private enterprise. This occurs in both civilian activities such as observation of Earth and its atmospheric phenomena, but especially in intelligence, connectivity and tactical support to war fighters. Therefore, commercial satellite networks increasingly see civil and military data coexist within them, with notable consequences for their regulatory status and security. At the boundary between commercial and military, these infrastructures are classified as "dual use." Dual-use systems represent a class of assets that can simultaneously engage in civil and defence activities. Ground stations are often employed for dual-use capacity given their capital-intensive nature and ability to be simultaneously commissioned for multiple missions. Such systems present considerable governance challenges given their ambiguity, especially in contested domains or conflict scenarios.

Starting with an analysis of dual-use space technology and its role in the militarization and weaponization of space, this paper will discuss the particularly complex security profile of satellite ground stations in the Arctic. This will be followed by an analysis of the legal implications of their dual use, interpreted through a lens of competition between powers in the Arctic region. Existing attempts at multilateral Arctic governance and their weakening structures, resulting from the growing international tensions arising from the invasion of Ukraine by the Russian Federation in February 2022, will be discussed in the context of dual-use infrastructure governance. Finally, innovative governance constructs are required to foster stability in the region, as the authors suggest through policy recommendations.

Dual-Use Technologies

What Are Dual-Use Technologies?

Dual-use technologies and infrastructure can serve civilian and military users without fundamental changes to the technology (Wolf 2012). Dual-use technologies are not new. For example, the advances in chemistry at the end of the nineteenth century greatly benefited peacetime economies but also caused millions of deaths in the trenches of the First World War. After the Second World War, space technologies represented one of the most striking examples of dual-use technologies. The rockets that brought Sputnik into space in 1957 and Yuri Gagarin in 1961 were nothing more than intercontinental ballistic missiles adapted to orbital flight.

One may question how space technology can be dual use without space weaponization and militarization. Despite efforts by the United Nations and the existence of international treaties that explicitly prohibit the use of space and celestial bodies for military purposes, space has become a warfighting domain. The *corpus juris spatialis*, in fact, imposes stringent limits almost exclusively on nuclear weapons but does not provide clear limits for the use of conventional weapons from, to, and in space. Thus, the militarization and weaponization of space has evolved.[2]

The evolution of the space sector, especially concerning the privatization mentioned above and the outsourcing of various services, has led to the further spread of the dual-use nature of space technologies. This trend is now visible in all mission segments, from the evident space segment to the ground and user segments. For example, among the most ubiquitous dual-use space technologies is the American GPS. This global navigation satellite system (GNSS) consists of a constellation of satellites in geostationary

2 "Space militarization" refers to the degree to which space technologies are used to support military activities on Earth. As evidenced by satellite constellations currently in orbit and the priorities of the various military space programs, space is already militarized. After all, the same geolocation systems, now ubiquitous in the lives and daily activities of civilians, arose from military needs and are still essential for the use of missiles or other technologies such as unmanned aerial vehicles. "Space weaponization" refers to the active use of weapons specifically designed to operate against space systems from the ground, against space targets from space, or against ground targets from space. This concept, therefore, presupposes an enlargement of the dimension of war.

orbit that, through specific radio frequencies, connects with terminals on the ground or in the sky and triangulates their position, also providing information about the coordinates, speed, altitude and several other parameters. It was developed by the US Department of Defense (DoD) as a military system for the tactical support of troops and improving ammunition guidance systems. The First Gulf War, fought by a US-led international coalition against the Iraqi government following the invasion of Kuwait, heavily relied on this system. Operation Desert Storm allowed the US military to use GPS in the field and satellite communications and information to manoeuvre missile systems against enemy targets; in fact, it was described as the "First Space War." Thereafter, the importance of space-based technologies became increasingly evident. The American military's satellite constellations were even more essential in NATO's 1999 bombing campaigns of Yugoslavia and more so in the Second Gulf War in 2003 and the consequent conflict in Afghanistan. These technologies proved to be not only an adjunct for the control of troops and enemy movements through GNSS and remote sensing systems but also for the use of high-precision ammunition. In the First Gulf War, about eight percent of ammunition was precision-guided; in the second, this number exceeded 60 percent; and in the 2014 operations in Syria, it exceeded 96 percent. GPS, however, has also been made accessible to private and civil users, segmenting the network and allowing the architecture to provide geolocation to both the most straightforward car-sharing systems and the most complex military assets on the battlefield. This system is still controlled and managed by American military forces, which segment the frequencies of use, differentiate the level of precision according to the users, and limit their commercial and civil use in case of military needs. All these aspects provide a clear description of a dual-use space system.

Why Does the Dual-Use Designation Matter?

Dual-use systems present interesting policy and regulatory questions, given that they often exist in a grey governance zone. They are not owned by defence entities but can be used for defence purposes intermittently. Therefore, it is unclear what protections they afford or if their militarization is legal under certain environments. Dual-use assets benefit from plausible deniability, given that they could be used for multiple purposes at a given time. As commercial or civil assets, dual-use infrastructures are generally more exposed to threats than military installations. Further, the disruption of dual-use assets has cascading consequences for civil parties, which has ethical consequences.

An interesting example of the collateral damage that attacks against dual-use space infrastructure yield on civilian users is the Russian cyberattack against Viasat that happened in February 2022. At the dawn of the Russian invasion of Ukraine, a cyberattack attributed by the United States and other countries to Russia targeted Viasat's KA-SAT, a commercial satellite communications network. KA-SAT is a high-throughput satellite optimized for consumer broadband services and users located beyond the range of high-speed terrestrial networks. It fully operates in Ka-band frequencies, suitable for high-throughput satellite communications, and provides internet broadband connectivity across Europe and the Mediterranean Basin. Viasat's user base varied widely, from the Ukrainian military forces to German wind energy farms that required access to remote infrastructure operations and private households — the epitome of a simultaneous dual-use capability (Boschetti, Gordon and Falco 2022). The attack ultimately disabled a variety of Viasat users' terminals, both military and civilian, even outside the Ukrainian territory. The repercussions on European infrastructure and civilian customers raised the question of whether this commercial satellite broadband provider was a legitimate target.

