Space ISAC Q1 2025 Public Report

TLP CLEAR: Released: 04/28/2025

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 Q1 2025 (01 January – 31 March)

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 towards the militarization of space. The current threat landscape for space forecasts increased threats, precipitated by geopolitical and economic factors.

1. Terrestrial Cyber Operations: The commercial space sector continues to face a myriad of cyber threats, which include geopolitically motivated operations intent on disrupting or defacing websites, opportunistic threats focused on extorting companies for financial gain, and targeted campaigns motivated by cyber espionage and intelligence gathering. Recent examples of this activity are as follows:

- Ransomware groups continue to target component manufacturers and solutions providers that serve space and aerospace sectors.
- Geopolitically motivated hacktivist groups continue to target the defense industrial base, space agencies, and other government organizations for their support to international entities.
- Initial access brokers such as DARK_ALPHA have offered the sale of sensitive files related to aerospace and defense on the dark web and clear web platforms.
- An international space agency disclosed that they had been impacted by an undisclosed cyber event, which prompted the organization to disconnect their network from the internet.
- An international aviation agency with ties to space partnerships confirmed a suspected breach of their recruitment database, which involved the unauthorized disclosure of application data records.
- Reports identified a series of infections tied to information stealing malware (infostealers) present in defense industrial base organizations.
- A new threat actor identified as ‘UNK_CraftyCamel’ was attributed to a campaign that targeted aviation, satellite communication, and critical transportation organizations in the UAE.
- Researchers identified a large-scale phishing infrastructure that targeted defense and aerospace entities linked to the Russia-Ukraine conflict.
- Cybercriminals are helping facilitate state-sponsored espionage campaigns through shared use of tools and infrastructure.

2. Supply Chain/Finance: Threat actors routinely target supply chain dependencies via the exploitation of commonly used enterprise software and edge devices to facilitate malicious cyber activities. Downstream vendors and solutions providers are often high-profile targets in widespread cyber campaigns. Recent examples of this activity are as follows:

- The nation-state actor Salt Typhoon was attributed to exploitation of unpatched Cisco network devices associated with telecommunication organizations.
- Large-scale brute-force activity targeted VPNs, firewalls, and SSH services from a variety of DoD-approved vendors in January 2025.
- Adversaries have shown consistent targeting of Ivanti products, underscored by the mass exploitation of Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) vulnerabilities in January 2025.
- An advanced persistent threat (APT) actor was attributed to a campaign that targeted aerospace supply chains via a legacy vulnerability in Check Point security gateways.
- Threat actors exploited CVE-2024-55591 authentication bypass vulnerability in FortiOS and FortiProxy in January 2025.
- According to US cybersecurity officials, threat actors are beginning to chain together multiple zero-day vulnerabilities to gain initial access, conduct remote execution, obtain credentials, and implant webshells on victim networks.
- The Ghost (Cring) Ransomware exploited legacy vulnerabilities in multiple prominent software vendors in recent campaigns.

3. Development and Production: The space sector features robust development environments that often contain highly valuable and sensitive information. Threat actors are expanding their tactics, techniques, and procedures to better infiltrate these environments through living off the land techniques and the use of legitimate services. Recent examples of this activity are as follows:

- Threat actors are conducting widespread malware distribution via open-source code repositories such as GitHub.
- North Korean threat actors leveraging fraudulent IT employment to conduct espionage, fraud, and generate revenue. This activity targets US technology and defense companies.
- “Codefinger” Ransomware tactic encrypts AWS simple storage service (S3) Buckets with server-side encryption with customer provided keys (SSE-C).
- AI malware masquerading as DeepSeek packages were distributed to developers via the Python Package index (PyPi).
- New cyber threat groups emerge focused on targeting operational technology (OT), in addition to increased ransomware threats targeting manufacturing and production.
- Researchers discovered a campaign that uses fake GitHub repositories to distribute malware loaders that deliver malicious payloads such as infostealers.

4. Launch, Landing, and Recovery: Launch segment operations encompass a dynamic space environment from terrestrial based challenges impacting launch operations to strategically important and often highly sensitive payloads being launched into orbit from adversarial nations. Recent examples of this activity are as follows:

- China has conducted 17 orbital launches in 2025, far outpacing 2024 rates with a majority being designated as 'Government / Top Secret' destined for the Geostationary (GEO) belt.
- China continues to expand their footprint in Low Earth Orbit (LEO) with their Thousand Sails constellation.
- Satellites under the TJS family line have been launched the most frequently from China, indicating the enhancement of on-orbit military support vehicles.
- Russia has conducted four orbital launches in 2025, currently behind 2024 rates. The disparity could stem from the fact that Russia has focused on launching multiple payloads per launch, primarily concerning 'Government / Top Secret' classifications.
- COSMOS 2581, 2582, and 2583 launched via Russia have generated the greatest cause for concern regarding dual-mission purposes.
- Both nations have placed satellites into unusual orbital slots in the respective LEO and GEO belts in conjunction with obfuscated mission operations.
- Uncontrolled space debris reentries pose critical concern to commercial aviation operations with over 2,300 rocket bodies currently set to reenter uncontrolled in the coming years.
- Due to the proliferation in global orbital launches, incidents of rocket body break events have generated concern and airspace closures across multiple nations.

