ADVISORY FOR ICM SECTOR

Trends in Cyber Threats to Satellite Communications Systems

Original report published on: April 09, 2026

Executive Summary

As satellite deployments and interconnected ground systems continue to expand, the attack surface of such systems increases. In many instances, satellite operations are targeted indirectly rather than directly via satellites in orbit. These include signal-layer techniques such as jamming and GPS spoofing, as well as the exploitation of weaknesses in ground-segment assets, including Internet-facing enterprise systems and credential-based access mechanisms. Credential theft and unauthorised access will remain persistent risks to both satellite service users and supporting infrastructure.[1,2] Social engineering and network traffic monitoring have been used to identify satellite system users and restrict their connectivity. These approaches are effective, scalable, easier to deploy, and are likely to remain central to the evolving threat landscape.

Background

Satellite communications (SATCOM) are being disrupted through a combination of network controls, electronic warfare (EW), and physical detection. In 2026, network monitoring, filtering, deep packet inspection, and VPN fingerprinting were reportedly used to identify and block Starlink and other satellite services, limiting user connectivity.[3] In these instances, the use of handheld and vehicle-mounted scanners can detect Wi-Fi signals and, in turn, help locate nearby satellite user terminals. Enforcement teams may then seize equipment and identify users of unauthorised satellite networks.

Additionally, signal interference, jamming, GPS spoofing, Automatic Identification System (AIS) spoofing, and satellite uplink interference were reportedly used to degrade internet connection via satellite and disrupt navigation and maritime tracking.[4]

Beyond the abovementioned signal-layer techniques, threats targeting the ground and user segments are increasingly being observed. In February 2026, fake Telegram channels and bots offering Starlink activation services were used to collect user data and payments from military-associated users. Local authorities then blocked related access without affecting satellite infrastructure.[5]

Since 2021, multiple threat actors, including NOMAD PANDA, AQUATIC PANDA, VANGUARD PANDA, and CAULDRON PANDA, have targeted Internet-facing systems across the government, defence, aerospace, and space sectors. They steal credentials by exploiting vulnerabilities to collect Active Directory authentication data, maintain persistence using web shells such as WhizShell, and move laterally within enterprise networks. From January to March 2025, the VIXEN Panda group used operational relay box (ORB) infrastructure to

route traffic through compromised systems and sustain persistent access to networks supporting satellite operations.

Detection and Mitigation

IMDA recommends that organisations that (a) leverage satellite communications or (b) offer such services perform continual testing and validation of their security controls to ensure the detection and prevention of satellite-related threat activities identified in this report:

With reference to *NASA's Space Security: Best Practices Guide (BPG) Rev B* and the *Australian Cyber Security Centre's Securing Space*:[6,7]

For organisations leveraging satellite connectivity (e.g., as backhaul or for remote sites), we recommend:

Detection

- Deploy continuous network monitoring, such as Network Detection and Response (NDR), at key ingress and egress points to detect anomalous traffic patterns, including suspicious use of satellite backhaul for outbound connections or potential adversary C2.
- Monitor user and service accounts with access to satellite-connected networks for anomalous behaviour, such as logins from unusual locations, abnormal access times, or access to systems outside normal patterns.

Mitigation

- Segment satellite-connected networks from core enterprise networks, using boundary protections such as firewalls, ACLs, and jump-host access to limit the exposure of internal systems via satellite links, in line with NASA's Space Security: Best Practices Guide (BPG) guidance on resilient architectures and boundary protection.
- Implement multi-factor authentication with unique named accounts for satellite management portals, remote access solutions, and VPN access points used to reach satellite-connected environments, eliminating shared credentials and periodically revoking unused accounts or API keys.
- Ensure critical services have redundant connectivity paths (for example, alternate terrestrial links or diverse SATCOM providers) and are covered by tested continuity plans that explicitly address satellite service loss or compromise.

For organisations offering SATCOM (providers/operators):

Detection

- Deploy network monitoring solutions, such as NDR, at external and internal mission boundaries to detect anomalous traffic, including connections routed through anonymising services, ORB networks, or proxy relays indicative of adversary C2 activity.

- Monitor subscriber, user, and service accounts for anomalous access behavior, such as logins from unusual locations, abnormal access times, or access to systems outside established patterns.

Mitigation

- Apply boundary protection and network segmentation using mediated access controls to logically and physically isolate Telemetry, Tracking, and Command (TT&C) and mission systems from internet-facing and enterprise networks, enforcing access via bastion hosts, allowlisted management networks, and strict firewall rules. Satellite TT&C and mission systems should not be directly connected to the public internet.

- Implement multi-factor authentication with unique named accounts across all ground-segment systems, satellite management portals, and VPN access points, eliminating shared credentials and periodically revoking unused or dormant API keys.

- Establish verified, controlled channels and processes for satellite service activation and configuration changes to prevent unauthorized modifications.

- Conduct regular resilience and failover testing for ground stations and gateways, including scenarios involving targeted cyber-attacks and loss of satellite or ground assets.

For organisations that own physical systems, we recommend:

Detection

- Deploy radio frequency (RF) sensors, including software-defined radio (SDR) based spectrum probes, to monitor navigation and communications bands for abnormal emitters and power levels, and apply behavioural anomaly detection to AIS navigation and timing data to flag baseline deviations indicative of threat actor EW activity.

- Validate the integrity and plausibility of positioning, navigation, and timing (PNT) data against multiple independent and trusted sources before using it for mission-critical decisions, mitigating risks from GPS spoofing and signal manipulation.

- Integrate RF anomaly detection and PNT integrity alerts into centralise monitoring platform and incident response playbooks, ensuring coordinated response across ground, user, and space segments.

Mitigation

- When EW activity is detected, confirm the interference, then shift or reroute critical services to alternate links or fallback paths where feasible, escalating to the incident response team while preserving RF captures, logs, and telemetry data for follow-up analysis and potential attribution.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

References

1. 2025 SpyCloud Identity Exposure Report
2. Space Threat Assessment 2025
3. Near-total digital isolation - digital rights group
4. Heightened Risk of GPS/AIS Interference in the Gulf of Oman and Strait of Hormuz
5. Fake Starlink service that revealed battlefield locations
6. NASA Space Security: Best Practices Guide (BPG) Rev B
7. Australian Cyber Security Centre - Securing space