COUNTERSPACE COMPETITION AND ORBITAL INFRASTRUCTURE

Electronic attack, cyber intrusion, co-orbital activity, and the erosion of space-domain stability.

DOCUMENT ID	SM-2026-TA-103	**DATE**	AUGUST 1, 2026
CLASSIFICATION	FOR INTERNAL USE ONLY	**TARGET CONTEXT**	SPACE / CRITICAL INFRASTRUCTURE

EXECUTIVE SUMMARY

Space is now a contested operational domain in which military, commercial, and civil services depend on shared orbital and terrestrial infrastructure. The most accessible threats are not necessarily kinetic anti-satellite weapons. Jamming, spoofing, cyber intrusion, supply-chain compromise, and interference with ground systems can disrupt services at lower political and operational cost. At the same time, growing orbital congestion and maneuvering activity make attribution and collision avoidance more difficult.

KEY JUDGMENTS

- Electronic warfare and cyberattack against ground and link segments are the most likely near-term means of disrupting space-enabled services.
- Proliferated architectures improve resilience but create a larger terminal, software, and supply-chain attack surface.
- Space-domain awareness is becoming the central prerequisite for warning, attribution, maneuver, and coordinated response.
- Kinetic attacks remain lower probability because of debris and escalation risk, but demonstrations and preparations will continue.

ANALYTIC CONFIDENCE: High on general threat categories; moderate on intent and operational readiness of specific national counterspace systems.

I. STRATEGIC CONTEXT

Modern economies and military forces rely on positioning, navigation and timing, satellite communications, weather data, missile warning, and remote sensing. These services depend on satellites, ground stations, data links, cloud infrastructure, and software. An attacker can therefore target the service architecture without physically destroying a spacecraft.

II. THREAT ARCHITECTURE

Link interference

Uplink and downlink jamming can create localized or regional service loss. GNSS spoofing can create more dangerous effects by providing plausible but false position or timing data.

Ground and cyber segment

Ground stations, mission systems, software supply chains, and user terminals may be more accessible than satellites and can provide persistent access or data manipulation opportunities.

Co-orbital activity

Rendezvous and proximity operations can support inspection, intelligence collection, interference, or pre-positioning, while maintaining ambiguity.

Kinetic and debris risk

Direct-ascent and on-orbit destructive actions can deny capability but create debris, international backlash, and uncontrolled effects.

Threat Matrix

Threat category	Level	Trend	Primary driver
GNSS jamming/spoofing	SEVERE	RISING	Low cost and regional scalability
Ground-segment cyberattack	HIGH	RISING	Accessible software and identity attack surface
Satellite link jamming	HIGH	RISING	Reversible and deniable disruption
Co-orbital operations	HIGH	RISING	Dual-use proximity capabilities

III. GRAPHICAL ANALYSIS

The risk profile emphasizes likelihood and potential for disruption during the next twelve months. GNSS interference and cyberattack rank above kinetic attack because they are more reversible, scalable, and politically deniable.

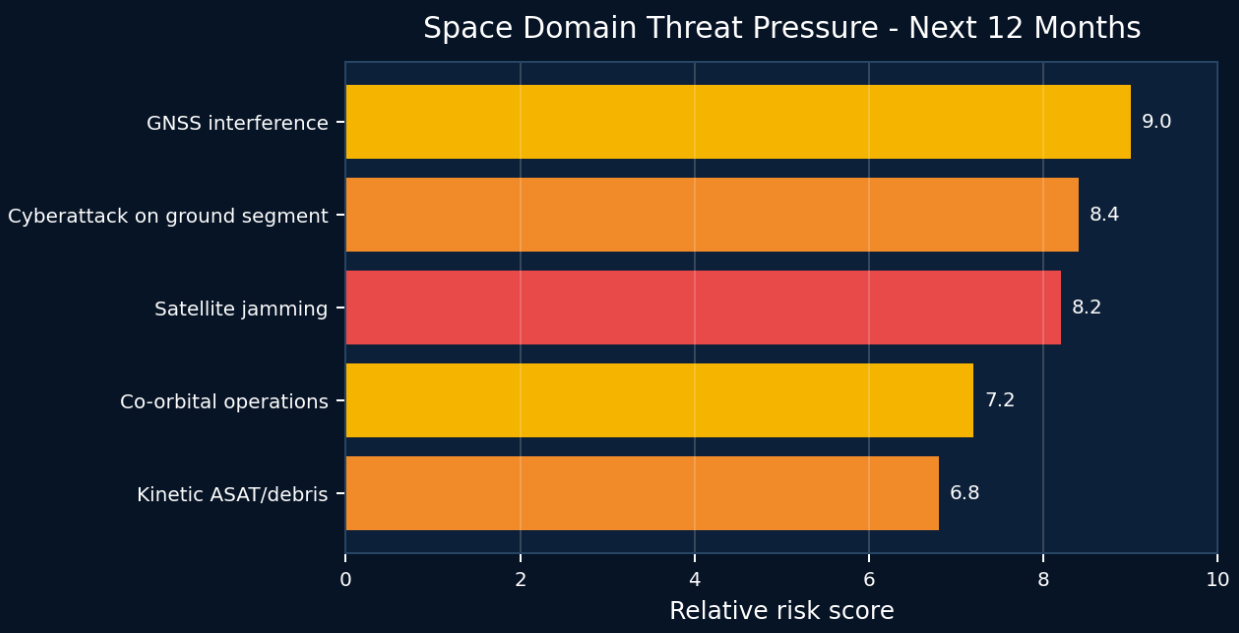

Figure 1. Sentinel Meridian analytic visualization based on cited open-source reporting.