The dilemma of targeting a dual-use asset continued as SpaceX's Starlink was deployed in Ukraine to provide a rapid KA-SAT replacement for the Ukrainian army. Starlink's dual-use nature is similar to that of KA-SAT; it allowed non-governmental organizations to continue working even in a war zone while it also provided the Ukrainian military the ability to operate drones and other weapon systems. Thus, Starlink has become a critical asset for Ukraine. Starlink similarly presents a regulatory quandary. SpaceX's Starlink was never intended to be weaponized, and SpaceX's president Gwynne Shotwell noted that Starlink was never meant to augment offensive capabilities (Foust 2023). Despite this public statement, the United States has covered expenses for shipping several terminals to Ukraine to foster its war-fighting capabilities. As a result, the distribution of a dual-use asset, such as Starlink, has been deployed by

the joint support of state and commercial actors into the war theatre, creating ambiguity about the context of its designation for governance purposes.

The prevalence of dual-use technologies has prompted calls to increase regulation and protection of dual-use assets. However, since such infrastructure straddles civilian and defence operations, applying existing legal and regulatory frameworks is imperfect. Identifying the relevant legal treatises, governing bodies and export control regimes for these technologies is crucial to evaluate options for their future governance.

The Ground Segment and Space Power Competition

What Is a Ground Station?

Space operations require a complex ecosystem of components to seamlessly interact for a successful mission. A space system consists of four segments: space, link, ground and user.

The space segment is focused on aspects related to all objects located in space and capable of receiving and/or transmitting information, including satellite payloads such as communication devices, imaging systems, orbital positioning systems such as GPS and Galileo, and on-board computer systems. The space segment includes satellites, spacecraft, probes, space stations, associated on-board systems, subsystems, software and related interfaces.

The link segment is responsible for the communication links between the various elements of the space mission, including ground-to-space, intersatellite crosslinks, optical communications, uplinks and downlinks.

The ground segment pertains to all ground-based elements involved in space missions, which include command-and-control systems, data-processing facilities, and network infrastructure such as fibre-optic cables and routers. This segment includes ground stations; control centres; telemetry, tracking and command stations; data-processing and storage centres; and launch infrastructures. Ground stations are a subcomponent of the ground segment, and are responsible for transmitting data to and receiving it from the spacecraft. These stations are composed of transmitter and receiver hardware that collects and communicates data via electromagnetic waves (NASA 2024).

The user segment is concerned with end-user elements that interact with or benefit from the space system, which includes end-user devices such as satellite phones and tablets, ground-based individual communication terminals, and software applications for navigation and remote sensing. This includes user terminals, devices, networks, and the data and services they access, spanning from GPS devices to satellite communication-enabled equipment.

While this paper focuses on the dual-use nature of the ground segment, the notion of dual-use operations for space systems can be extended to each of these segments.

Why Do Ground Stations Matter in the Context of Space Power Competition?

Defensive neo-realism is particularly suited to evaluate the current state of power competition with respect to space-ground systems, given the space domain's competitiveness and lack of regulation. Given that the Arctic is at the centre of power interest in a time of resurgent international tensions, space-ground infrastructure is well suited for serving as a force multiplier of nation-state capability (Boschetti et al. 2022).

The lack of a central governing body with significant control over state behaviour leads to each state pursuing actions that optimize its interests. While there is no formal hierarchy among states, an implicit hierarchy arises from the varying capabilities they possess. Thus, states share common needs but differ significantly in their capacities to fulfill those needs (Mearsheimer 1994). The distribution of capabilities determines the ranking of states in terms of power. This structural arrangement limits cooperation among states due to concerns about other states' relative gains and potential dependence. The pursuit of enhancing relative power, driven by each state's desires and capabilities, mutually constrains their actions, resulting in a "balance of power." This balance shapes international relations, either encouraging or impeding collaboration among nations. This equilibrium among

states is the fundamental behavioural pattern within the international system, observable in both bipolar and multipolar systems.

Considering the potential cascading consequences of kinetic destruction on space-based assets, nation-states perceive electronic and cyberattacks on ground-based infrastructure as effective means to undermine the capabilities of adversaries' space assets. Moreover, remote ground stations could be particularly vulnerable targets due to their isolation, making them easier to disrupt or incapacitate through electronic and cyber means.

Why Does the Arctic Matter?

The Arctic region, defined by the Arctic Circle at 66° N, is a complex expanse marked by varying borders, shifting ice and geopolitical influences. Its dynamic nature encompasses diverse features such as the Arctic Ocean and spans the northern territories of countries such as Canada, Greenland, Iceland, Norway, Sweden, Finland, Russia and the United States. With a population of more than four million, the Arctic is undergoing continuous transformation. The history of Arctic competition, particularly in the military realm, is not new. During the Cold War, the Arctic acted as both a buffer and a battleground between the Soviet Union and the Western bloc. Its significance lay in serving as the shortest route for intercontinental ballistic missiles, prompting the establishment of early-warning radar systems on both sides of the Arctic Ocean (Hilde 2013).

The Eurasian Arctic has recently experienced a significant shift in its regional security landscape due to Russia's military intervention in Ukraine in February 2022. This intervention has led to Sweden and Finland, historically neutral, aligning themselves with NATO. This decision, in turn, grants Russia a new 1,300-kilometre land border with NATO, altering the geopolitical dynamics. Coastal states bordering the Baltic Sea, now NATO members, dominate the area, further isolating Russia's Kaliningrad exclave. This strategic realignment of Sweden and Finland has broader implications, extending to the Arctic Council — the primary platform for international collaboration in the High North (Boschetti et al. 2022). While the majority of its member states are part of NATO, Russia remains an outlier, which could strain diplomatic relations further amid existing Western sanctions. This shift could potentially create space for China, which has been seeking to enhance its economic and political influence in the region. China's interest in utilizing emerging near-polar maritime routes, facilitated by ice melt, aligns with its Belt and Road Initiative, including the envisaged Polar Silk Road (Brady 2017). Against the backdrop of deteriorating East-West diplomatic relations and escalating rearmament, initiatives such as the enhanced satellite connectivity projects by the United States and Europe gain strategic and military importance in the Arctic. As the Arctic landscape continues to evolve, these endeavours assume a crucial role, reflecting the broader geopolitical shifts and the evolving security challenges in the region.

