Space ISAC Q4 2025 Public Report

TLP CLEAR: Released: 12/19/2025

The purpose of this report is to provide a broad overview of the space threat landscape through the lens of the prominent attack vectors, active campaigns, and recent activities impacting the ground, link, space, launch, and user segments of the space domain. These contents include observations of significant events and trends from Q3 2025 (01 October – 12 December)

Space infrastructure is a vital component of national security and an enabler of nearly all critical functions that are relied upon globally. The current dialogue on security for space systems centers around creating safe practices to protect our global space infrastructure, heightened by the continued proliferation of space assets and the growing concerns regarding the militarization of space. The threat landscape for space forecasts increased threats, driven in part by AI-assisted operations and underscored by advanced tradecraft.

1. Terrestrial Cyber Operations: The commercial space sector continued to experience sustained levels of targeting, driven primarily by financially motivated cybercriminal activity. This threat landscape is further intensified by growing collaboration among cybercriminal ecosystems, including the convergence of hacktivist collectives and Ransomware-as-a-Service (RaaS) operators. These actors increasingly refine their tactics, techniques, and procedures (TTPs) to enable prolonged access to high-value targets. Recent examples of this activity include the following:

- Pro-Russian hacktivist NoName057(16) claimed multiple targets in aerospace, satellite communications, and telecommunications throughout Q4 2025
- The pro-Iranian hacktivist group *HEZI RASH* conducted a purported distributed denial-of-service (DDoS) attack against NASA's Open Data Portal.
- The *Everest* ransomware group claimed to have exfiltrated and subsequently leaked data allegedly belonging to Collins Aerospace, consistent with double-extortion ransomware operations.
- Threat actors continue to leverage a cyber espionage tool known as *VShell*, representing a notable tool in the broader cyber threat landscape, according to researchers at NVISIO.
- The *Lazarus Group* conducted spearphishing campaigns against aerospace and defense organizations, leveraging tailored lures to deliver malware and establish persistence.
- *Mandiant* published analysis attributing sustained cyber operations against the aerospace and defense ecosystem to Iran-linked threat cluster *UNC1549*, highlighting espionage-focused objectives.
- The *J* ransomware group targeted the Australian Defense Industrial Base, including an intrusion against *IKAD Engineering*, consistent with financially motivated ransomware activity.
- Researchers identified an increasing number of cyber campaigns launched against multiple entities in the Russian Aerospace ecosystem
- The Maritime sector was targeted in a campaign involving the Mirai Botnet, posing potential disruptions to satellite connectivity.

2. Supply Chain/Finance: Software and hardware supply chain dependencies continue to represent a systemic risk to the space and aerospace ecosystem. Threat actors continue to exploit vulnerabilities in widely trusted platforms, update services, and third-party components to achieve scalable access across downstream environments. These activities highlight how compromise of suppliers or providers can perpetuate operational risk across support infrastructures. Recent examples of this activity are as follows:

- Additional exploitation of the ToolShell exploit chain was observed in October 2025, compromising multiple sectors and agencies globally.
- China-nexus Advanced Persistent Threat (APT) actors were observed deploying the Airstalk malware in targeted supply chain attacks against Business Process Outsourcing (BPO) organizations.
- Security researchers identified exploitation of a critical vulnerability affecting Microsoft Windows Server Update Services (WSUS), leading to unauthorized execution of commands.
- Adversaries exploited multiple vulnerabilities in FortiWeb, including zero-day exploitation of CVE-2025-64446 and a separate OS command injection vulnerability tracked as CVE-2025-58034
- Security researchers disclosed and patched a three-year-old command injection vulnerability in NASA's CryptoLib, a widely used cryptographic library in spacecraft and ground-station systems.
- Researchers introduced a framework for studying supply chain threats in small satellite systems called SpyChain, examining risks from third-party commercial-off-the-shelf (COTS) hardware
- China-linked *Salt Typhoon* threat actors leveraged zero-day vulnerabilities in conjunction with DLL side-loading techniques to compromise global targets, demonstrating advanced tradecraft.
- Threat actors actively exploited the *React2Shell* vulnerability (CVE-2025-55182) in React Server Components to achieve remote code execution via maliciously crafted requests to server function endpoints, enabling post-exploitation activity on affected web applications.
- The Cybersecurity and Infrastructure Security Agency (CISA) identified active exploitation of CVE-2025-58360 affecting GeoServer, indicating continued adversary abuse of this software.

