



Space ISAC Q2 2026 Public Report

TLP CLEAR: Released: 07/09/2026

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 Q2 2026 (01 April – 30 June)

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: Space, Aerospace, and Defense sectors continue to face a consistent level of cyberattacks perpetrated by a variety of threat actors. Throughout Q2 2026, open-source reporting identified 40 attacks that targeted organizations operating in the space and aerospace sectors, consistent with Q1 2026 attack volumes. While attribution of these attacks remains largely uncertain, they emphasize the growing sentiment among adversaries that the space sector is a valuable target for financial gain and espionage. Recent examples of this activity include:

- In April 2026, researchers released an analysis of TTPs associated with the Iranian APT-C-13 (Sandworm), highlighting their use of persistent intrusion methods and SSH tunneling.
- Multiple initial access brokers claimed data breaches against spacecraft operators and international space agencies throughout May – June 2026.
- From April – June 2026, multiple security firms and government agencies reported activity associated with the Scattered Lapsus\$ Hunters (SLSH) group, emphasizing the impact of their attacks.
- Reporting identified a campaign targeting Eurasian aerospace sector tracked as *Operation Silent Rotor*.
- A new Chinese-nexus threat actor *UAT-8302* was discovered leveraging multiple malware toolkits in attacks against government entities throughout South America and Southeastern Europe.
- Researchers published an analysis of recent espionage campaigns attributed to the *Iranian Dream Job* (aka: Screening Serpens) cluster targeting global aerospace firms.
- A new espionage campaign was disclosed targeting secure equipment access Linux-based edge routers.
- Researchers reported new activity associated with the *PCPJack* campaign, targeting cloud resources across major providers.
- A Russian-speaking forum user advertised an alleged decryption tool for a global satellite provider.
- There were 19 total distributed denial of service (DDoS) attacks claimed against space-sector entities, claimed by pro-Russian and Pro-Iranian groups.
- The Iran-nexus APT Nimbus Manticore expanded its operation to include malware operations and sideloaded infection chains.



2. Supply Chain/Finance: Software and hardware supply chains are increasingly being targeted by threat actors and represent a prominent risk for the commercial space sector. Exploitation campaigns are conducted predominantly by targeting known vulnerabilities in widely used platforms or via trusted software libraries procured from public sites. These activities underscore the impact of compromised suppliers and amplify identity and trust concerns in integrated applications. Recent examples of this activity are as follows:

- Threat actors are prioritizing mass exploitation of known exploited vulnerabilities in widely used edge devices such as Palo Alto PAN-OS and Cisco SD-WAN.
- Researchers disclosed multiple vulnerabilities in Citrix NetScaler devices related to insufficient input validation and memory overflows, potentially leading to denial of service (DoS) conditions.
- A Microsoft insider threat going by the alias *Nightmare Eclipse* leaked multiple zero-day vulnerabilities in Windows OS, leading to reported exploitation.
- Researchers attributed the Axios supply chain campaign to a North Korean group tracked as *UNC1069*.
- *Storm-1175* actors deployed medusa ransomware at high operational tempo via multiple vulnerabilities in Microsoft Exchange, CrushFTP, and JetBrains' TeamCity platforms.
- Attackers compromised a legitimate vulnerability scanner *Trivy* with infostealer malware in a purported supply chain attack.
- Researchers identified significant exposure of space and defense industrial base to foreign-owned suppliers, manufacturers, and upstream dependencies.
- Secure Equipment Access (SEA) Linux-based Edge Routers were targeted by a *Cobalt Strike*-related espionage campaign.
- Threat actors increased targeting of popular AI libraries via abuse of trusted platform *HuggingFace*.
- Over 70,000 FortiGate devices were discovered to be exposed to scanning and exploitation in a broad campaign tracked as *FortiBleed*.