Today, military competition in the region continues, but the Arctic offers new commercial business potential as well. For example, the melting of Arctic ice shelves and the subsequent emergence of new trans-Arctic shipping routes have made the region more commercially valuable. Trans-Arctic routes could offer shorter transit times for ships travelling between North Atlantic and North Pacific ports. This possibility is already being explored. China's state-owned China Ocean Shipping Company Limited completed the first transit of the Northeast Passage in 2013, proving the viability of this trading route and the competitive advantage it could provide. Competition is not solely limited to the global shipping industry. Fishing and natural resource extraction are also industries that concern Arctic operations. Additionally, the Arctic is a reservoir of natural resources, such as nickel, copper, zinc, silver, gold, coal, uranium and rare earth elements.

Nation-State Ground Station Interests in the Arctic

The rising number of satellites, especially in polar orbits, has fostered the installation of satellite ground stations in the polar regions. A polar orbit is where satellites pass over the Earth's poles, which is particularly useful for Earth-observation or surveillance satellites because of their relatively low altitude (ranging from 200 to 1,000 kilometres) and because they can observe the Earth's entire surface, passing the poles multiple times a day.

Molniya and Tundra orbital regimes, particularly suited for high-latitude operations, also benefit from an extended polar infrastructure. The cost of infrastructure development in the Arctic is high given its remoteness; therefore, it is desirable to spread the cost of ground stations in this region across multiple stakeholders who may make use of its service. The new paradigm of ground stations as a service has enabled users of ground stations to purchase time slots for satellite communications on shared infrastructure, typically owned and operated by a commercial entity. The introduction of such commercial entities, which have an expanding defence customer portfolio, has increased the complexity of the Arctic space security landscape and led to an increased number of dual-use ground stations (Boschetti et al. 2022).

Another rapidly expanding sector of the Arctic space economy is satellite-based internet connectivity. Companies such as SpaceX's Starlink and OneWeb have deployed satellites in polar orbits, with OneWeb already operating at least 14 antennas at Svalbard, offering internet connectivity in the region (Erwin 2021). As commercial activities and remote settlements grow in the Arctic, the significance of such infrastructures is expected to increase, necessitating additional supporting communication infrastructure. Moreover, these satellite communications have strategic importance. For instance, OneWeb's expansion in the Arctic is funded by the DoD under the Air Force's Defense Experimentation Using Commercial Space Internet program (OneWeb 2021). This is one such example of dual-use infrastructure in the region. Another provider of satellite internet connectivity is Space Norway, with its Arctic Satellite Broadband Mission satellites (Erwin 2022). Scheduled to launch in mid-2024, the two satellites, built by Northrop Grumman, will have highly elliptical orbits over the Arctic and accommodate payloads from other partners. The presence of Enhanced Polar System-Recapitalization payloads on board will provide high-frequency connections to US forces in the Arctic region. Additionally, payloads from Inmarsat and the Norwegian Armed Forces will be part of the satellite mission.

Finally, in relation specifically to the European Arctic, the High North is gaining importance for the GNSS. As naval and aerial traffic is expected to increase in the area, investments in positioning, navigation and timing, and automated identification systems are becoming crucial. The European Union is setting up ground stations for its satellite-based augmentation system, known as the European Geostationary Navigation Overlay Service (EGNOS), from Iceland to Jan Mayen and the Svalbard islands.[3] EGNOS will greatly enhance navigation services for aviation and maritime users.

Moreover, the region is witnessing the rise of satellite launches in polar, Molniya and other typologies of high-eccentricity orbits, leading to the proliferation of launch sites. The Esrange Space Center in northern Sweden is being upgraded to accommodate space rocket launches and bolster the capabilities of the European Space Agency (ESA) and the Swedish Space Corporation (SSC). Iceland has already served as a testing ground for the British Skyrora company, generating increased interest in launches from its territory. Additionally, Norway boasts two launch sites: one in Andøya and the other in the Svalbard islands, with the latter being particularly advantageous for scientific purposes due to its latitude (Boschetti et al. 2022).

The Russian Federation

More than half of the Arctic coastline is Russian territory. Consequently, the only Arctic Russian permanent infrastructures outside the federation's territory are in the Svalbard islands. In addition, the Russian space sector is much less privatized than in other countries, leading to a lower presence of dual-use services. In the Arctic context, however, it should be noted that in recent years, Russia has particularly criticized the space activities of Kongsberg Satellite Services (KSAT) and other operators concerning the satellite infrastructure of the Svalbard Satellite Station (SvalSat). It has been repeatedly pointed out that Russia considers dual-use space activities in the Svalbard islands as a violation of the Svalbard Treaty, thus raising doubts about Norway's and NATO's compliance with the treaty.[4] The Russian Svalbard settlement of Barentsburg, currently hosting satellite antennas, was considered by the Roscosmos State Corporation for Space Activities (Roscosmos) in 2022 as a possible site for the establishment of a near-space tracking station (Nilsen 2023). Currently, the status of the project is unknown, but this would be the first case of Russian dual-use space infrastructure outside its territory.

3 See www.euspa.europa.eu/european-space/egnos/what-egnos.

4 See www.csis.org/analysis/arctic-geopolitics-svalbard-archipelago.

The Russian Federation has recently significantly increased its focus on the Arctic, resulting in several revisions of national policy and military strategy. Substantial military investments are under way to safeguard the Northern Sea Route along the northern coasts of Russia. Abandoned Soviet-era military bases have been renovated and reactivated, while the Northern Military District was established to strengthen electronic warfare capabilities in the Kola Peninsula and secure naval supremacy. These developments reflect the resurgence of the Cold War strategic concepts aimed at creating a protected area encompassing Russian territories in the Barents Sea, Svalbard and the Scandinavian Peninsula. A prominent example of this investment is the Nagurskoye base on Alexandra Land in the Barents Sea, equipped with electronic defence, missiles and radar to strengthen the Northern Military District and possibly interfere with foreign satellite ground stations in the region (Boschetti et al. 2022).

