Cybersecurity for Military Satellite Systems: Threats, Domains, and Engineering Countermeasures

Chuck Easttom
Vanderbilt, Georgetown, and Capitol Technology University, USA

chuckeasttom@gmail.com

Abstract: Military operations increasingly depend on satellite-enabled services for beyond-line-of-sight command-and-control, intelligence, surveillance and reconnaissance (ISR), missile warning, and precision navigation and timing. As space becomes more contested, adversaries can achieve operationally significant effects by cyber-compromising the end-to-end satellite enterprise rather than physically destroying spacecraft. A prominent example is the 24 February 2022 KA-SAT incident, where an intrusion into terrestrial management infrastructure and downstream user terminals disrupted connectivity for tens of thousands of users across Ukraine and Europe (CyberPeace Institute, 2022; Viasat, 2022). This paper develops an engineering-oriented threat model for military satellite systems across the ground, link, space, and user segments, then translates that model into implementable security controls and mission assurance design patterns. Using a quantitative, model-based risk assessment (Monte Carlo simulation) and control-to-attack-surface mapping, the paper prioritizes high-leverage mitigations such as privileged access management for mission operations, authenticated command and telemetry protection using standards-based space data-link cryptography, and zero trust architectures adapted to intermittent, high-latency RF environments (CISA, 2024a; CCSDS, 2020). Finally, the paper synthesizes resilience engineering principles—redundancy, graceful degradation, rapid reconstitution, and cyber-informed autonomy—into a pragmatic roadmap that aligns security investments with operational tempo. The central finding is that satellite cybersecurity must be treated as mission assurance: an integrated set of architectural, procedural, and cryptographic controls that preserve capability under sustained cyber pressure and enable recovery within tactically relevant timelines.

Keywords: Satellite cybersecurity, SATCOM, TT&C, Zero trust, Mission assurance, Space systems security

1. Introduction

Satellites underpin modern military power by enabling globally distributed forces to communicate, sense, navigate, and coordinate at speed and scale. NATO recognizes space as an operational domain and highlights that space capabilities are critical enablers for communications, navigation, early warning, and ISR in support of collective defense and crisis response (NATO, 2025). As constellations proliferate, the cyber-physical attack surface expands: spacecraft are controlled by ground mission operations centers (MOCs), telemetry-tracking-and-command (TT&C) infrastructure, key management systems, and a large population of geographically dispersed user terminals. These dependencies create numerous digital pathways for adversaries to generate denial, deception, or espionage effects without resorting to kinetic anti-satellite operations.

The KA-SAT incident illustrates the operational asymmetry of cyber-attacks against space services. Public reporting indicates that malware delivered via terrestrial management systems caused widespread modem disruption, producing cascading impacts beyond the immediate conflict area (CyberPeace Institute, 2022; SentinelOne, 2022). The implication for military systems is that mission assurance requires an enterprise view: protection of spacecraft alone is insufficient if ground or user segments can be compromised to deny or manipulate the mission.

This paper contributes an engineering-focused synthesis that (i) formalizes a threat model across satellite segments, (ii) presents a model-based quantitative risk ranking to guide prioritization, (iii) maps controls and standards—including CISA space-sector guidance and CCSDS data-link security—onto concrete attack surfaces, and (iv) operationalizes resilience patterns into an implementation roadmap (CISA, 2024b; RAND, 2024).

2. Satellite Enterprise Architecture and Cyber-Relevant Dependencies

Military space systems are end-to-end enterprises rather than monolithic spacecraft. From a security engineering perspective, the primary decomposition is into space, ground, link, and user segments, augmented by supply chain and lifecycle processes (Willbold et al., 2023). Each segment introduces distinct trust boundaries, timing constraints, and failure modes that must be incorporated into the security architecture.

2.1 Segment Decomposition

The space domain can be decomposed into multiple architectural segments in order to support systematic security engineering and risk analysis (Falco et al, 2024). Segmenting the satellite enterprise enables security controls to be mapped to specific operational domains, trust boundaries, and communication pathways within

the overall mission architecture. Such decomposition also allows threat modeling, attack-surface enumeration, and defensive control implementation to be applied in a structured and domain-specific manner across the satellite ecosystem.