3. Development and Production: Development and production environments remain high-value targets as adversaries increasingly exploit trusted tools, code repositories, and recruitment workflows to gain initial access. Recent activity highlights how compromises of vendors and open-source networks can introduce risk across aerospace, defense, and other critical infrastructure sectors. Recent examples of this activity are as follows:

- A nation-state affiliated cyber threat actor compromised F5's systems and gained access to sensitive data, generating cascading impacts to critical infrastructure sectors.
- North Korea–aligned *Lazarus Group* targeted European aerospace organizations via social engineering as part of its ongoing *DreamJob* campaign, using fraudulent recruitment lures to facilitate initial access.
- Researchers identified malicious NuGet packages that injected time-delayed destructive payloads into database operations and targeted industrial control systems.
- Researchers cited a 140% increase in use of open-source malware, used by attackers to target data and trusted dependencies.

- Chinese-backed Storm-1849 actors attributed to the targeting of Cisco ASA devices used by governments, defense contractors, and military organizations throughout October 2025.
- The Shai-Hulud npm campaign resurfaced, compromising over 25,000 repositories, impacting major packages, exposing secrets, and exfiltrating sensitive data.
- North Korea–aligned actors refined the *"Contagious Interview"* campaign by abusing public JSON storage services as covert malware delivery channels, using trojanized code repositories and legitimate web traffic patterns to evade detection.

4. Launch, Landing, and Recovery: Launch segment operations encompass a dynamic space environment that includes on-board hardware components and their criticality to launch missions, what payloads of interest are being launched, and multiple nations advancing their space faring capabilities. Recent examples of this activity are as follows:

- China has conducted 25 orbital launches in Q4 2025, marking the most in any quarter. China has also officially surpassed their previous record launch total within a calendar year.
- China has shifted focus to bolster some of their Geostationary fleets such as the TJS and SJ constellations, of which are believed to support unknown military functions.
- At least one launch service provider postponed a launch due to concerns from Space Weather activity.
- Launch activity has generated concerns regarding a possible near collision with a launch and a satellite on-orbit. Official investigations are currently underway.
- Poland has launched the nation's first military satellite aboard a dedicated rideshare mission, signifying the nation's advancing space capabilities.
- Multiple Chinese Taikonauts faced a delayed return mission due to space debris with the returning capsule.
- Azerbaijan is set to begin domestic satellite manufacturing - including developing a satellite production plant and training facilities for future engineers.
- The Philippine Space Agency continues to cite concerns for rocket and space debris from launch activity related to China as this debris continues to reenter uncontrolled near mainland areas.
- A Russian launch resulted in the destruction of the nation's most significant launch pad for sending astronauts into orbit.
- India has launched the nation's largest communication satellite (4,410 kilograms / 9,722 pounds), matching only the U.S., Russia, and China in launch service capabilities.

5. Critical Infrastructure Protection: Critical infrastructure protection displays a dynamic hybrid warfare environment from the physical threat towards subsea cables to the routine cyber targeting of government infrastructure, telecommunications, and global political / military investments bolstering defensive space capabilities. Recent examples of this activity are as follows:

- Russian state-sponsored cyber operations have drawn concern regarding the evolution of physical and cyber espionage.
- Unknown drone activity remains a concern across multiple European countries as Russian disinformation campaigns have contributed to obfuscation of activity.

- Germany and France signed an implementation agreement for a satellite-based early warning system called Odin's Eye to defend against emerging threats.
- Taiwan and the United Kingdom are increasingly under threats due to subsea cable disruption events, launching security initiatives for protection.
- The European Space Agency has announced a roughly €1 billion plan for the development of a military-grade reconnaissance satellite network.
- The Federal Network Agency of Germany has tightened security measures for the Telecommunications sector predominantly stemming from growing cyber threats.
- Nation state actors are blending cyber-enabled kinetic targeting in which nation-state threat actors systematically use cyber operations to enable and enhance physical operations.
- China has announced plans for a satellite manufacturing complex capable of producing ~1,000 satellites annually.
- Nearly 50% of observed ransomware attacks target critical infrastructure sectors such as manufacturing, energy, transportation, and more, according to cybersecurity agency KELA.
- Cybercriminals and Hacktivist groups routinely target critical infrastructure sectors globally with Distributed-Denial-of-Service attacks.

