Recorded Future®

EXECUTIVE INSIGHTS REPORT | JULY 2025

Space and Cyber: The Race Above and the Battle Below

From Insikt Group®



Summary

"Space Race 2.0" is gaining momentum, fueled by the extraordinary value of resources located on Earth's moon, asteroids in our solar system, and other planetary bodies.

Cyber threat actors are increasingly targeting organizations operating in the space domain. Many of these state-sponsored cyber threat actors are believed to have ties to military units, in part due to the rapid expansion of space commands/forces within militaries.

Space Race 2.0 will become increasingly polarized, with US-led and Chinese-led confederations. This competition will supercharge the 21st-century space race.

Cybersecurity is playing a pivotal role in this race and will continue to do so. Espionage focused on intellectual property theft is expected to help nations gain competitive advantages. The risk of destructive attacks will increase. As a result, the supply chain, in particular, needs to be closely monitored.

Analysis

A new version of the Space Race that began in the twentieth century has emerged as the Fourth Industrial Revolution gains momentum. The demand for minerals, energy, and other resources is a major driving factor. Today, the race is playing out in Earth's orbit, with a growing number of countries launching both commercial and military satellites.

Earth's moon is the next target for space powers. It is believed to hold water ice, valuable minerals, and critically, helium-3, an isotope with potential to be used as fuel for future nuclear fusion reactors, offering a clean, efficient, and transformative energy source. Companies are already planning to harvest it, and lunar bases are being designed to secure and protect the moon's resources.

Asteroids are also incredibly rich in minerals vital for electronics and space infrastructure. At current market prices, these minerals' potential value is astronomical. Companies are preparing to survey nearby asteroids, deploy robotic mining systems, and transport the extracted materials back to Earth or space-based facilities.

Other planets and moons are already being explored. Many nations have landed robotic systems on Mars and are scanning the solar system for habitable planets, some of which have been identified.

In the 2020s and beyond, space operations will only be as secure as the cybersecurity programs that defend them. Cyber threat actors can disrupt operations in three key ways: by targeting the ground stations, the communication links, or the space assets themselves.

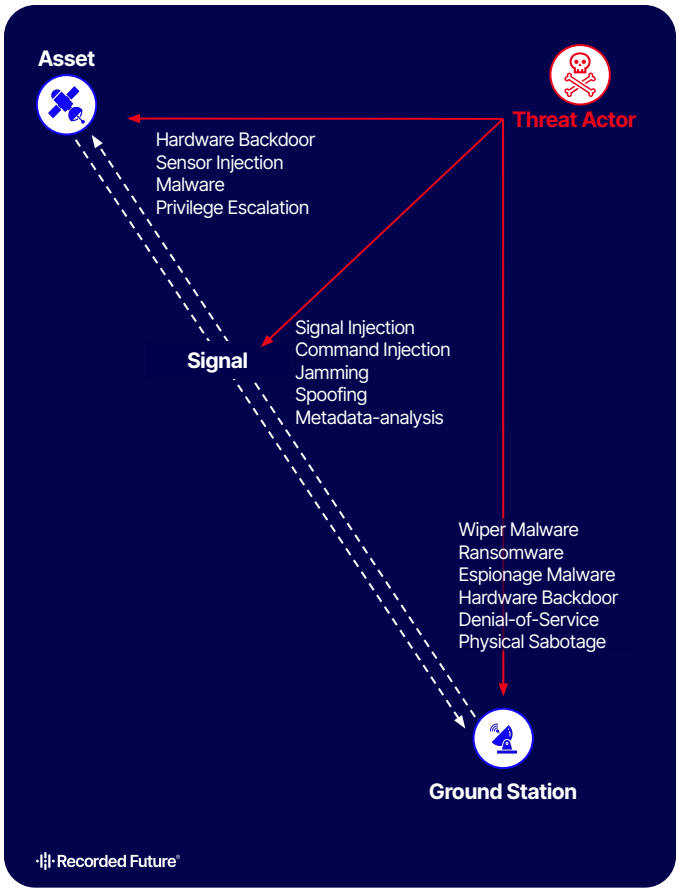


Figure 1: *Simplified diagram of how a cyber threat actor could target space operations (Source: Recorded Future)*

Countries are increasingly militarizing space operations. The primary objective at this stage appears to be protecting satellites and ground stations. The US Space Force contains Space Delta 6, which "conducts Cyberspace Operations to defend United States Space Force space systems from adversarial attack through the cyber domain...".