3. Development and Production: Targeting of development environments continues to rise as adversaries evolve their tactics, techniques, and procedures (TTPs), indicating the threat to developers, their environments, and the dependencies they rely on. Furthermore, vulnerabilities to critical systems emphasize the risk of exploitation by adversaries. Recent examples of this include:

- The Operational Technology ISAC identified multiple critical vulnerabilities impacting operational technology systems.
- Reporting suggested the risk of adversaries leveraging Artificial Intelligence (AI) to exploit Application Programming Interfaces (APIs).
- Cloud infrastructure provider, *Vercel*, faced with data breach leading to exfiltration of customer account OAuth tokens.
- *Contagious Interview* and *DPRK IT Worker* threat evolved to self-propagating model infecting code repositories.
- The Australian Security Intelligence Organisation (ASIO) attributed the DPRK and PRC to a dual-state-sponsored threat dynamic to Australian sectors.



- In June 2026, the *Miasma* worm targeted Node Packet Manager (npm) packages across multiple platforms in credential theft campaign.
- Forgotten trust relationship vulnerabilities were discovered impacting OpenID Connect federation models in *GitHub Actions*, *GitLab CI*, and *Terraform Cloud*.
- Researchers observed a notable rise in *Node Packet Manager (npm)* packages targeted in supply chain attacks throughout 2026 indicating an elevated risk to code repositories.
- Threat actors exploited vulnerabilities in *Lantronix* Serial-to-IP converts, leading to potential impacts of Denial-of-Service (DoS), lateral movement, and data tampering.
- *Nimbus Manticore*, Iranian-sponsored threat actor, evolves targeting of critical sectors in dual approach operations with use of AI-assisted malware.

4. Launch, Landing, and Recovery: The launch segment is best characterized by a high pace launch environment, launch failures both in-orbit and at the terrestrial layer generating debris reentry concerns, and payloads being launched into unusual orbits. Recent examples of this activity are as follows:

- Blue Origin's New Glenn rocket suffered an undisclosed failure in May and placed a satellite into an "off-nominal" orbit in April.
- *Space Pioneer* conducted the maiden flight of the *Tianlong-3* launch vehicle that ultimately ended in failure.
- A commercial firm has demonstrated the ability for their reusable launch system to surpass Mach 4 speeds for suborbital missions.
- *Shijian 31* was launched into an unusual *Molniya* orbit exhibiting characteristics of 63.4° inclination, Argument of Perigee of approximately 171°.
- One recently launched Russian satellite composing their *Rassvet* constellation reentered 75 days after launch due to unknown reasons.
- *Bill C-28* has been proposed in Canada, and, if enacted, would establish a federal legislative framework for space launch and re-entry activities in Canada.
- Reporting indicates growing concern related to atmospheric effects of rocket launches and uncontrolled reentries due to advancements in rocket body technology that may survive reentries.
- NASA's launch facilities will likely reach capacity by the end of the decade as the number of commercial launches continues to skyrocket as launch cadence rises to reach 268 in 2030—up from 109 in 2025.
- The FAA has required *SpaceX* to complete a mishap investigation into a failed *Starship-Super* heavy rocket flight before launches of the rocket body line can resume.
- Multiple countries are either launching satellites for the first time, or operating space centers supporting launch activities within their respective nation, indicating a growing presence for on-orbit capabilities.



5. Critical Infrastructure Protection: Adversaries continue to target critical infrastructure, posing both direct and indirect impacts to space systems. This includes impacts to systems that provide supporting services for space systems (e.g., ground stations) and infrastructure that is directly supported by satellite services (e.g., GNSS receivers). This class of critical infrastructure is uniquely impacted by physical threats, alongside more sophisticated brands of cyber activity that seek to extend to physical threats.

Recent examples of this activity are as follows:

- Security researchers warn that Iranian hackers are targeting US critical infrastructure through cybercriminal and ransomware proxies.
- Open-source researchers *InformNapalm* reported a joint cyber operation targeting the Russian Gonets satellite system.
- Cybersecurity researchers discover a previously undocumented data wiper known as *Lotus Wiper* in attacks on energy systems.
- In May 2026, Taiwanese authorities attributed an April disruption of their high-speed rail system to a compromise of the TETRA interface.
- Use of Starlink terminals on drones and oil tankers by both Russia and Ukraine spark concerns over use of commercial satellite services.
- Polish security officials warned of cyberattacks shifting from espionage and data theft toward physical disruption of critical infrastructure.
- The FBI and intl agencies released an advisory stating that Chinese military intelligence services are using a wide array of recruitment platforms to target FVEY government and military personnel.
- Iran's Ministry of Intelligence (MOIS) extends Handala operations against critical infrastructure to include threats of physical attacks.
- Ukraine launches kinetic attack on Russia's largest satellite teleport, the Dubna Communications Center, following strike on Russian satellite and radar R&D facility in May 2026.
- Russian, Iranian, and Chinese state-sponsored hackers continue to conduct attacks against water regulation systems via weak passwords and exposed PLCs.