- Space segment: satellite bus and payload, onboard avionics, flight software, software-defined radios (SDRs), inter-satellite links, attitude and orbit control, and onboard data handling.
- Ground segment: MOCs, TT&C stations, scheduling systems, key management infrastructure (KMI), mission data processing pipelines, and the supporting enterprise IT environment.
- Link segment: RF uplinks/downlinks for telemetry and command, mission payload data links, gateway backhaul, and cross-support interfaces.
- User segment: tactical SATCOM terminals, ship/aircraft modem stacks, handheld receivers, gateways, and coalition partner interconnects.
- Supply chain and lifecycle: multi-tier vendors, firmware provenance, software bill of materials (SBOM), cryptographic key lifecycle, and long-term sustainment over decade-scale lifetimes.

An infographic describing the segments is shown in figure 1.

Figure 1: Satellite Domain Segmentation

The attack surface grows with the number of operational satellites and associated terminals. The Union of Concerned Scientists database lists more than 7,560 operational satellites in orbit, illustrating the scale and

heterogeneity of the modern space environment (Union of Concerned Scientists, 2025). Greater scale increases the importance of automation, standardization, and robust identity-centric controls because manual, perimeter-driven approaches do not compose across distributed enterprises.

3. Threat Landscape and Attack Surfaces

The threat landscape must be systematically analyzed to identify potential attack surfaces across the satellite enterprise. Attack surface analysis involves identifying all interfaces, communication channels, software systems, and operational processes that could potentially be exploited by an adversary. Understanding these exposure points is a foundational step in cybersecurity engineering because it enables defenders to prioritize mitigation strategies, develop layered defensive architectures, and reduce the probability of successful exploitation across the ground, link, space, and user segments.

3.1 Ground-segment Intrusion and Mission Operations Compromise

Ground networks frequently contain conventional IT services such as identity providers, remote administration tooling, virtualized computers, and vendor maintenance channels. Adversaries can exploit misconfigurations, unpatched vulnerabilities, or compromised credentials to traverse from enterprise networks into mission operations enclaves. Once inside, attackers can disrupt scheduling, corrupt mission data pipelines, or tamper with command authorization workflows, achieving disproportionate operational impact without interacting directly with spacecraft.

3.2 TT&C Compromise and Command Authority

TT&C links represent the highest-consequence control surface because they encode command authority. Attack vectors include unauthorized command injection, replay of previously valid commands, manipulation of time-tagged command sequences, and corruption of telemetry to induce operator misinterpretation. Inconsistent cryptographic protection and operationally fragile key management remain recurring weaknesses; consequently, standards-based link-layer security and robust key lifecycle management are foundational countermeasures (CCSDS, 2020; CCSDS, 2020a).

3.3 User-terminal and Tactical Edge Exploitation

Tactical terminals operate in contested environments with constrained physical security and complex logistics. Because terminals are numerous, sometimes commercially derived, and frequently forward-deployed, they are attractive scaling targets. Terminal compromise can expose cryptographic material, enable traffic manipulation, or provide a pivot into gateway infrastructure. The KA-SAT event demonstrated a terminal-focused disruption mode at scale (CyberPeace Institute, 2022).

3.4 Supply Chain and Long Lifecycle Vulnerabilities

Spacecraft lifecycles span a decade or longer, while many embedded components have shorter support windows. Patch logistics are constrained by uplink bandwidth, certification processes, operational risk, and limited contact windows. These constraints elevate the importance of secure-by-construction engineering, reproducible builds, SBOM-driven vulnerability management, and cryptographic verification of updates. Space-specific risk management guidance emphasizes that cybersecurity requirements must be planned early and integrated with system engineering rather than retrofitted after launch (CISA, 2024b).

3.5 Historical Incidents and Observed Patterns

Public reporting indicates that satellite systems have been subject to cyber interference via ground infrastructure. For example, reports describe interference affecting NASA's Terra and the Landsat-7 system in 2007–2008, accessed via a ground station, underscoring the criticality of ground-segment security (Space.com, 2011; Satellite Today, 2011). In 2014, media reporting described a cyber intrusion affecting the U.S. National Oceanic and Atmospheric Administration network supporting weather operations, highlighting that space-enabled services are exposed through terrestrial IT dependencies (CBS News, 2014). These cases reinforce a consistent pattern: ground and user segments are often the most accessible adversary entry points, while the operational impact can manifest in the space mission.