China

China's interest in the Arctic has attracted global attention in recent years (Doshi, Dale-Huang and Zhang 2021). Like other nation-states, China is attracted to the Arctic for prospective strategic military and commercial benefits (Brady 2017). China's ground stations in the Arctic are all labelled as scientific outposts for polar and atmospheric research, but China's Arctic strategy and the wide deployment of technology to the Arctic may also suggest dual-use operations. China's first Arctic research centre was established at the Ny-Ålesund Yellow River Station in 2004 in the Svalbard islands. This station is mainly used for scientific purposes, but it also collects data on atmospheric physics and geodetic observations that can find military applications in surveillance and field support domains. This first Chinese step in the European Arctic was followed by the China-Iceland Arctic Science Observatory in Kárhóll in 2016 and the China Remote Sensing Satellite North Polar Ground Station in Kiruna, Sweden, in 2017. Additionally, the Greenland Satellite Ground Station was built in Kangerlussuaq, Greenland, in the same year. The Greenland Satellite Ground Station is also part of a Chinese research effort to study climate change, but its instrumentation reveals various satellite ground terminals that are identical to the other stations previously mentioned. Therefore, China's ground station activity in the Arctic, publicly labelled as scientific, has the possibility of being integrated (if not already) into military operations (Boschetti et al. 2022). Moreover, China's intent of achieving its strategic goals in the region makes these dual-use ground stations relevant to the security and governance discussion for the region.

The United States

As a polar nation and global superpower, the United States is a significant player in the Arctic region. The United States National Strategy for the Arctic Region is a clear indicator of the United States' goals in the region. These include increased security, environmental protection, climate change mitigation, and international cooperation and governance (The White House 2022). The United States has military forces in the Arctic and conducts exercises with allies and NATO to increase interoperability. Therefore, the United States' military presence and intent in the region are unquestionable. This makes dual-use ground stations operated by the United States a point of interest.

The United States has partnered with commercial provider OneWeb for satellite connectivity services. OneWeb has deployed satellites in polar orbit for high-speed internet connectivity that are used by the United States at Pituffik Space Base in Greenland. Additionally, the SvalSat ground station in Svalbard, Norway, is used by the United States Coast Guard for satellite telemetry and science data specifically for the Landsat 8 and 9 operations (Earth Resources Observation and Science Center 2020). These missions aim to provide geographic imaging data that could be used for intelligence purposes. Given this partnership, it is logical that other OneWeb stations engaging Arctic ground terminals could equally be integrated into the United States' defence programs. Therefore, it is plausible that the OneWeb station in Nuuk, Greenland, could easily be absorbed into the DoD network. This array of ground station capabilities makes it possible for the United States to conduct science missions while simultaneously supporting military operations and opening the door for the future military use of the stations.

Canada

Canada is intensifying its defence and surveillance efforts in the Arctic by leveraging space capabilities and new technologies. The 2022 federal budget allocates $252 million for modernizing the joint Canada-US North Warning System (NWS), including

research into long-range communications and over-the-horizon radar systems (Pugliese 2022). These investments are driven by concerns over Russian activities in the Arctic, prompted by the Ukraine invasion. Canada aims to enhance its defences in collaboration with the United States and prioritize the modernization of the North American Aerospace Defense Command. Key to this strategy is upgrading the NWS, a network of air defence radar sites constructed in the late 1980s (DoD 2021). Canada and the United States also prioritize situational awareness, aiming to replace the NWS with advanced technological solutions, including next-generation radar systems, seafloor and space sensors, and resilient communications. In the space sector, Canada's initiatives include the Enhanced Satellite Communication Project – Polar, which focuses on reliable Arctic communications. Another project, the Defence Enhanced Surveillance from Space Project, aims to upgrade surveillance capabilities in the Arctic and maritime areas (DoD 2021). Canada's comprehensive approach seeks to fortify its defence posture in the Arctic, combining advanced space technology and collaborative efforts with allies to ensure effective monitoring and response capabilities.

Nordic Countries

The Nordic countries of Norway, Sweden, Finland and Iceland hold significant roles in the competitive landscape of the Arctic, with each contributing distinctive strategic elements to the realm of space operations, particularly within the military domain. Norway stands out due to its expansive territories and active engagement in space endeavours. The Svalbard archipelago, housing several research stations, is a focal point of interest. KSAT, co-owned by the Norwegian government, operates vital ground stations across the archipelago, such as SvalSat, as well as stations such as Tromsø and Grimstad on the mainland.[5] These stations are integral to KSAT's worldwide network, enabling satellite connectivity for diverse tasks such as environmental monitoring, maritime surveillance and bolstering the ESA's Copernicus initiatives. Capitalizing on its NATO membership, Norway leverages its advanced space infrastructure for both domestic and allied military operations, thus reinforcing its strategic influence in the Arctic theatre. Sweden is another significant player in the Arctic, boasting an expansive network of ground infrastructure devoted to space operations. Spearheading this domain is the SSC, a state-owned entity catering to institutional and commercial clients. Key assets include the Esrange Space Center in Kiruna, Sweden, and the Stockholm Teleport Station in Ågesta.[6] While the immediate link between these facilities and military activities might be less overt, Sweden's anticipated NATO accession is expected to facilitate a deeper integration of its space infrastructure with alliance operations. This implies that while currently focused on commercial objectives, these ground stations hold the potential to pivot toward military applications, underlining Sweden's adaptability within an evolving security landscape. Finland and Iceland, while occasionally less prominent in this context, also contribute to the Nordic space narrative. Finland's strides in space operations are highlighted by projects such as the Finnish Meteorological Institute's space weather service PECASUS, Vaisala's instruments on NASA's Curiosity and Perseverance Mars rovers, and ICEYE's synthetic aperture radar constellation as highlighted by the New Space Economy program of Business Finland. In Iceland, the distinct environmental conditions offer research potential, although the nation's space presence remains relatively fledgling. Together, these Nordic countries encompass a spectrum of strategic approaches to space activities within the Arctic. Norway's robust military role contrasts with Sweden's potential for NATO-integrated endeavours. Finland and Iceland, although making progress, showcase the potential for further growth. As the dynamics of Arctic competition evolve, the space capabilities of these nations remain poised to shape the region's security landscape profoundly.