The Chinese military has also recognized that space operations heavily rely on network systems and that cybersecurity is critical to ambitions in space. As a result, in 2024, the People's Liberation Army created the PLA Cyberspace Force (CSF), Information Support Force (ISF), and Aerospace Force (ASF).

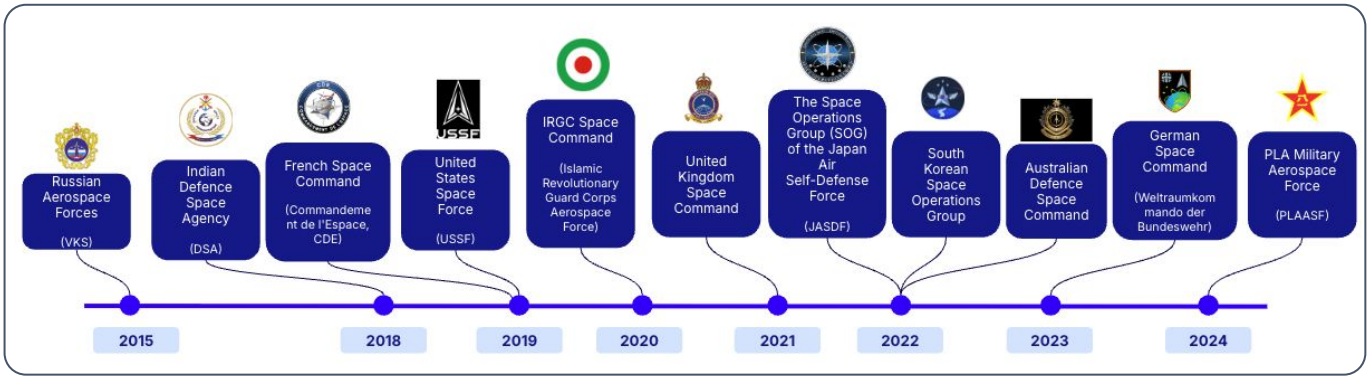


Figure 2: *Timeline of countries that have been investing in space commands and forces (list not exhaustive)(Source: Recorded Future)*

As indicated in Figure 3, there has also been a continued trend in cyber threat actors — many of whom are believed to be affiliated with military units — targeting aerospace companies developing space technologies. Insikt Group has observed these threat actors targeting contractors or using fraudulent identities to gain access to organizations.

