Space ISAC Q3 2025 Public Report

TLP CLEAR: Released: 10/06/2025

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 July – 30 September)

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 militarization of space. The threat landscape for space forecasts increased threats, precipitated by geopolitical and economic factors and underscored by sophisticated campaigns.

1. Terrestrial Cyber Operations: Throughout Q3 2025, the commercial space sector was subject to an increased number of cyberattacks, driven by escalations in geopolitical tensions. These attacks included mostly disruptive attacks such as distributed denial of service (DDoS), web defacement, and theft of publicly available information. Beneath this noise however, multiple sophisticated campaigns were reported that targeted the space industry and its various subsectors, alongside a noted shift from adversaries toward western communications firms. Recent examples of this activity are as follows:

- Middle Eastern and US-based aerospace firms saw an increase in geopolitically-motivated cyber targeting following the escalation of conflicts between Israel and Iran.
- A pro-Iranian group known as “Cyber Insaad Front” claimed cyberattacks against satellite control segments of multiple Israeli companies.
- Pro-Palestinian hacktivist group GhostSec claimed to have disrupted 10 Israeli VSAT systems.
- Newly reported information on the China-nexus threat actor Salt Typhoon confirmed that they targeted a US satellite communications provider as part of broader operations against US telecos.
- Cybercriminal groups LAPSUS$, ShinyHuters, and Scattered Spider extend cyber operations beyond retail into aviation and other space-related sectors.
- Researchers reported a new campaign attributed to UNG0901 called *Operation Cargo Talon* that targeted Russian aerospace and defense sectors via highly targeted spear-phishing lures.
- A threat actor known as “Lab Dookhtegan” purportedly conducted multiple campaigns targeting satellite software support maritime VSAT infrastructure.
- Reporting indicates that the Iranian APT group UNC159 (Subtle Snail) targeted European telecom, aerospace, and defense organizations with a tailored malware payload known as MINIBIKE.
- A separate Iranian cyber threat cluster known as Nimbus Manticore has expanded its interest in European targets in telecommunications, defense, aerospace, and satellite sectors.
- Reports of a recent cyber espionage campaign indicate a new China-nexus APT group tracked as *RedNovember* has extended its operations to aerospace, defense, and space organizations.

2. Supply Chain/Finance: Dependencies in software supply chains remain a critical entry point for threats to the space industry. These risks are underscored by widely exploited vulnerabilities in edge devices and ubiquitous services, as threat groups decrease the time to weaponize exploits post disclosure. Recent examples of this activity are as follows:

- Multiple China-aligned threat actor groups (UNK)FistBump, UNK_DropPitch, and UNK_SparkyCarp were observed targeting the Taiwan semiconductor industry from March – June 2025.
- Vulnerabilities in Citrix NetScaler ADC and Gateway devices have been subject to widespread exploit activity attributed to multiple threat actor groups.
- Microsoft reported a wave of attacks against on-premises SharePoint instances via a bypass of previously patched vulnerabilities known as *ToolShell*
- FBI and Cisco Talos attributed Russian state-sponsored cyber actors to exploitation of Cisco devices.
- Researchers disclosed new exploit activity related to CVE-2025-31324 in SAP NetWeaver leading to the deployment of a linux-based malware known as Auto Color.
- Threat actors continue to target a remote code execution vulnerability in the GeoServer application, leading to multiple compromises in the wild, including a US federal agency.
- The Akira ransomware group exploited a legacy vulnerability in SonicWall firewalls in a new wave of attacks, combining attack vectors for initial access.
- Two new vulnerabilities in Cisco ASA and FTD Software and VPN Web Server have been exploited by a suspected nation state actor with ties to the previously disclosed Arcane Door campaign.

3. Development and Production: Recent APT campaigns underscore growing interest in the space sector and adjacent industries, driven by the value of designs, operations, and supply chain access to foreign intelligence entities. Key TTPs include abuse of legitimate services for obfuscation and targeting of open-source frameworks. Recent examples of this activity are as follows:

- Threat actors are conducting widespread malware distribution via open-source code repositories such as GitHub and NPM.
- Adversaries from both Iran and North Korea continue to utilize TTPs associated with the “Dream Job” operation, which include impersonating HR representatives and recruiters.
- Researchers continue to uncover novel AI-powered malware samples that range from ransomware toolkits to fully functional command-and-control (C2) platforms.
- CrowdStrike reported new activity from *MURKY PANDA*, a Chinese-backed group who routinely targets cloud environments via trusted-relationships for information harvesting.
- Multiple threat actors including *UNC6040* and *UNC6395* were attributed to targeting of Salesforce instances via the compromise of third part Salesolft drift integration.
- The U.S., Japan, and the Republic of Korea (ROK) issued a joint statement and new advisories warning businesses and the public about the persistent threat posed by North Korean IT workers.
- Researchers identified over 187 compromised NPM packages as part of a supply chain attack delivering a wormable malware known as *Shai-Hulud*

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 the expansions of mega-constellation projects. Recent examples of this activity are as follows:

- China has conducted 18 orbital launches in Q3 2025, remaining on pace to have their most launches in the nation's history.
- China has put increased focus on their Low Earth Orbit mega-constellations by rapidly increasing launch rates.
- Iran and Russia have routinely collaborated on launch missions with one another, bolstering each nations launch capabilities.
- Iran has announced plans for the maiden launch of its first satellite constellation, which has coincided with the nation routinely testing rocket body launch capabilities.
- While Russia's launch activity has slowed, there is a continued focus on military related payloads under their 'KOSMOS' constellation.
- Russia is eyeing a Low Earth Orbit mega-constellation project to rival other nations which showcases the global expansion and posturing into Low Earth Orbit and Very Low Earth Orbit.
- Multiple commercial providers continue to experience launch malfunctions that generate uncontrolled debris reentry concerns.
- The Philippine Space Agency has cited concerns for rocket debris / space debris from launch activity related to China as this debris has reentered uncontrolled near mainland areas.
- Notice to Air Missions citing 'debris' related to launch activities continue to remain elevated, predominantly impacting the Africa-Indian Ocean region and the Oceanic-Pacific region.
- There have been 86 trackable payloads and 15 trackable rocket bodies reenter during Q3 2025, which have overwhelmingly been uncontrolled reentries. In some cases, these have reentered over mainland populated areas causing concerns across flight information regions globally.

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:

- A Microsoft subsea cable was damaged in the Red Sea with major implications towards Ground Station as a Service providers they rely on low latency Azure cloud services.
- Multiple NATO nations have cited concern regarding Russia activities in relation to subsea cable protection.
- Drone sightings across Europe have generated concern regarding nefarious intelligence, surveillance, and reconnaissance operations in proximity to military and satellite ground station installations.
- On two separate occasions, Very Small Aperture Terminals have been reputedly disrupted, impacting hundreds of maritime vessels related to Iranian logistics operations.

- NATO is investing $728 million in space capabilities while Germany is investing $41 billion in space capabilities.
- The Salesforce Salesloft Data Breach impacted over 700 companies including prominent cybersecurity and IT companies due to reliance on a third-party chat bot application.
- Telecommunications, government, aerospace, manufacturing, and IT remain some of the most targeted and impacted sectors from extensive cyber espionage campaigns.
- An extensive campaign targeting Taiwan's semiconductor industry was identified that occurred between March – June 2025. Taiwan's semiconductor industry remains routinely targeted by Chinese related threat actors.
- Telecommunication entities are routinely targeted to conduct 'signal hijacking' attacks to display propaganda in relation to geopolitical events.
- Network edge devices, cloud environments, and operational technology infrastructure remain routinely targeted components to infiltrate and compromise critical infrastructure sectors.

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:

- Two geostationary satellites known as SJ-25 and SJ-21 have performed an on-orbit refueling mission, marking a historic advancement in China's on-orbit capabilities.
- Both the United States and China have snapped pictures of each other's satellites, displaying an advancement in on-orbit tactics and spacecraft capabilities.
- On multiple occasions in Q3, Russia has launched satellites that have released sub-satellite objects that have demonstrated the capability to maneuver on their own, generating concern.
- Multiple Russian and Chinese satellites routinely conduct Rendezvous & Proximity Operations on-orbit for unknown purposes.
- Multiple Russian and Chinese satellites routinely have close approaches with military and telecommunication satellites external to these nations.
- Multiple commercial aviation flights routinely encounter GNSS disruptions that impact the ability to conduct landing procedures.
- Maritime operators transiting the great Red Sea / Strait of Hormuz areas are routinely reporting GNSS impacts to their respective location, speed, and ability to transit safely.
- Publicly available GNSS jamming and spoofing reports total over 2,000 on a month-to-month basis.
- Russia has maneuvered satellites on 39 occasions across seven satellites.
- China has maneuvered satellites on 74 occasions across 23 satellites.

7. Space Environment: The orbital environment remains highly dynamic, largely due to space weather activity that can impact satellite operations, mission lifespan, and degrade overall performance. Additional consideration is given to space debris generating events on-orbit and governmental investment in space assets. Recent examples of this activity are as follows:

- Geomagnetic G3 (Strong) storms remain some of the more common space weather alerts issued by global space weather agencies.
- There were three significant space weather events between 01 September – 01 October observed at the G3 (Strong) threshold as outlined by global space weather agencies.
- A X1.2 solar flare was released, marking one of the largest solar flares of 2025, bringing strong impacts to communication modalities such as low frequency and high frequency.
- Multiple lower level G1 – G2 (Minor – Moderate) and Radio Blackout R1 – R2 (Minor – Moderate) storm levels were observed throughout Q3 2025.
- The orbital drag environment between the 400 – 900-kilometer range in Low Earth Orbit routinely sees 'danger' levels of drag in excess of 200%.
- Surface Charging elements for geostationary satellites appears to be a more common impact than internal charging when a geomagnetic storm is occurring.
- The United Kingdom Space Agency has devoted £75.6m for cleaning up space debris on-orbit, more precisely to remove defunct satellites.
- A recent study outlines how electrical discharges on a spacecraft directly correlate to the number of electrons in the surrounding environment, better informing spacecraft operators on how to protect satellites from solar storms.
- Multiple nations have begun to announce plans / projects for tackling space debris, generating concerns for possible dual-use purposes on-orbit.
- European countries have begun to invest more in space defense capabilities as well as bolstering space supply chains and production facilities.