Resilience requires diverse sensors, protected timing, alternate communications, rapid anomaly detection, and plans to operate through partial degradation rather than assuming uninterrupted service.

IV. OPERATIONAL TIMELINE AND MECHANISM

2025

U.S. Space Force leadership emphasizes space-domain awareness, resilient architectures, and counterspace capabilities as top operational priorities.

SEPTEMBER 2025

The ATLAS system is operationally accepted to support catalog maintenance, maneuver detection, and sensor tasking.

APRIL-MAY 2026

The Space Force announces major upgrades to optical surveillance and early employment of the Deep Space Advanced Radar Capability.

NEXT 12 MONTHS

More objects, maneuvers, and dual-use capabilities will increase the need for rapid characterization and allied data sharing.

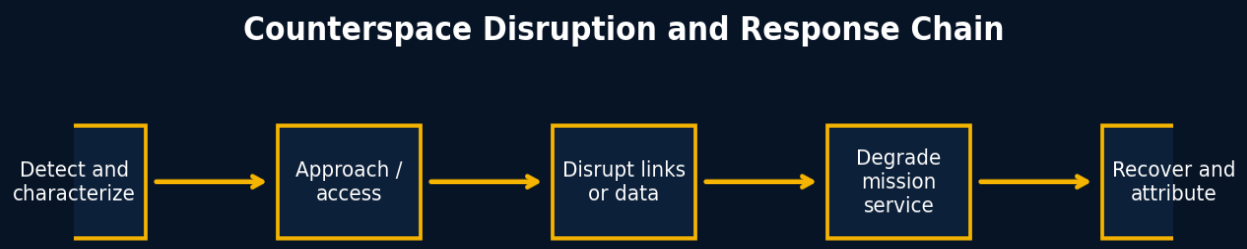

Figure 2. Simplified operational pathway; actual activity may involve additional intermediaries and technical steps.

V. CASE STUDY / SCENARIO ANALYSIS

Improving awareness as a response to ambiguous on-orbit behavior

In April 2026, U.S. Space Force reporting stated that an optical sensor upgrade at Maui doubled field of view and search speed and more than tripled sensitivity for detecting smaller and harder-to-see objects across multiple orbital regimes. In May, the service described early employment of the Deep Space Advanced Radar Capability, a trilateral U.S.-Australia-U.K. sensor network supporting awareness to geosynchronous orbit. These investments illustrate a central reality: before a defender can deter, maneuver, or attribute, it must see and characterize activity quickly.

VI. IMPLICATIONS FOR CLIENTS AND PARTNERS

- Protect ground systems and satellite operations networks as critical infrastructure.
- Develop assured alternatives for timing, navigation, and communications.
- Use multi-sensor data and allied information sharing to reduce ambiguity.
- Exercise operations during partial loss, spoofing, or latency of space services.
- Assess commercial-provider concentration and contractual continuity risks.

INTELLIGENCE GAPS

- True readiness and rules of engagement for co-orbital systems.
- Cyber vulnerability of commercial ground segments and mission software.
- Attribution thresholds for interference and reversible attacks.
- Capacity to replace specialized satellites after loss or sustained degradation.

VII. OUTLOOK

Competition will intensify below the threshold of destructive attack. States will test jamming, spoofing, cyber access, close approaches, and legal or commercial pressure because these methods are scalable and can be calibrated. Proliferation will make complete denial harder, but dependence on common software, terminals, and cloud services may create new concentration risks.

SENTINEL MERIDIAN BRIEFING CONCLUSION: The decisive question is not whether satellites can be attacked. It is whether essential services can continue under interference, cyber compromise, congestion, and uncertainty. Space resilience is therefore an enterprise architecture problem, not only a spacecraft-hardening problem.

SOURCES AND METHODOLOGY

This assessment uses open-source reporting and official public records. Judgments are analytic assessments, not statements of confirmed fact unless specifically attributed. Source access dates and publication dates should be checked before external release.

• U.S. Space Force, "Space Force delivers warfighting effects, protects homeland," March 21, 2025.

• U.S. Space Force, "Visibility in space magnified," April 14, 2026.

• U.S. Space Force Combat Forces Command, "New Deep Space Radar Capability Employed Early," May 4, 2026.

• U.S. Space Force Combat Forces Command, "ATLAS: A Paradigm Shift in Space Domain Awareness," April 7, 2026.

ASSESSMENTEND