5. Critical Infrastructure Protection: Critical infrastructure protection displays a dynamic hybrid warfare environment from the physical destruction of subsea cables to the routine cyber targeting of government infrastructure, telecommunications, and global political / military actions with implications for the space sector. Recent examples of this activity are as follows:

- Seven subsea cables were damaged in Q1 2025 concentrated in the Red Sea, Baltic Sea, and Taiwan Strait. These disruptions pose impacts to global communications infrastructure and underscore the current risk posture for terrestrial infrastructure.
- The Peace subsea cable was damaged in the Red Sea due to unknown reasons.
- The C-Lion1 subsea cable in the Baltic Sea was damaged for the third time in four months.
- The Trans-Pacific Express subsea cable is being investigated due to possible sabotage from a Chinese linked cargo ship.
- Chinese attributed Advanced Persistent Threat Actor Aquatic Panda conducted 'Operation FishMedley', targeting critical infrastructure organizations globally.
- Ransomware as a Service (RaaS) operators continue to target critical infrastructure sectors, including Medusa Ransomware which targeted over 300 critical infrastructure organizations since 2021.
- Government agencies are reporting increased threats to telecommunications firms, following the Salt Typhoon attacks that began in late 2024.

6. Space System Operations: The link segment is routinely under disruption from Global Navigation Satellite System (GNSS) interference, jamming, and spoofing impacting aviation and maritime 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:

- Global Navigation Satellite System (GNSS) interference routinely coincides with large scale and low-level geopolitical events.
- Multiple United Nations agencies have released a joint statement regarding protection of GNSS and Radio Navigation Satellite Systems against harmful interference.
- The greater Baltic Sea area and adjacent Flight Information regions are commonly identified as high interference corridors. Moreover, The International Air Transport Association identified a 500% increase in GPS Spoofing in 2024.
- Global subsea cable disruption events overlap with heightened levels of GNSS interference and nefarious manipulations of Automatic Identification System broadcasting.
- There has been one incident capture of a ship running ashore in the Baltic Sea due to GNSS interference.
- Radio Frequency spoofing is commonly reported at higher rates than jamming, indicating a possible connection to military operations, thus displaying a dynamic hybrid warfare environment and driven by the presence of geo-fencing.
- The greater Red Sea / Strait of Hormuz area has recently seen a slight increase in GNSS interference in conjunction with an uptick in Houthi Rebel operations.
- There have been five unique instances of flights aborting landing, commonly citing a variety of anomalies to navigation services. On one occasion, a flight crash landed due to a multitude of events with the noted presence of GNSS interference.
- Russia has maneuvered satellites on 77 occasions across 13 satellites.
- China has maneuvered satellites on 53 occasions across 25 satellites.

7. Space Environment: The orbital environment remains highly congested and dynamic, due to the continued proliferation of space assets and increased space weather events. This highly contested environment is further enumerated by the overcrowding of low earth orbit satellites and space debris objects derived from on-orbit breakups. These events contribute to satellite concerns in low earth orbit and continue to be a key factor in the safe and sustainable operation of space assets. Recent examples of this activity are as follows:

- Since 1 Jan ‘25, there have been 21x notices of significant geomagnetic activity. These notices fall within acceptable limits dictated by global space weather agencies but have been impactful to multi-Global Navigation Satellite System (GNSS) noise levels to date as a result.
- Although the space environment during this solar max cycle has been dynamic, some maneuvers across classical orbits are still not commensurate with basic station keeping measures.
- The number and diversity of commercial satellites across Low Earth Orbit (LEO) plus the proliferation of their constellations is driving density, collision avoidance and added orbital drag concerns.

- Technological and disruptive advancements led to surges in satellite market diversity to include viable integrations across constellations via aggregations in Earth Observation & Sensing technologies.
- Several high-resolution satellites and constellation payloads have been launched since the beginning of the year constituting an increase primarily in Earth Observation technologies to include some radar calibration capabilities bolstered by Artificial Intelligence and edge capabilities.
- Upticks in impressed space weather energy have led to reports of signal attenuation and scintillation across lower bands up into satellite GNSS downlink frequencies.
- Several solar flare emissions, upticks in electron High Speed Streams (HSS) from expanding Coronal Holes and Coronal Mass Ejections (CMEs) during the first quarter of 2025 alone, have generated radio blackouts across 3 continents and were key to Position, Navigation and Timing (PNT) errors.
- The number of satellites in a state of decay messages via publicly available captures fluctuated from 513 on 8 Jan ‘25 to 341 by end of Mar ‘25, at times correlating with space weather energy onsets.