6. Space System Operations: The link segment is routinely under disruption from Global Navigation Satellite System (GNSS) interference, jamming, and spoofing impacting aviation, maritime, and satellite operations. Additional consideration is given to the dynamic on-orbit environment regarding verified spacecraft maneuvers in Low Earth and Geostationary Earth orbit. Recent examples of this activity are as follows:

- Electronic warfare activity attributed to Russia continues to generate concerns regarding possible Signals Intelligence (SIGINT) facilities targeting spacecraft on-orbit.
- For most of Q4 2025 the greater India Flight Information Region has felt impacts relating to GNSS interference, jamming, and spoofing.
- Chinese researchers have outlined ways to disrupt and jam the communication connections between mega-constellations.
- A Russian satellite tracked as *COSMOS 2589* has lost stability in orbit and is tumbling out of control.
- The *LUCH OLYMP (OLIMP-K1)* Russian SIGINT satellite, operating in a geostationary orbit, has officially been decommissioned as it maneuvered into a graveyard orbit.
- China's SJ-21 & SJ-25 appear to have finished the nation's first on-orbit refueling mission in the Geostationary belt.
- The United Kingdom Maritime Trade Operations continues to outline GNSS interference across the greater Middle East, specifically the Persian Gulf.
- Russia has maneuvered eight specific satellites approximately 54 times across the Low Earth and Geostationary orbits in Q4 2025.
- China has maneuvered 28 specific satellites ~87 times across the Low Earth and Geostationary orbits in Q4 2025.
- The United Kingdom is beginning to develop advanced collision avoidance system tailored for Low Earth Orbit (LEO) satellite constellations.

7. Space Environment: Thanks to a highly dynamic and eruptive space weather environment, there have been several events chronicled across the past few months. These events have ranged in impact from regional blackouts in radio transmissions to increases in Global Navigation Satellite System (GNSS) noise and a potential linkage to a software vulnerability impact triggering an emergency directive. Recent examples of this activity are as follows:

- Geomagnetic G2 (Moderate) and G3 (Strong) levels were reached during this quarter, including one instance of G4 (Severe) storm levels being reached on 12 November 2025.
- Although there were several flares during this period that emanated off the solar disk, one of the strongest was an X5.1 on 11 November 2025 from Active Region 4274. This Active Region has been one of the most active this quarter, dispatching several different classes of flares due to its complexity.
- Coronal hole based high speed streams have continued varying in velocity & intensity but spiked from an average of ~ 450 km/s to a peak of ~ 800 km/s with a surge in temperature from ~ 150,000 to ~ 600,000 Kelvin as detected by the Advanced Composition Explorer (ACE) satellite on 11 October 2025.
- The orbital drag environment between the 400 – 900-kilometer range in Low Earth Orbit (LEO) has routinely seen levels of drag concurrent with 'alert' and 'danger' call outs spanning 70-130% comparison changes in density between daily captures & enhancement distinctions.
- On or about 11-12 November 2025, the Jet Propulsion Laboratory (JPL) GNSS-based Upper Atmospheric Realtime Disaster Information and Alert Network (GUARDIAN) plotted a broadly impacting multi-GNSS noise level surge spanning multiple latitudes in both hemispheres and linked to an elevated planetary K-index (Kp).
- NASA's Center for Geospace Storms (CGS) on 13 December 2025 released the Multiscale Atmosphere-Geospace Environment (MAGE) model as a science center initiative involving over 50 experts from seven global institutions thereby combining efforts to improve predictive modeling of solar effects on Earth's space environment.
- Using 11 years of magnetic field measurements from the European Space Agency's Swarm satellite constellation, scientists have discovered that the weak region in Earth's magnetic field known as the South Atlantic Anomaly (SAA) has expanded by an area half the size of continental Europe since 2014 towards South Africa.
- A recent issue with a software version known as L104 (Elevator Aileron Computer – ELAC B) and its potential linkage to a solar radiation event on a JetBlue Flight exposed a critical vulnerability in the Airbus A320 family of aircraft software. This issue is globally impactful and drove the European Union Aviation Safety Agency (EASA) to issue an Emergency Airworthiness Directive impacting over 5,000 in service aircraft.
- Based on the European Union Space Surveillance and Tracking (EU SST) dashboard, there have been 23 total reentry events tracked (both minor and medium categories) impacting over 40 areas of interest globally with three upcoming events.