Russian Spy Satellites Intercepting European Satellite Communications

February 8, 2026

European space security officials are increasingly concerned that two Russian “inspector” satellites have been used to collect communications associated with multiple European satellites, including traffic linked to government and military users. This has evidently been a sustained pattern over several years, with the alleged consequence being intelligence collection and a clearer mapping of how European satellite services could be constrained or disrupted in crisis conditions.

Such activity risks compromising sensitive information transmitted by the satellites but could also allow manipulation of the satellite flight paths or even lead to accidents.

What is reported to have happened

The reporting attributes the assessment to European security and intelligence officials who have been tracking two Russian spacecraft commonly referred to as Luch-1 and Luch-2. Officials reportedly believe these spacecraft were able to intercept communications from at least a dozen European satellites. The reporting also notes close approaches to a wider set of satellites over a multi-year period, which, if accurate, would reflect deliberate station-keeping near targets rather than incidental co-location in geostationary orbit.

A key technical qualifier is that interception risk is not uniform. A close look points to legacy vulnerabilities,

including the fact that some older satellites may still rely on weak or unencrypted command links, creating exposure not only for confidentiality but also for command authentication and operational integrity.

None of this requires assuming a “weapon” in orbit. Persistent proximity operations, combined with modern signals-intelligence payloads, can be sufficient to collect metadata, waveform characteristics, traffic volumes, and in some cases content, depending on encryption and link discipline. Even where encryption holds, the collector learns usage patterns, the contours of the ground segment, and system behavior under stress.

Why proximity operations matter commercially

Geostationary orbit is a commercial operating environment. Many satellites carry mixed traffic of commercial connectivity, leased capacity, and governmental payloads or services. That makes “space security” inseparable from commercial service continuity and contract performance.

Three immediate consequences follow.

First, security standards will move from guidance to gating. Encryption, authenticated command and telemetry, and disciplined key management are no longer features that win competitive bids. They are baseline conditions for eligibility, particularly for government and critical-infrastructure customers.

Second, underwriting and financing will harden around cyber-physical risk. The market already prices launch and debris risk. Persistent proximity and interception concerns introduce a more political category: contested-domain operating risk. That tends to produce tighter warranties, more onerous security representations, and narrower coverage around interference events.

Third, customers will demand assurance, not only service levels. Expect procurement language to expand beyond uptime and throughput into incident response timelines, sovereign control of command chains, ground segment resilience, and demonstrable ability to maintain service under interference conditions.

These pressures are intensified by Europe's parallel policy direction toward sovereign secure connectivity. In January 2026, public statements from the European Commission described the commencement of GOVSATCOM operations, explicitly framed as secure and encrypted governmental satellite communications under European control.

The legal consequences: duties exist, but enforcement is political

The legal framework for outer space has not suddenly become obsolete. It is, however, strained by conduct that sits *below* the threshold of overt attack while still producing strategic harm.

Under the Outer Space Treaty, States must conduct activities with "due regard" to the corresponding interests of other States, and where a State has reason to believe an activity would cause "potentially harmful interference," it should undertake appropriate international consultations. This is not a direct prohibition on collection, and it does not neatly capture intelligence operations. It does, however, create a lawful diplomatic pathway: if proximity operations are credibly framed as creating a risk of harmful interference or unsafe behavior, consultations are the treaty-based mechanism to press the issue.

Separately, Article VI's responsibility principle matters in today's mixed government-commercial architecture: States bear international responsibility for national activities in outer space, including those by non-governmental entities, and must

authorize and continuously supervise such activities. In practical terms, this pushes European regulators toward more explicit security supervision of licensed operators whose systems carry government traffic, and it strengthens the policy case for security conditions in licensing and procurement.

The radio layer adds another legal and regulatory vocabulary. The International Telecommunication Union radio regime is designed to prevent harmful interference and imposes obligations on administrations regarding stations under their responsibility. If interception evolves into jamming, spoofing, or service disruption, that framework provides process and terminology even when remedies remain political.

The limiting factor across these regimes is attribution and proof. Legal consequences scale with confidence. That reality will drive investment in independent tracking, data fusion, and evidentiary discipline, because sustaining a position in a diplomatic, regulatory, or legal forum matters.

Strategic meaning: below-threshold pressure becomes normal

The most consequential implication is not that satellites can be listened to. It is that space is being treated as a continuously contested domain, and that this contest is increasingly conducted through activity that stays below the threshold of overt interference.

For operators, the lesson is straightforward: resilience must be engineered and contractually demonstrated.

For governments, the implication is equally clear: the line between commercial service and national capability is thin, and it will continue to thin. Hybrid payloads, shared capacity, and multi-use constellations bring efficiency, but they also bring shared exposure.

For Europe, this incident reporting will likely accelerate

three tracks already underway: (1) hardening of legacy systems and uplink security practices; (2) procurement and licensing reforms that make security a condition of market access; and (3) sovereign and allied connectivity architectures that reduce single points of failure and impose higher security baselines.

The diplomatic posture should remain measured. The objective is to reduce strategic ambiguity, raise the cost of intrusive behavior through collective standards and coordinated responses, and ensure that Europe’s commercial satellite market remains credible to the customers who depend on it.

In short, the future will not be defined by a single episode of proximity collection. It will be defined by whether Europe treats this as an intelligence curiosity, or as a governance and market-structure inflection point.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile: https://waselandwasel.com/about/abdulla-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com