6. Space System Operations: The link segment is routinely under disruption from Global Navigation Satellite System (GNSS) interference, jamming, and spoofing impacting the GPS L1 (1575.42 MHz) band. 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:

- GPS signal interference testing near White Sands Missile Range in the United States impacted the GPS L1 band across a two weeklong time frame.
- According to reporting, a Royal Air Force (RAF) jet encountered GNSS signal jamming near Russian territory, marking the second reported time a RAF jet experienced similar jamming since 2024 near Russian territory.
- Recent reporting indicates that multiple GNSS interference events between 2019 – 2026 impacted the GPS L1 band, attributed to a satellite from the Russian *Edinaya Kosmicheskaya Sistema* constellation.



- Recent reporting indicates that Russia has rejuvenated their electronic warfare (EW) platform known as Volna Kupol Garant capable of jamming the 14-14.5 GHz band.
- Daily Position, Navigation, and Timing reporting provided by the JCO indicate consistent low-medium grade interference globally, with degraded GNSS values ranging from 30% - 100% in some areas.
- Russian satellite COSMOS 2589 and United States satellite USA 325 have routine photometric changes with lighting conditions favoring USA 325 in the Geostationary belt.
- Chinese spacecraft SJ-29A & SJ-29B have performed multiple close approach maneuvers under 32 kilometers with confirmation of Rendezvous & Proximity Operations.
- Multiple Russian satellites have remained either co-planar or in the neighborhood of two ICEYE satellites operating in Low Earth Orbit.
- Two Russian satellites came within ~3 meters of one another, citing growing concerns regarding testing of on-orbit capabilities.
- Norway has announced plans to place additional monitoring stations for GNSS interference levels.

7. Space Environment: Space environmental impacts and activity continue to be persistent with notable Radio Blackout and Geomagnetic storming conditions multiple times per month. Additional consideration is given to space debris events, or the potential for these events to occur. Recent examples of this activity are as follows:

- Between 05 – 10 May there were pockets of elevated activity consisting of Radio Blackout and Geomagnetic storming conditions of the moderate level.
- Between 03 – 04 June, Geomagnetic and Radio Blackout conditions reached the Strong levels, with impacts consisting of degraded HF propagation and GPS L1 range errors moderately depressed.
- China's Zhuque-2E rocket body suffered a breakup in Low Earth Orbit possibly generating 100 - 150 pieces of debris.
- China's Qianfan low earth orbit mega constellation has 87/200 satellites in operational altitudes, thus signaling that enhanced awareness and caution should be exhibited due to unknown operational capacity of these satellites.
- The Defense Advanced Research Projects Agency (DARPA) has solicited a Request for Information regarding technologies and operational concepts to allow the reconstitution of space assets damaged or destroyed by adversaries, or on-orbit accidents.
- The American Institute of Aeronautics and Astronautics has published version 3.0 of the "*Orbital Safety Best Practices for Satellite Operators*" setting technical baselines due to the high probability of collision avoidance maneuvers.
- China has abandoned a total of 96 rocket bodies in Low Earth Orbit, predominately at altitudes above 800 kilometers, thus generating concern due to long term debris, possible collisions, and possible explosions related to defunct payloads.
- Research has identified that if all satellites in orbit lost the ability to maneuver, it would just roughly 2.5 days before collisions begin to occur, down from 164 days in 2018.
- Once sunspot numbers climb past roughly two-thirds to three-quarters of a cycle's peak, debris in low Earth orbit can begin losing altitude much faster as the drag environment becomes harder to mitigate.
- A commercial company has demonstrated the ability to send an Earth-Moon-Earth (EME), or moon bounce, communications method to send radio signals from the Earth's surface to the Moon and back.