4. 4. Quantitative, Model-based Risk Assessment

Because incident data for national security space systems is sparse and frequently classified, programmatic prioritization commonly relies on model-based risk assessment. This section presents a lightweight quantitative

approach intended to support engineering decision-making. The analysis uses Monte Carlo simulation to propagate uncertainty in likelihood and impact for representative threat vectors and to produce relative risk rankings. Results are illustrative rather than empirical; they should be calibrated with program-specific telemetry, vulnerability data, and red-team results.

4.1 Methodological Framework

The proposed approach employs a stochastic risk propagation model using Monte Carlo simulation to estimate the distribution of mission risk across heterogeneous threat vectors. Each threat vector is parameterized by likelihood of successful exploitation modeled as a Beta distribution, and operational impact severity modeled as a lognormal distribution. The resulting risk functional is defined as the product of likelihood and impact.

Monte Carlo sampling (N = 20,000) is used to estimate expected risk, tail risk (95th percentile), and higher-order statistical properties. This formulation aligns with probabilistic risk assessment methodologies used in safety-critical aerospace systems and extends them to cyber-physical threat domains in the space sector (Varadharajan & Suri, 2024; Falco et al., 2024; Khan et al., 2024).

Uncertainty is treated explicitly through wide prior distributions and scenario-based stress testing. Epistemic uncertainty is captured through expert-informed priors, while aleatory uncertainty reflects inherent stochastic variability in system behavior.

4.2 Results

The simulation outputs should be interpreted as relative prioritization indicators rather than absolute measures. Ground-segment intrusion demonstrates the highest expected risk due to accessibility and control-plane centrality. Conversely, TT&C compromise and supply-chain insertion exhibit lower likelihood but significantly higher tail risk, indicating catastrophic mission consequences.

Table 1: Illustrative risk model outputs (relative units; Monte Carlo simulation)

Threat vector	Segment	Likelihood (mean)	Impact (median)	Risk (mean)	Risk (P95)
Ground-segment intrusion	Ground	0.286	19.9	6.86	17.58
TT&C command compromise	Link/Space	0.074	36.8	3.14	8.81
User-terminal compromise	User	0.200	18.0	4.31	11.26
Supply-chain insertion	Supply chain	0.057	44.7	3.23	10.03
Data/telemetry integrity attack	Link/Space	0.123	24.4	3.50	9.55

Figure 2 visualizes the relative risk ranking from the model; programs should use the ranking to focus assurance effort on the highest-consequence, highest-accessibility pathways first.

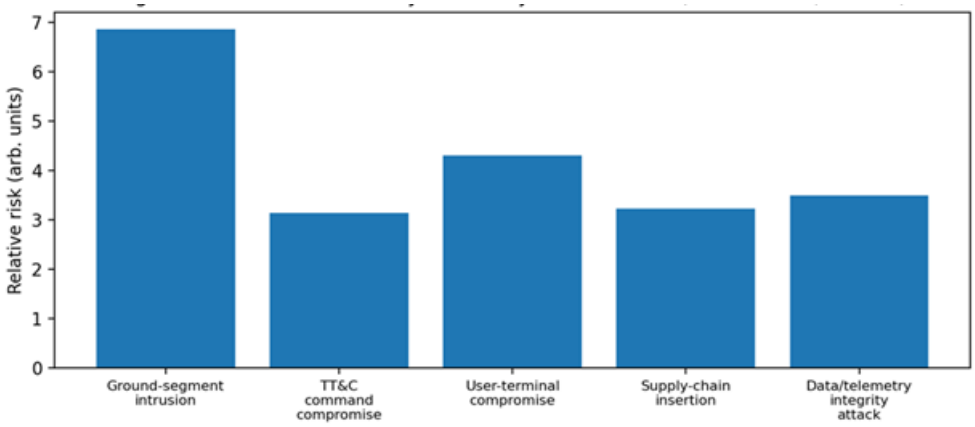

Figure 2: Modeled relative cyber-risk by threat vector (illustrative; Monte Carlo, N=20,000)

User-terminal compromise demonstrates systemic scaling effects, where moderate likelihood combined with large fleet size produces substantial aggregate risk. These findings are consistent with observed attack patterns and recent scholarship on space cyber resilience and attack-surface growth in satellite ecosystems (Varadharajan & Suri, 2024; Khan et al., 2024; Falco et al., 2024).

5. Security Engineering Controls and Architectures

Once the attack surface has been identified and characterized, the next phase of the security engineering process involves evaluating the security controls and architectural safeguards that protect each system component. This assessment includes analyzing authentication mechanisms, cryptographic protections, network segmentation strategies, and operational security procedures to determine their effectiveness against identified threat vectors. Through this process, organizations can systematically identify capability gaps, architectural weaknesses, and control deficiencies that must be addressed to achieve acceptable mission assurance levels.