Arctic Ground Stations with Dual-Use Potential

Unified resources that explicitly and comprehensively document commercial and scientific ground stations are unavailable. Drawing from previous research by Nicolò Boschetti et al. (2022) in the mapping of commercial space infrastructure in the European Arctic and High

5 See www.ksat.no/ground-network-services/satellite-operation/.

6 See https://sscspace.com/about/the-company/.

North, open-source intelligence techniques to collect data have been used to provide a list of Arctic ground stations of interest. Such techniques included reviewing material from corporate, scientific and government websites, engaging open-source intelligence tools such as Shodan.io and conducting informational interviews with scientific researchers (who wished to remain anonymous) engaged in Arctic studies. The authors' research suggests that there are ground stations in the Arctic with dual-use potential, operated by a multitude of organizations, which pose security and regulatory challenges. Several of these ground stations are owned and operated by commercial entities, while others are owned and operated by universities or multinational scientific research consortiums. The geographical dispersion of Arctic ground stations is depicted in Figure 1, followed by a tabular description of each in Table 1.

Security Risks to Dual-Use Ground Station Infrastructure

Currently, matters relating to Arctic cooperation are principally focused on the region's environmental and, more broadly, human security. Several Indigenous communities inhabit remote areas presently endangered by the consequences of climate change and international confrontation. The dual-use nature of the space-ground infrastructure now active in the Arctic threatens the security of local populations. Satellite stations and related services such as broadband connectivity are particularly crucial in the case of search and rescue operations, assistance to remote settlements and the fight against the digital divide.

There are three primary risks to dual-use ground station infrastructure that are not explicitly considered acts of war under international treaties as subsequently described. These include cyber risks, electronic threats and the physical disruption of telecommunication lines.

Cyber Risks

Ground stations, especially those in remote regions that do not host 24/7 human operations, are generally internet-connected devices. As an industrial control system, their internet-connected nature presents cyber risks unique to this class of device. Industrial control systems generally contain embedded processors with limited computing resources, which results in their inability to host intrusion detection systems or other malware mitigation tools (Boschetti et al. 2023). Their relative ease of access and discoverability on search engines such as Shodan.io make them easy targets for attackers via a variety of tactics, techniques and procedures.

Electronic Threats

The radio frequency signals disseminated from and directed to ground stations are highly exposed, stationary targets for electromagnetic disruption. Such threats could take the form of jamming, spoofing or replay attacks. Software-defined radio technology advancements have considerably lowered the barrier to engage in such disruptive electronic activity. Given the directional nature of electromagnetic waves, electronic threats require proximity to the target. Such proximity operations could be easily noticeable in highly populated areas, whereas remote ground stations in the Arctic present increased opportunities for motivated adversaries to approach the target by land or sea and wage electronic disruption techniques against the ground asset.

Physical Disruption

The remote nature of ground stations and their connection to network infrastructure make them vulnerable to disruption by the physical severing of communication lines via undersea cable cutting. Such underwater activities are difficult to detect and then attribute, as demonstrated by the Nord Stream 2 natural gas pipeline explosion in 2022. Cutting telecommunication seabed cables could pose an effective means of isolating ground stations, thereby reducing their utility (Boschetti et al. 2022). An attack on a communication cable is distinctly different from a physical attack on the ground station itself, in which case aggression could be considered an act of war.

Figure 1: Arctic Ground Stations

Source: Google Maps, modified by the authors. See Table 1, opposite, for key to ground stations.

Regulation of Dual-Use Ground Stations in the Arctic

The regulatory regime surrounding space-ground infrastructure in the Arctic grapples with intricate challenges due to the dual-use nature of many assets and the absence of dedicated international treaties governing the region. The presence of dual-use ground stations introduces significant changes to the security landscape, intensifying tensions within an already competitive Arctic environment.

This juxtaposition of military and civilian functionalities creates ambiguity in distinguishing between legitimate wartime targets and civilian facilities. The elusive characteristics of certain dual assets, compounded by limited transparency, render the identification of military and civil objectives challenging. Recent cyber incidents, exemplified by the attack on Viasat's KA-SAT satellite, underscore the potential repercussions extending beyond mere military objectives. Additionally, vulnerabilities in cyber- and electronic security arise when military entities target dual-use ground stations, thereby raising concerns about the funnelling of civilian data into the military sphere and compromising privacy and overall safety.

Navigating the governance of these dual-use assets presents a complex paradigm. Unlike Antarctica, the Arctic lacks a dedicated international treaty or regime tailored to the region's dynamics. Instead, it falls predominantly under international sea law, which poses limitations, given the Arctic's oceanic nature. This regulatory void has historically fostered conflict, particularly during the Cold War, and continues to embolden the assertive behaviours of major powers competing for sea routes and natural resources today. Notably, the United Nations Convention on the Law of the Sea assumes significance in delineating maritime spaces, especially with regard to continental shelves beyond 200 nautical miles.[7]

In such a poorly regulated and contested domain, assessing regulatory tools for managing dual-use space technologies and infrastructures deployed in the area is particularly complicated. It is possible to derive rules or standard practices from legal regimes applied to other domains, such as international space law. Most central to this issue is the OST, a legally binding multilateral treaty signed in 1967. This treaty ensures all states peaceful access to outer space, bans the use of weapons of mass destruction in outer space and outlines rules for peaceful space exploration, consequently banning hostile space activities. Unfortunately, this legal regime applies

7 *United Nations Convention on the Law of the Sea*, 10 December 1982, 1833 UNTS 387 art 76 (entered into force 16 November 1992).