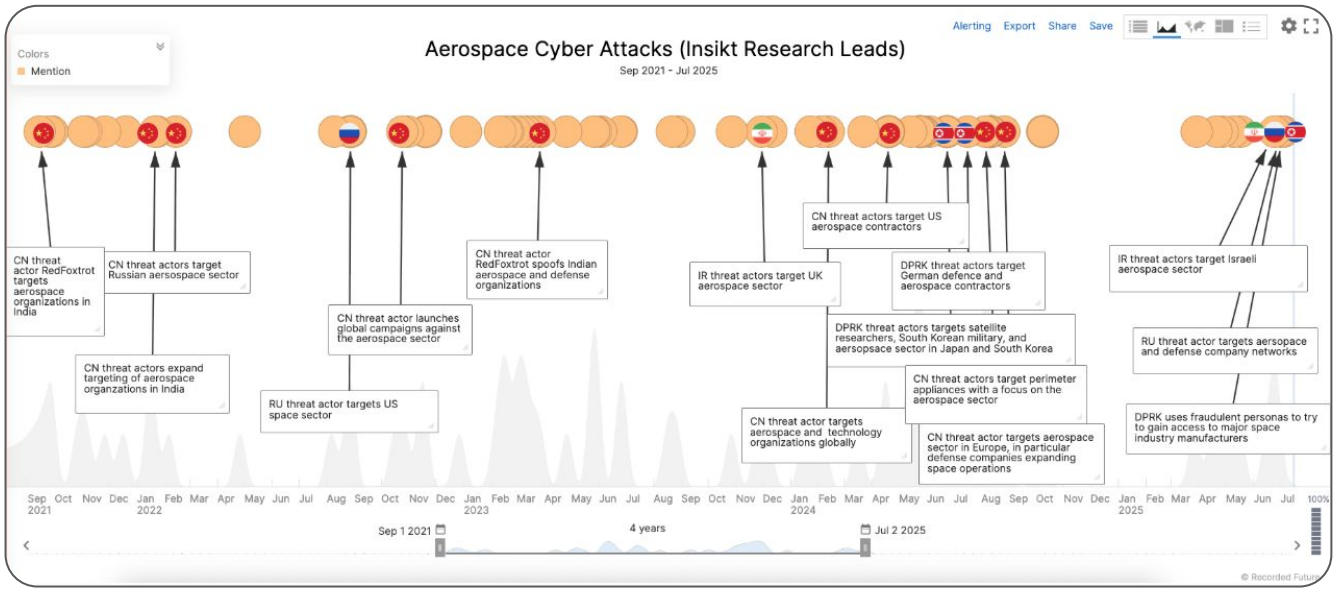


Figure 3: *Timeline of Recorded Future Insikt Research Leads, showing some key State-sponsored targeting of the aerospace sector from September 2021 to July 2025 (Source: Recorded Future)*

Governments are rightly focused on securing ground stations by patching vulnerabilities, blocking phishing attacks, resetting leaked credentials, and monitoring for insider threats. While these defensive measures are essential, outsourcing the production of space equipment to private suppliers makes those companies an attractive target for cyber threat actors seeking to exploit weaker links in the supply chain.

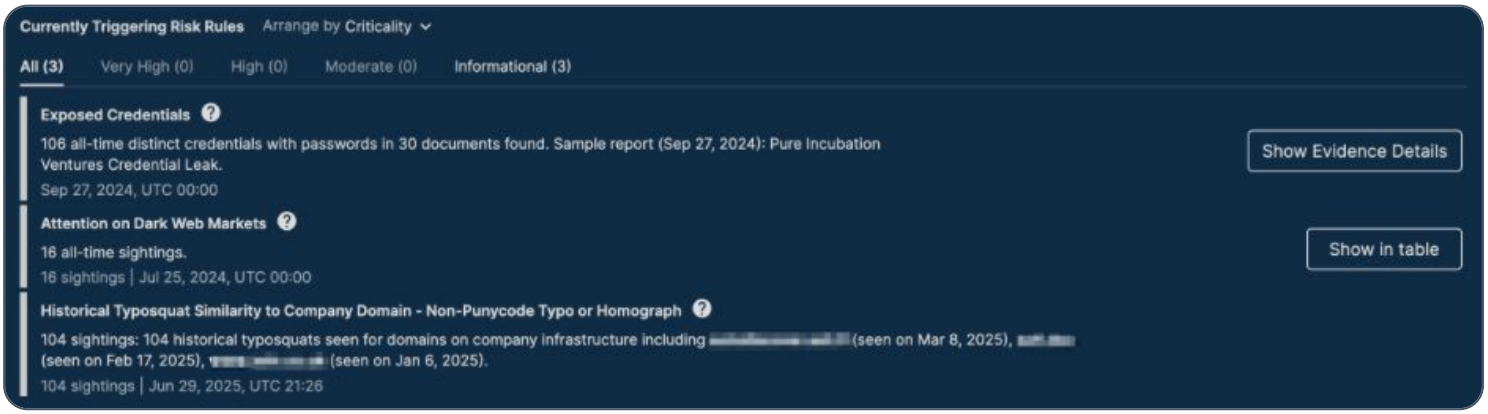
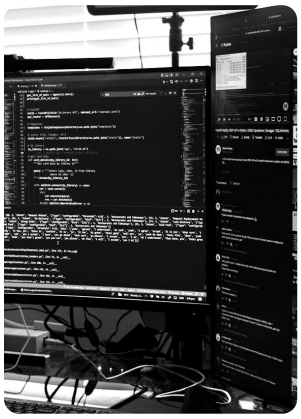


Figure 4: *Screenshot of Third Party Intelligence risk rules from a major supplier to a military operating its equipment in space (Source: Recorded Future)*

Organizational Impact

Scenario: "Space Systems Inc.", operating assets in the space domain, has not implemented a robust cybersecurity program or third-party supplier monitoring program.



