IDSS PAPER

25 March 2026

The Earth–Space Interface
An Overlooked Vulnerability

Marine Ourahli

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSiS 30

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ponder the Improbable since 1996

IDSS Paper
Ponder. Analyse. Prepare. Engage. Refresh.

www.rsis.edu.sg
No.052– 25 March 2026

The authors' views are their own and do not represent the official position of the Institute of Defence and Strategic Studies of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the authors and RSIS. Please email to Editor IDSS Paper at RSISPublications@ntu.edu.sg.

The Earth–Space Interface: An Overlooked Vulnerability

Marine Ourahli

KEY TAKEAWAYS

- *The Earth–space interface that enables outer space activities, including infrastructure like control centres, ground stations and launch sites, is a highly visible target that is exposed to a diverse range of both kinetic and non-kinetic threats.*

- *The emergence of low-orbit satellite constellations expands the area of vulnerability on the ground since they require more receivers and antennas to capture and process signals. This creates a paradox: while the space segment becomes less vulnerable, the Earth–space interface becomes more exposed.*

- *These interfaces are positioned at the intersection between outer space, electromagnetic, and cyber domains, making resilience critical.*

COMMENTARY

On 5 March 2026, the United States claimed to have destroyed Iran's military space capabilities as part of strikes on Tehran's command-and-control and intelligence capabilities. Iran responded by warned "countries hosting ground stations and companies providing uplink services transmitting anti-Iranian terrorist networks". While discussions on military activity in outer space naturally focus on what is happening in orbit, this recent example highlights the reality that space-based assets and capabilities depend on infrastructure that is terrestrial.

In this context, the Earth–space interface, defined as Earth-based institutions and infrastructure that control and coordinate human activities in space, becomes critical. While attacks on space infrastructure in orbit pose significant risks – including potential damage to an attacker's own space assets and unintended escalation with third parties – targeting terrestrial infrastructure allows for greater precision using far more accessible capabilities, while at the same time limiting collateral risks. Furthermore, the Earth–space interface is expanding rapidly as an increasing number of states are developing sovereign infrastructure and supporting capabilities for their growing presence in outer space. This development is increasing the potential attack surface, since the Earth–space interface represents an accessible and strategically impactful point of disruption for space systems.

A Strategic Asset

The Earth–space interface plays a central role within the ecosystem of modern military capabilities. It enables the monitoring of all Earth-based activities from outer space through satellite command and control as well as the infrastructure that converts signals and data into operational services and actionable intelligence. Ground stations can support near real-time intelligence, significantly reducing data latency and extending geospatial coverage.

The Earth–space interface plays a central role within the ecosystem of modern military capabilities.
Image source: ESA/C. Lezy, CC BY-SA 3.0 IGO, via Wikimedia Commons.

The rapid proliferation of satellite constellations in low-Earth orbit (LEO) is accelerating the expansion of the Earth–space interface. While traditional geostationary satellites also rely on specialised ground infrastructure, LEO satellite constellations require dense global networks of antennas, gateways and data routing infrastructures. While this is meant to enhance operational resilience by multiplying the number of satellites and mitigating capacity loss, it simultaneously extends the surface area of ground-based vulnerability for space systems.

More importantly, militaries rely on private-sector actors when it comes to LEO satellite constellations, with companies such as Starlink, Project Kuiper and OneWeb owning the infrastructure that serves military customers. Their space systems depend on hundreds of ground stations connected via terrestrial fibre networks and cloud-based control platforms. A single ground base can serve multiple states, making it both a strategic asset and a high-value target.

Moreover, states that lack the resources to domestically develop capabilities in telemetry and satellite control are adopting a "ground station as a service" (GSaaS) model. GSaaS allows states with satellites to lease access to shared global networks of ground antennas on a pay-per-use basis, often from major commercial providers such as Amazon Web Services. Ground stations become digitalised, enabling mission control functions to be managed through shared infrastructure.

Navigating Dependencies

Many spacefaring states depend on the ground-based infrastructure of a handful of states such as the United States, Russia, China, India and Japan for launching their satellites. For example, Timor-Leste's first satellite will be launched from Japan under a bilateral agreement. Satellite launch facilities remain rare because they require highly specific geographical conditions and substantial financial resources.

Given their strategic nature, access to launch facilities has naturally become entangled in geopolitics. A striking example is the Baikonur Cosmodrome, leased by Kazakhstan to Russia, a legacy of the USSR's rule over the country. Tensions between Russia and the United Kingdom forced the British company OneWeb, which provides many states with satellite-based services – including Thailand and Vietnam in Southeast Asia – to cease its operations at Baikonur.

Challenges with access are prompting spacefaring states to try to develop sovereign capabilities to support their space-based assets. This is why Earth–space interface infrastructure is being developed in Malaysia and Brazil. In late 2025, Turkey announced plans to build a spaceport in Somalia.

For these states, developing sovereign Earth–space interface infrastructure is aimed at reducing dependence on foreign powers and commercial operators. These facilities can also allow states to position themselves as alternatives to others facing challenges with access. This trend signals the growing significance of regions previously considered peripheral in the global space race.

A Kinetic and Non-Kinetic Vulnerability

Space systems are extremely sensitive to intrusions regardless of their scale; even a minor disruption can have a disproportionately significant impact on the operational performance of space-based assets. Under these circumstances, the Earth–space interface emerges as an indispensable strategic asset. However, this comes with significant vulnerability. Ground-based infrastructure is fixed, visible and frequently connected with civilian networks, making it easily identifiable and vulnerable to attack.

The attack by Russian hackers on ViaSat's KA-SAT network in February 2022, which disrupted the Ukrainian military's satellite communications, highlighted the cyber vulnerabilities of space systems and their importance as targets. An overlooked aspect of this attack was that the hackers gained entry through the Earth–space interface. Cyber operations focusing on ground-based infrastructure provide attackers with a cost-effective alternative to kinetic strikes that is difficult to attribute. This was demonstrated by the January 2026 intrusion into the European Space Agency's systems, in which 200 gigabytes of data, including source code repositories, were reportedly stolen.

In August 2025, the UK Department for Science, Innovation and Technology issued a warning about the threats associated with the growing integration of cloud computing into space systems through GSaaS. The report highlighted the challenges to operational technology systems, particularly antenna control and telemetry, tracking and command. Such systems may be vulnerable to denial-of-service attacks or timing signal manipulations. Although virtualisation through GSaaS enables states to control their satellites from thousands of kilometres away from where ground-based infrastructure is located, it also introduces risks such as unauthorised command hijacking, data manipulation, and service disruption.

Conclusion

Cyberspace has become the preferred domain for space-related conflicts, allowing for the exploitation of increasing vulnerabilities while remaining below the threshold of open warfare. As reliance on space-based services continues to grow, enhancing Earth–space interface resilience will become a critical challenge not only for national security agencies but also for the commercial space sector, given that cyberattacks like the ViaSat case exploit vulnerabilities within supply chains through subcontractors and third-party service providers. To enhance this resilience, governments need to consolidate ties between national cybersecurity authorities and private companies in the space sector and encourage and support the latter in fully assuming their responsibilities for developing more rigorous cybersecurity capabilities.

Marine Ourahli *is a Senior Analyst with the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS).*