Table 1: Catalogue of Dual-Use Ground Stations, Their Locations, Operators and Dual-Use Capabilities

	Ground Station	Location	Operator	State Clients
1	Ny-Ålesund Yellow River Station	Svalbard, Norway	PRIC	China
2	China-Iceland Arctic Science Observatory	Karholl, Iceland	PRIC	China
3	Greenland Satellite Ground Station	Kangerlussuaq, Greenland	Beijing Normal University	China
4	China Remote Sensing Satellite North Polar Ground Station	Kiruna, Sweden	Institute of Remote Sensing and Digital Earth	China
5	Nuuk KSAT Ground Station	Nuuk, Greenland	OneWeb, KSAT	United States
6	European Organisation for the Exploitation of Meteorological Satellites	Svalbard, Norway	KSAT	Norway, European Union
7	OneWeb Pituffik Space Base	Thule, Greenland	OneWeb	United States
8	Jan Mayen KSAT	Jan Mayen, Norway	KSAT	Norway
9	SvalSat Ground Station	Svalbard, Norway	KSAT	Norway, United States
10	Grimstad KSAT	Grimstad, Norway	KSAT	Norway
11	Tromsø KSAT	Tromsø, Norway	KSAT	Norway
12	Inuvik KSAT	Inuvik, Canada	KSAT	Norway
13	Fairbanks KSAT	Fairbanks, Alaska	KSAT	Norway
14	Azure Stockholm	Stockholm, Sweden	Microsoft	United States
15	Inuvik Station SSC	Inuvik, Canada	SSC	Sweden
16	North Pole Station SSC	North Pole, Alaska	SSC	Sweden
17	Esrange Space Center	Kiruna, Sweden	SSC	Sweden

Source: Boschetti et al. (2022) and further reconnaissance performed by the authors.

Note: PRIC = Polar Research Institute of China.

only to activities carried out in space, leaving the other segments mostly unregulated.

When aimed at satellite ground stations, attacks are most likely to be electronic or cyber. A remote area such as the Arctic allows attackers to perform efficient and covert disruptions of communication systems, a strategic goal much more valuable than using armed force in this context. It is problematic, however, that article 41 of the UN Charter states that "the Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions....These may include complete or partial interruption of...telegraphic, radio, and other means of communication."[8] In simpler words, the UN Security Council would not consider complete or partial disruptions of satellite communications in the Arctic as the use of armed force. The international law regulating hostile activities toward space-ground infrastructures in the Arctic is consequently highly vague.

Therefore, any legislation or rules of conduct that may apply to satellite stations in the Arctic region must be deduced from other international treaties and regimes that govern specific territories or

8 *Charter of the United Nations*, 26 June 1945, Can TS 1945 No 7, art 41.

circumstances of the domain discussed here. One of these is the Svalbard Treaty[9] since, due to its latitude and international regime, the Svalbard archipelago is particularly exploited for space-ground infrastructures. Located east of Greenland, it hosts numerous scientific, research and commercial space infrastructures operated by several countries. The treaty established the "absolute sovereignty of Norway over the Archipelago of Spitsbergen [Svalbard]" and allowed signatories "equal liberty of access and entry for any reason or object whatever to the waters, fjords and ports of the territories specified in Article 1; subject to the observance of local laws and regulations, they may carry on there without impediment all maritime, industrial, mining and commercial operations on a footing of absolute equality."[10] Thus, the treaty established Norwegian sovereignty of the archipelago, but it gave signatory states equal commercial access to the region. As of today, 48 countries are part of this treaty and can use the Svalbard territory under the authorization and control of the Norwegian governor. The prohibition of any military activity on the islands makes the condition of dual-use satellite ground stations a source of international litigation between the states that are signatories to the treaty. For example, in November 2021, Russian Foreign Ministry spokesperson Maria Zakharova explicitly stated that the Russian Federation considers Norwegian satellite installations technically equipped to conduct dual-use operations. The SvalSat complex managed by KSAT now also hosts OneWeb's teleports under the latter's contract for providing satellite connectivity to American forces in the Arctic theatre, making the treaty application even more complex and insecure for infrastructure security and users. In addition, as will be explained in more detail shortly, the progressive weakening of multilateral negotiating fora, such as the Arctic Council, makes it more unacceptable to powers such as Russia and China that Norway conducts the control of operations in Svalbard, the same subject accused of violating the treaty.

In sum, the regulatory landscape governing space-ground infrastructure in the Arctic is multi-faceted and riddled with complexities. The dual-use nature of these assets, coupled with the absence of dedicated treaties and the evolving geopolitical environment, contributes to a challenging milieu for effective regulation. The competition among major powers and the intricate governance paradigms of the Arctic ultimately influence the security and operation of these critical assets.

Intergovernmental Cooperation

The Arctic, historically a site of contention, has seen the emergence of various international initiatives aimed at fostering cooperation among nations with interests in the area. These governance mechanisms, while aiming for collaboration, face challenges in the wake of heightened geopolitical tensions following Russia's actions in Ukraine. The evolving landscape of Arctic governance includes the Arctic Coast Guard Forum, established in 2015, which unites Coast Guard agencies from various Arctic nations. However, geopolitical tensions stemming from Russia's incursion into Ukraine have affected its diplomatic atmosphere.

Similarly, the Arctic Council, a pre-eminent governing body, comprises permanent members and observers, including China. Its successes include creating guidelines for exploration and rescue operations. However, its effectiveness has been strained due to increased tensions. The Barents Euro-Arctic Council and the Council of the Baltic Sea States, while focused on regional development, have also been influenced by strained international relations resulting from the Ukraine crisis.

In this intricate tapestry of Arctic governance, the Nordic Council fosters cooperation among Nordic countries, but geopolitical shifts have cast uncertainty over its collaborative efforts. Similarly, the Northern Dimension, initiated to address region-specific challenges, has faced setbacks due to international tensions. The Organization for Security and Co-operation in Europe (OSCE) provides a forum for addressing security matters, but Russia's conduct in Ukraine has affected its cooperation with the West.

Amid this backdrop, the Shanghai Cooperation Organisation, while not explicitly focused on the Arctic, covers a significant portion of the region, providing a platform for Arctic discussions. These efforts to navigate Arctic governance are impacted by shifting geopolitical dynamics, particularly in the aftermath of Russia's invasion of Ukraine. The complex realm of military cooperation in the Arctic further shapes the region's landscape. Defence organizations play a

9 *Svalbard Treaty*, 9 February 1920 (entered into force 14 August 1925).

10 *Ibid*, art 3.

crucial role in Arctic security and influence the region's space-ground infrastructures. Notable entities include NATO, ensuring collective defence for Arctic Council member countries, except Russia, which deepens mistrust while engaging in dialogue through the NATO-Russia Council.