5.1 Control Baselines and Governance

Military satellite cybersecurity programs typically adopt formal control baselines and assurance processes. CISA's space-sector guidance recommends using the NIST Cybersecurity Framework to develop profiles and risk mitigation plans and identifies common sources of cyber risk across space infrastructure (CISA, 2024b). For national security systems, additional overlays and profiles can improve fidelity by tailoring control intent to space-segment constraints. The Aerospace Corporation's space-segment cybersecurity profile provides a threat-focused rationale for tailoring controls to spacecraft avionics and mission contexts (The Aerospace Corporation, 2023).

5.2 Data-link Cryptography and Key Management

Cryptographic protection of telemetry and command is a prerequisite for preventing command injection and for preserving integrity under RF interception. The CCSDS Space Data Link Security (SDLS) family specifies services for authentication, confidentiality, and security parameter management at the data-link layer (CCSDS, 2020a). Engineering implementation requires: (i) hardware-backed key storage where feasible, (ii) rotation and revocation procedures compatible with limited contact windows, (iii) separation of mission keys from operator credentials, and (iv) resilient key distribution mechanisms that maintain continuity under degraded connectivity.

5.3 Zero Trust for Satellite Enterprises

Zero trust replaces implicit trust with explicit, continuously evaluated trust decisions based on identity, device posture, and policy. CISA's analysis of zero trust in the space environment identifies opportunities to apply zero trust tenets across ground, link, space, and user segments, while accounting for intermittent connectivity and latency (CISA, 2024a). Practically, this implies: strong identity for operators and devices, micro-segmentation of mission operations networks, policy enforcement points at control-plane interfaces, and continuous verification for privileged actions such as commanding and key management. Figure 3 describes zero trust control plane for satellites.

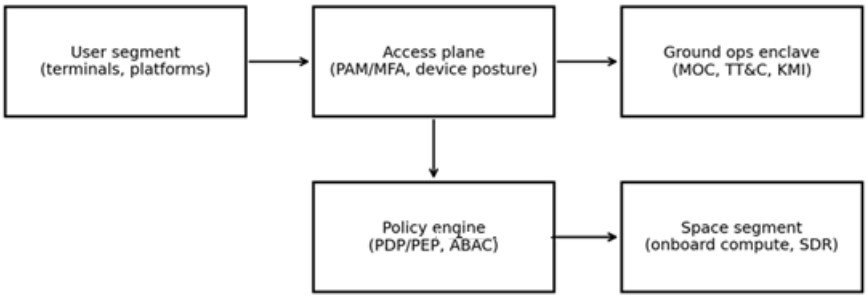

Figure 3: Reference zero trust control-plane adapted for satellite enterprises (conceptual)

5.4 Control-to-attack-surface Mapping

Table 2: Representative controls mapped to satellite attack surfaces

Control / mechanism	Primary segment	Engineering rationale
Privileged access management (PAM) + MFA for MOC/TT&C	Ground	Reduces credential theft and unauthorized operator actions; constrains lateral movement.
Network segmentation + unidirectional gateways for command paths	Ground/Link	Limits traversal from enterprise IT into operational enclaves; supports deterministic command pipelines.
SDLS authentication + encryption with robust key lifecycle	Link/Space	Mitigates command injection/replay and RF interception; preserves telemetry integrity.
Secure boot + signed updates + SBOM-driven vulnerability mgmt	Space/User/Supply chain	Reduces firmware insertion risk; improves patch trustworthiness and auditability.
Anomaly detection on TT&C telemetry and command sequences	Ground/Link	Detects deception and abnormal state transitions; supports rapid containment.
Degraded-mode operations and reconstitution playbooks	All	Enables mission continuation and rapid recovery under cyber disruption (RAND, 2024).

6. Resilience Engineering and Mission Assurance

Resilience engineering, sometimes referred to as reliability engineering, focuses on designing systems that can maintain operational capability despite failures, attacks, or unexpected disruptions. In complex cyber-physical systems such as military satellite architectures, resilience is evaluated using quantitative engineering methodologies including reliability modeling, failure mode analysis, and probabilistic risk assessment. These techniques allow engineers to measure system robustness, identify single points of failure, and design architectures that maintain mission functionality even when components are degraded or compromised.6.1 Resilience as a design requirement.

