Space ISAC Q1 2026 Public Report

TLP CLEAR: Released: 04/08/2026

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 2026 (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 threat landscape for space centers around known impacts to ground and link segments, alongside burgeoning irregular impacts to on-orbit assets and hybrid architectures. This evolving attack surface for space forecasts increased threats, driven by evolving adversary capabilities and shaped by geopolitical conflicts.

1. Terrestrial Cyber Operations: The global space sector experienced a significant uptick in reported cyberattacks, influenced heavily by conflicts in the Middle East. Throughout the first quarter of 2026, open-source reporting identified 46 attacks that targeted organizations operating in the space and aerospace sectors, which is a 30% increase compared to the same timeframe in 2025. While attribution of these attacks remains uncertain, they emphasize the growing sentiment among adversaries that the space sector is a viable target for financial gain and political credibility, and notoriety. Recent examples of this activity include:

- In January 2026, a threat actor group named Sentap claimed multiple attacks against US defense contractors, including the leak of a satellite project dataset and a coordinated infostealer campaign.
- An initial access broker claimed to have access to data from an official government server pertaining to projects related to teleradiology imaging.
- In January 2026, the European Space Agency (ESA) publicly disclosed a cybersecurity incident, which was attributed to threat actor groups *888* and *ScatteredLapsus$Hunters*.
- Threat actors continue to leverage a critical vulnerability in React Server Components, called React2Shell. CVE-2025-55182 was initially exploited in late 2025 and continues to be leveraged in 2026.
- The *NightSpire* ransomware group claimed to have exfiltrated sensitive, unclassified U.S. government data via the compromise of a trusted vendor.
- The Konni (aka Opal Sleet) APT group was observed adopting AI to generate PowerShell backdoors, underscoring the evolving tactics of DPRK-affiliated actors.
- Pro-Iranian groups Handala Hack and APT Iran claimed multiple disruptive attacks against defense targets following coordinated strikes from Israel and the U.S. on February 28.
- Reporting from security firm CyberShelter identified a sophisticated cyber-espionage campaign targeting the UAE's aerospace, defense, and government sectors, attributed to APT33.
- A threat actor tracked as *Mobir* claimed an attacks against multiple UAE aerospace organizations, gaining access to target systems and using wiper malware to destroy data.
- Extortion groups such as *ShinyHunters* continue to target cloud platforms for data theft via exploitation of third-party Software-as-a-Service (SaaS) integrations.

2. Supply Chain/Finance: Software and hardware supply chains are increasingly being targeted by threat actors. Vulnerabilities in widely used and trusted platforms are being exploited. Campaigns specifically targeting the supply chain represent the risk to space and related sectors. These activities underscore the impact compromise of suppliers and providers can have across support infrastructures. Recent examples of this activity are as follows:

- China-linked threat actors exploit three vulnerabilities in VMware ESXi, Workstation, and Fusion products that can cause code execution and information disclosure.
- North Korean-sponsored APT *PurpleBravo* targeted IT software supply chain in North Korean IT worker campaign.
- Threat actor group *TeamPCP* compromised Trivy through the platform's GitHub Actions, leading to a supply chain attack compromising at least four platforms.
- Cisco Secure Firewall Management Center remote code execution (RCE) vulnerability (CVE-2026-20131) exploited by *Interlock Ransomware* in campaign targeting enterprise firewalls.
- An independent security researcher discovered over 20 vulnerabilities in International Datacasting (IDC) SFX2100 satellite receivers.
- Semiconductor manufacturer, Trio-Tech International's Singapore subsidiary hit by ransomware attack, claimed by Gunra Ransomware.
- AWS Console supply chain vulnerability *CodeBreach* presented risk of platform-wide compromise if exploited.
- Cisco SD-WAN Manager vulnerabilities (CVE-2026-20127, CVE-2026-20128, CVE-2026-20122) exploited in various regions with highest activity of exploitation observed in the United States.
- Threat actors compromised a legitimate developer's resources in Open VSX, leading to supply chain attack pushing malicious updates to downstream users.