Moreover, the Nordic Defence Cooperation fosters flexible defence collaboration among Nordic nations, including areas beyond the Arctic. The Collective Security Treaty Organization, a Eurasian alliance comprising states such as Russia, contributes to regional security dynamics through military exercises, including those in the Arctic.

These intertwined threads of international initiatives and military mechanisms shape Arctic security, impact space-ground infrastructures and contribute to the evolving security landscape of the region. As the competition among powers in the Arctic unfolds in an anarchic and potentially dangerous manner, the fate of ground stations and regional security remains uncertain.

Discussion and Recommendations

The Arctic region is undergoing a significant evolution. Geographically, climate change resulting in melting sea ice is leading vessels into waters particularly rich in resources, generating renewed tensions between nations. Geopolitically, the Russian invasion of Ukraine has accelerated Sweden and Finland's ascension to NATO, drastically changing the European Arctic's strategic landscape. These increasing geopolitical tensions have weakened traditional multilateral Arctic management bodies such as the Arctic Council and the OSCE. Deepened Sino-Russian regional cooperation is mirrored by NATO's renewed interest in ensuring strategic dominance. Lack of dialogue between major powers and growing military activities make the Arctic particularly unstable, with substantial consequences for critical infrastructures such as satellite ground stations. When deployed in remote areas, satellite ground stations are particularly reliant on fragile infrastructures such as seabed fibre-optic cables. Recent events such as the September 2022 Nord Stream 2 pipeline attacks have demonstrated that hostile actors are not hesitant to target critical infrastructure in the region. Monitoring, attribution and prevention of such acts becomes even more complex due to the lack of cooperation and dialogue among Arctic powers.

As previously illustrated, international agreements and treaties regarding space activities, such as the OST, are outdated and do not involve ground operations. This leads to a dualism in the security of space missions. If the orbits are strongly militarized but, by international law, not weaponized, the signals and ground infrastructures can be simultaneously militarized and weaponized. An attack against a satellite ground network is consequently not ruled by international space law but by the UN Charter. The current regulatory regime greatly improves the sustainability of the space environment. However, nothing specific is being done at the international and intergovernmental levels to reduce the insecurity of the other segments of space missions. The international community lacks legal tools to establish a safe regime for dual-use space-ground infrastructures. Space-based services and technologies serve several civilian purposes, from commercial services to more essential emergency and rescue operations. Networks concurrently serving military, intelligence users and human security operations are not sufficiently separated.

This situation, coupled with rising tensions in the Arctic, yields a double source of risk for space-ground infrastructures and, most of all, their users. As the Russian cyberattack against Viasat's KA-SAT telecommunications network during the early stages of the Ukraine invasion demonstrated, civilian users will likely be victims of attacks aimed at infrastructures serving military purposes. Apart from the impact on the daily operations of infrastructures relying on that network, commercial users lacked the certainty of a prompt solution by the affected company. Military and civilian users were not part of different problem-solving regimes, and in a war scenario, clear priorities regarding the users were absent.

In the current international scenario, dominated by an escalating trend of violation of international law and redefinition of blocs, it is difficult to glimpse the possibility of international cooperation on these issues in the short term. However, the security of space infrastructures in the Arctic, their users, and the data flowing through them can be addressed at national and NATO levels.

Dual-use technologies are currently mainly controlled at the national level through export regulations. These regimes focus on military, nuclear, chemical and biological technologies, while data systems are often under-represented. Despite the growing interest of countries such as the United States in outsourcing space intelligence to private individuals, the security of both physical infrastructure and computer systems should be particularly monitored. Projects under development, such as the American Hybrid Space Architecture program and the NATO Alliance Persistent Surveillance from Space, aim for a constant fusion of satellite data using a mixture of military and, above all, private infrastructure. Much of the data constituting the common intelligence picture of NATO forces will pass through the same antennas and servers as private data and civilian services. This means that offensive actions aimed at reducing NATO's intelligence or military support capabilities will dramatically affect the civilian and commercial activities that use that infrastructure.

Policy Recommendations

A first policy measure that NATO countries can adopt is to impose on commercial providers an effective and complete segmentation of their infrastructure. They should physically and/or virtually separate data-handling segments on the ground, reducing spillover effects in the event of an attack and, simultaneously, the chances for the attacker to make lateral movements in the system. In the current state of the international community, the main challenge to securing dual-use ground stations in the Arctic region is establishing multilateral agreements on the space segment. Although UN treaties and international agreements provide general guidelines, specific dual-use ground-station technology regulations must be addressed. Similar to efforts in defining and maintaining peaceful maritime operations in the Arctic, incorporating ground-station segment sustainability would be beneficial. The current political climate of mistrust is weakening international dialogue processes that could lead to new regulatory frameworks. The international community, especially the Arctic countries, should exploit every tool of global governance and diplomacy to secure expensive space infrastructure and the lives of the populations, depending on the services that the infrastructure at risk makes possible.

Additionally, learning from analogous regimes for dual-use technologies, such as those in nuclear energy or biotechnology, could shed light on practical management approaches to reduce suspicion and security concerns regarding space technologies. Taking inspiration from technologies deployed in Antarctica, where inspections of assets ensure peaceful usage, similar instruments promoting transparency in the Arctic could enhance the safe utilization of dual-use ground stations.[11]

Management Recommendations

In the Arctic's dual-use space-ground infrastructure context, it is imperative to consider a diverse mix of technologies across sectors to counteract potential cascading failures. The interconnectedness of diverse sectors with space systems emphasizes the need for a heterogeneous ecosystem to minimize compromised systems' impact. Past instances, although unintentional, have demonstrated that disruptions to space systems can propagate effects far beyond their intended targets, impacting critical infrastructure. Aerospace organizations should prioritize software diversity in their system configurations to limit the potential fallout of a single compromised system, ensuring resilience against unexpected consequences.

To enhance the security and responsiveness of dual-use space-ground infrastructure in the Arctic, organizations should streamline operational control, security practices and incident response policies across their entities, even when dispersed geographically. The complexity of organizational structures, typical in the aerospace domain, poses challenges in maintaining cohesive security control processes. Fragmented command structures across subsidiaries and geographical locations weaken the overall security posture of space systems. Mergers, acquisitions and geographical dispersion demand clarity in cyber-risk incident response plans and the delineation of responsibilities. Ensuring consistent cyber-risk management processes that all entities understand and follow becomes pivotal for maintaining security in such scenarios.