First-order Implications

Development 1 Unhardened ground-station networks become low-effort targets	**Effect** Default passwords, unpatched systems, and exposed ports allow intrusion within days	**Risks** Operational disruption Brand impairment
Development 2 Unvetted suppliers insert counterfeit or back-doored components	**Effect** "Need-it-now" procurement bypasses rigorous parts checks; malicious firmware is hidden inside components	**Risks** Operational disruption Legal/compliance failure



Second-order Implications

Development 1 Supply-chain compromise manifests on-orbit	**Effect** Anomalous satellite behavior, unplanned safe-modes	**Risks** Operational disruption Competitive disadvantage
Development 2 Persistent foothold in ground segment enables data exfiltration	**Effect** Attackers move laterally across the network, gaining privileges, then leak proprietary data	**Risks** Brand impairment Legal/compliance failure



Third-order Implications

Development 1 Satellite hijack or kinetic debris incident	**Effect** Attacker communicates with satellite and starts to issue rogue thrust commands, causing collision or uncontrolled de-orbit; litigation soon follows	**Risks** Legal/compliance failure Brand impairment
Development 2 Investor class-action or SEC enforcement	**Effect** Material cyber weaknesses were not disclosed; post-incident stock drop triggers lawsuits and regulatory probes	**Risks** Financial fraud Legal/compliance failure

Outlook

The second era of the Space Race will almost certainly become polarized: The US-led Artemis Accords are attracting signatories from countries aligned with the US, while China and Russia have declined to sign and are pursuing their own joint ventures, such as plans for a shared lunar base. This signals that Space Race 2.0 will likely be defined by competition between a US-led bloc and a China-led bloc.

Control of the Moon and its resources will very likely decide who becomes the dominant superpower: Plans to establish lunar bases are advancing and could become a reality in the 2030s. The race to colonize the Earth's moon is set to create intense strategic competition between the US and China. The first nation to harvest lunar resources will likely gain a major boost to its industrial capabilities.

Cybersecurity will almost certainly be pivotal to the success of space operations: Cyberattacks are already being used to steal sensitive intellectual property from organizations developing space technologies, increasing the risk of competitive disadvantage. While many attacks so far have avoided outright destruction, satellite-related incidents like the 2022 Viasat attack and recent signal hijacking highlight the growing threat of operational disruption.

Supply chains are almost certain to be the Achilles' heel of space operations: As private companies and government agencies rapidly outsource software development and equipment manufacturing, supply-chain risks are often overlooked. Critical aerospace components continue to be produced in adversarial countries, substantially increasing the risk of operational downtime or even the installation of backdoors in delivered systems.

Mitigations

Cybersecurity basics really matter: If your organization manages any space operations from Earth, review your vulnerability patching program and identity and access management practices. Ensure you are ingesting high-fidelity indicators of compromise (IoCs) related to threat actors known to target the aerospace sector into your SIEM and EDR tools.
Recorded Future's Integrations, Vulnerability, Identity, and SecOps Intelligence can help support these efforts.

Conduct an in-depth audit of your supply chain: Maintain a detailed inventory of who manufactures your components and where they are produced. Rank suppliers by criticality and monitor their cybersecurity hygiene. If critical components are linked to suppliers with high Risk Scores, consider restricting their access or replacing them. At a minimum, factor these risks into your business continuity planning.
Recorded Future's Third-Party Intelligence can help support these efforts.

Do not underestimate the threat of removable media: Even with air-gapped systems, the risk of "Replication Through Removable Media" (MITRE ATT&CK Technique T1091) remains significant. This technique is increasingly reported as an initial access vector for state-sponsored threat actors.

Familiarize your blue teams with the SPARTA Matrix: This is a space-focused adaptation of the MITRE ATT&CK framework. It offers a structured knowledge base of cyber adversary tactics, techniques, and procedures (TTPs) specific to space systems.

Further Reading

SOURCE	TITLE
Recorded Future	The Convergence of Space and Cyber: An Evolving Threat Landscape
Insikt Group	Near-Space in China's Military Strategy: Strategic Reconnaissance, Precision Strike, and Battlefield Advantage
ENISA	ENISA Space Threat Landscape 2025

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform delivers end-to-end visibility across adversaries, infrastructure, and targets. Powered by precise AI-driven analytics and the proprietary Intelligence Graph®, the platform enables organizations to see the complete picture, act with confidence, and get ahead of threats that matter. With real-time intelligence built from over 15 years of threat data, Recorded Future supports security teams in proactively defending against evolving threats. Headquartered in Boston with global offices, Recorded Future works with over 1,900 businesses and government organizations across 80 countries. Learn more at www.recordedfuture.com.

© Recorded Future®, Inc. All rights reserved. All trademarks remain property of their respective owners.