3. Development and Production: Adversaries are increasingly evolving their tactics for initial access and execution, implementing more methods for defense evasion and persistence, to gain access to high-value development environments. These TTPs often involve exploitation of trusted relationships, abuse of legitimate tools, and compromise of open-source libraries and code repositories. These TTPs combine elements of Living-off-the-Land (LOTL) and supply chain attacks to exploit dependencies in CI/CD. Recent examples of this activity are as follows:

- Cisco Talos identified increased targeting from a suspected China-nexus actor UAT-8837 involving exploitation of a zero-day vulnerability in SiteCore platforms.
- Researchers discovered a new cloud-focused malware framework named VoidLink, which was developed almost entirely by AI toolkits.
- A denial-of-service (DoS) risk associated with Microsoft Azure Private Endpoint and Private DNS architecture was uncovered by researchers in late January 2026.
- The Shai-Hulud npm supply chain attack continued to proliferate in scale throughout 2026, compromising over 700 packages and 25,000 repositories following the discovery of a new strain.
- Threat actors employed ransomware against over 3,000 unprotected instances of the database management system (DBMS) MongoDB in a broad campaign.

- Researchers uncovered multiple attack vectors in GitHub code Codespaces to exploit unprotected VS Code instances.
- Multiple members reported malicious use of Microsoft Graph API to facilitate intrusion activity across Microsoft 365 and Azure environments, underscoring the use of Living-off-the-Land (LOTL) tactics.
- The Iran-nexus group SeedWorm (aka MuddyWater) was attributed to the compromise of a US.S.-based defense and aerospace software provider.
- Researchers identified new developments in the toolkits of North Korea-linked APT37, enhancing the group's ability to compromise air-gapped networks.

4. Launch, Landing, and Recovery: Launch segment operations encompass a dynamic space environment that includes multiple launch failures, cybersecurity hardening for the launch segment, and payloads of interest being launched. Recent examples of this activity are as follows:

- China, India, and Japan have all experienced launch failures in 2026. Additionally, multiple companies have experienced launch failures or aborted launches due to 'anomalies.'
- Launch failures for Japan have cascading impacts to the nation's ability to expand sovereign launch capabilities and decrease overall reliance on other nations for launch activities.
- China ceased launch operations for nearly one month following back-to-back launch failures.
- The U.S. Space Force has established two Defensive Cyber Operations Squadrons to protect launch operations from cyber threats.
- Russia launched a satellite for Iran that drew little attention, with multiple open-source reporting indicating that the satellite could possibly be holding a slot on-orbit for a future Russian satellite.
- A rocket body tracked as 'Zhuque-3' highlighted the dangers posed by uncontrolled reentries as its reentry time and date fluctuated until mere hours before official reentry occurred.
- The Space Force has halted forthcoming launches involving the Vulcan rocket due to a 'significant performance anomaly', thus delaying mission critical launched by multiple months.
- Russia has launched the first batch of satellites for their Starlink rival constellation known as 'Rassvet' with 900 total satellites planned by 2035.
- The reentry environment remains dense, with over 20+ trackable and confirmed reentries per week culminating rocket bodies, debris, and defunct payloads.
- Poland launched their second & third military satellites. Additionally, Sweden opened the Esrange Space Center to military launches indicating nations continued evolution towards on-orbit defenses.

5. Critical Infrastructure Protection: Critical infrastructure protection displays a dynamic hybrid warfare environment from the physical destruction of satellite related infrastructure to the increasing reliance on drones. Additional consideration is given to space-based data center talks and repeated cyberattacks against multiple critical infrastructure sectors.

Recent examples of this activity are as follows:

- Iran has threatened to cut subsea cables amidst the ongoing conflict in the Middle East.
- On multiple occasions, satellite terminals, radars, domes, teleports, and aerospace headquarters have been targeted and destroyed across the Middle East.

- The U.S. and China have emerged as global leaders in space-based data center computing, thus potentially altering the threat landscape over the coming years.
- Iran is reportedly utilizing 'satellite' like launches to double their missile range from 2,000 kilometers to 4,000 kilometers.
- According to a report from the U.S. Government Accountability Office, nation-state adversaries have repeatedly targeted contractor networks to gain access to sensitive defense information.
- Germany recently committed €35 billion ($41 billion) towards sovereign military space capabilities, signaling a departure from purely defensive posturing due to growing threats.
- Evidence points towards increased collaboration between Iran and Russia to bolster drone technology and outfit them with anti-jamming technology.
- Iran has begun seizing portable Starlink terminals in an effort to suppress internet access across the country.
- The Federal Communications Commission has warned the telecommunications sector to elevate cybersecurity hygiene due to the growing number of ransomware victims.
- Researchers have mapped 130 real-world cyber techniques utilized by five Iranian threat groups against NIST SP 800-171 to better understand how prepared the Defense Industrial Base is.