Mission-critical systems within dual-use space-ground infrastructure must be equipped with agile, software-enabled response strategies rather than rely solely on slow hardware replacements. Rapid response capabilities become crucial when facing cyberthreats that compromise functionality; for example, when modems are rendered inoperable due to malware, underscoring the need for swift over-the-air updates and the availability of redundant systems. Lessons from cases such

11 See www.ats.aq/e/peaceful.html.

as SpaceX's agile response to a jamming attack highlight the importance of developing responsive software updates and redundant systems to mitigate the impact of attacks on mission-critical space assets. In an environment characterized by evolving threats, agility and versatility are paramount for maintaining the functionality of dual-use space-ground infrastructure in the Arctic.

Conclusion

The policy recommendations above highlight the need for multilateral action to define new and updated legal regimes concerning ground-space infrastructures. This is difficult to achieve without a return to dialogue, even with hostile or opposing powers, and a precise definition of the concept of "dual use in the space sector." Volumes of data flow through icy antennas across the Arctic, from radar surveys of natural disasters to military communications. The security of such assets concerns not only the operation of military forces, but also the daily lives of billions of people, sometimes thousands of kilometres from the Arctic. Therefore, improved governance pertaining to these critical dual-use systems should be urgently addressed.

Works Cited

Boschetti, Nicolò, Nathaniel G. Gordon and Gregory Falco. 2022. "Space Cybersecurity Lessons Learned from the ViaSat Cyberattack." ASCEND 2022, Las Vegas, NV, October 24–26. https://doi.org/10.2514/6.2022-4380.

Boschetti, Nicolò, Nathaniel Gordon, Johan Sigholm and Gregory Falco. 2022. "Commercial Space Risk Framework Assessing the Satellite Ground Station Security Landscape for NATO in the Arctic and High North." In *MILCOM 2022 — 2022 IEEE Military Communications Conference,* 679–86. New York, NY: IEEE. https://doi.org/10.1109/MILCOM55135.2022.10017538.

Boschetti, Nicolò, Chelsea Smethurst, Gregory Epiphaniou, Carsten Maple, Johan Sigholm and Gregory Falco. 2023. "Ground Station as a Service Reference Architectures and Cyber Security Attack Tree Analysis." In *2023 IEEE Aerospace Conference,* 1–12. New York, NY: IEEE https://ieeexplore.ieee.org/document/10115903/.

Brady, Anne-Marie. 2017. *China as a Polar Great Power.* Cambridge, UK: Cambridge University Press.

DoD. 2021. "Joint Statement on NORAD Modernization." Press release, August 17. www.defense.gov/News/Releases/Release/Article/2735041/joint-statement-on-norad-modernization/.

Doshi, Rush, Alexis Dale-Huang and Gaoqi Zhang. 2021. *Northern expedition: China's Arctic activities and ambitions.* Washington, DC: Brookings Institution. April. www.brookings.edu/articles/northern-expedition-chinas-arctic-activities-and-ambitions/.

Earth Resources Observation and Science Center. 2020. "USGS EROS Archive — Landsat Archives — Landsat 8–9 Operational Land Imager and Thermal Infrared Sensor Collection 2 Level-1 Data." US Geological Survey, March 4. www.usgs.gov/centers/eros/science/usgs-eros-archive-landsat-archives-landsat-8-9-operational-land-imager-and.

Erwin, Sandra. 2021. "OneWeb looking to fill demand for connectivity in the Arctic." *Space News,* March 28. https://spacenews.com/oneweb-looking-to-fill-demand-for-connectivity-in-the-arctic.

———. 2022. "Space Force delivers first of two U.S. payloads to launch on Space Norway's arctic broadband mission." *Space News,* June 9. https://spacenews.com/space-force-delivers-first-of-two-u-s-payloads-to-launch-on-space-norways-arctic-broadband-mission/.

Foust, Jeff. 2023. "Shotwell: Ukraine 'weaponized' Starlink in war against Russia." *Space News*, February 8. https://spacenews.com/shotwell-ukraine-weaponized-starlink-in-war-against-russia/.

Hilde, Paal Sigurd. 2013. "The 'new' Arctic — the Military Dimension." *Journal of Military and Strategic Studies* 15 (2): 131–53. https://jmss.org/article/view/58098.

Mearsheimer, John J. 1994. "The False Promise of International Institutions." *International Security* 19 (3): 5–49. www.jstor.org/stable/2539078.

NASA. 2024. "Ground Data Systems and Mission Operations." In *State-of-the-Art of Small Spacecraft Technology*, 290–353. February. www.nasa.gov/smallsat-institute/sst-soa/ground-data-systems-and-mission-operations.

Nilsen, Thomas. 2023. "Russia plans Svalbard science complex in cooperation with 'friendly states.'" *The Barents Observer*, June 12. https://thebarentsobserver.com/en/arctic/2023/06/russia-plans-svalbard-science-complex-cooperation-friendly-states.

OneWeb. 2021. "Hughes and OneWeb to Demonstrate Low Earth Orbit Service in Arctic Region for U.S. Air Force Research Lab." Press release, May 5. https://oneweb.net/resources/hughes-and-oneweb-demonstrate-low-earth-orbit-service-arctic-region-us-air-force-research.

Pugliese, David. 2022. "Satellites key to Canada's Arctic surveillance strategy." *Space News*, May 17. https://spacenews.com/satellites-key-to-canadas-arctic-surveillance-strategy/.

The White House. 2022. "National Strategy for the Arctic Region." October. www.whitehouse.gov/wp-content/uploads/2022/10/National-Strategy-for-the-Arctic-Region.pdf.

Wolf, Harrison G. 2012. "ITAR reforms for dual-use technologies a case analysis and policy outline." In *2012 IEEE Aerospace Conference*, 1–12. New York, NY: IEEE. https://doi.org/10.1109/AERO.2012.6187448.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

@cigionline