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:

- Iran has been identified jamming mobile Starlink Terminals across the entire country, indicating a much larger and possibly coordinated campaign against internet suppression.
- Multiple Iranian State TV channels were subject to satellite disruption to telecommunication services
- A Russian Telegram account released satellite images of what appear to be two Tiran-2S systems, generating speculation that Russian-made EW systems may have been utilized in early January.
- Multiple Pakistani and Iranian telecommunications channels (and associated satellites) have been subject to 'signal hijacking' attacks to display propaganda.
- Characteristics concurrent with Position, Navigation, and Timing Geofencing have been observed via irregular maritime vessel patterns near the Strait of Hormuz.
- Two Chinese nationals were charged with installing miscellaneous satellite equipment (dishes and computers) atop buildings in France for possible satellite signal reception exploitation operations.
- Three Russian satellites in Low Earth Orbit have engaged in Rendezvous & Proximity Operations, similar to maneuvers identified nearly one year ago that were described as 'dogfighting' maneuvers on-orbit.
- A Russian satellite tracked as Luch Olymp 2 has been observed conducting Rendezvous & Proximity Operations ranging from 10 – 50 kilometers away from a U.S. communications satellite.
- The International Air Transport Association's (IATA) 2025 Annual Safety Report goes on to highlight the dangers, risks, and mitigation measures across multiple flight corridors globally.
- A Chinese commercial satellite has completed a refueling test in low Earth orbit using a flexible "octopus tentacle" robotic arm.

7. Space Environment: Space environmental impacts and activity have remained overall low entering the first quarter of 2026, with isolated G1 to G3 geomagnetic watches that slightly materialized into a few notable impacts. Kp indices remained in a state of flux although on the lower end of the scale up until the third week in March indicating a heightened risk to satellite operations and triggering minor surface and internal charging observations. Recent examples of this activity are as follows:

- The bulk of Geomagnetic watches put forth in the first quarter ranged from G1 (Minor) to G2 (Moderate) levels with a G3 (Strong) potential put forth in later March 2026.
- Several common surface charging longitudes in Geostationary Orbit (GEO) as called out via public reporting were indicated as 40°E–180°E, 90º West – 150º East, and several others. The potential for surface charging and differential charging depending on satellite conductivity was therefore present.
- G3 (Strong) level watches were published as indicated above later in March 2026 and came about after an uptick in solar flare activities, and electron flux variations driving ionospheric Total Electron Content (TEC) changes although those remained on the lower scale.
- Solar active regions and flare activity continued to remain low, although on or about 13 March 2026 at or about 20:23 UTC, a large flare (C8.9 - SIDC Flare 7187) was observed as dispatching from NOAA Action Region 4392 on the solar face.
- Although coronal hole based high speed streams vary, on several occasions this quarter there were “under the influence” call outs mainly associated with positive polarity stream arrivals. Speeds ranged from normal & quiet (300-400 km/s) to 700 km/s which are capable of geomagnetic storm potentials.
- During the 18-21 January window, there were multi-day impacts brought about by an X1.9 solar flare eruption and coronal mass ejection (CME) combination which brought about radio blackout conditions within the Arctic Region across radio shortwave frequency spectrums.
- Within the February to March 2026 timeframe, several different and independent atmospheric scientists published the first direct observational proof linking a specific spacecraft re-entry event to detectable chemical pollution in the mesosphere and stratosphere. The Leibniz Institute for Atmospheric Physics in Germany reported that a high-resolution Light Detection & Ranging (LiDAR) system detected a sudden spike in metallic vapor at ~ 95 km altitude linked to a Falcon 9 rocket upper stage reentering uncontrolled several weeks earlier by tracking atmospheric lithium exchanges.
- Based on the European Union Space Surveillance and Tracking (EU SST) dashboard across the first quarter, there have been ~ 46 total reentries versus 23 from the previous quarter. Most of them were payloads with the worst week being denoted as being on and around 19 February.
- With the proliferation of satellites in Low Earth Orbit (LEO) and collision risk escalation on the rise, the Outer Space Institute recently (as of 20 March 2026) updated their Crash Clock based on community and owner operator feedback. This downward adjustment from 3.8 to 3 days is based on a fundamental question: What is the expected time for a potential collision in LEO between tracked artificial objects, satellites, debris and abandoned rocket bodies if all maneuvers were to stop?