Perfect prevention is infeasible in complex, long-lived satellite enterprises. Mission assurance therefore treats resilience—continued operation and rapid recovery under attack—as a first-class requirement. RAND defines space mission assurance as deterring adversaries, countering risk from man-made and natural threats, and pursuing resilient architectures that sustain mission outcomes even when components fail or are compromised (RAND, 2024).

6.1 Engineering Patterns for Resilience

- Functional redundancy: multi-path communications (SATCOM + terrestrial backhaul), redundant ground stations, and cross-band contingency links.
- Diversity: heterogeneity across vendors, waveforms, and software stacks to reduce common-mode failure and supply-chain monoculture.
- Graceful degradation: pre-planned reduced capability modes (e.g., lower data-rate, reduced ISR product fidelity) that maintain critical functions under constraint.
- Rapid reconstitution: scripted rebuilds of ground services, golden images for terminals, and contingency keying material to restore trust quickly after compromise.
- Cyber-informed autonomy: onboard fault isolation and safe-mode transitions triggered by detected command anomalies or inconsistent state estimation.

6.2 Operational Metrics

Resilience must be measurable. Programs should define target recovery time objectives (RTO) and recovery point objectives (RPO) for mission services, then align engineering investments accordingly. For example, an RTO measured in hours for SATCOM service restoration implies pre-positioned terminal rekey capability, automated configuration management, and rehearsed playbooks for switching to alternate gateways. Where feasible, programs should instrument security-relevant telemetry—authentication failures, anomalous command sequences, and configuration drift—to support rapid triage and forensics.

7. Recommendations and Implementation Roadmap

Based on the previously developed threat model, the current cybersecurity standards landscape, and the results of model-based risk prioritization, a phased implementation roadmap can be constructed for defense organizations seeking to modernize satellite cybersecurity. This roadmap emphasizes controls that provide the highest marginal improvement in mission assurance while minimizing operational disruption and integration complexity. The proposed sequence addresses both technical and organizational transformation requirements across near-term, mid-term, and long-term horizons.

7.1 Near-term (0–12 Months)

Near-term efforts focus on high-impact, low-disruption controls. Organizations should implement privileged access management with hardware-backed authentication and just-in-time privilege escalation. Mission networks should be segmented with clearly defined trust boundaries, including isolation of TT&C command pathways using unidirectional gateways where feasible. Incident response capabilities must be operationalized through playbooks addressing terminal compromise, rapid re-imaging, and cryptographic key revocation. Regular cyber exercises should be conducted to validate response effectiveness.

- Enforce strict privilege access management, and time-bound privileged sessions for all mission operations and key management roles; eliminate shared accounts.
- Establish a segmented mission operations with segment boundaries well defined and secured.
- Create and exercise incident response playbooks for modem/terminal fleet compromise, including rapid re-imaging and key revocation.

7.2 Mid-term (12–36 Months)

Mid-term efforts introduce architectural transformation. Zero trust principles should be applied across mission interfaces with continuous authorization based on identity, device posture, and context (CISA, 2024a; Falco et al., 2024; Khan et al., 2024).

Secure software engineering practices, including reproducible builds, SBOM integration, and signed firmware pipelines, should be adopted. Telemetry-driven anomaly detection should be deployed across TT&C and mission data pipelines and integrated into a centralized security operations capability.

Threat intelligence integration should incorporate space-specific adversary tactics, techniques, and procedures, leveraging structured adversary-behavior frameworks and recent empirical analyses of satellite cyber-attack paths to support detection engineering and campaign analysis (Willbold et al., 2023; Khan et al., 2024; Peled et al., 2025).

- Adopt zero trust policy enforcement at mission control interfaces, integrating device posture and continuous authorization for high-consequence actions (CISA, 2024a).
- Introduce rigorous software engineering requirements, reproducible builds, and signed update pipelines for both spacecraft and terminal firmware; integrate supply chain risk assessment into acquisition.
- Instrument TT&C and mission data pipelines with anomaly detection tuned to satellite operational state models; integrate with a security operations capability.
- Integrate space oriented cyber threat intelligence into the development pipeline.

7.3 Long-term (36+ Months)

Long-term efforts focus on autonomous and resilient architectures. Cyber-informed autonomy should be embedded in spacecraft to enable anomaly-triggered safe modes and onboard decision-making under contested conditions. Constellation-level resilience should be engineered through distributed mission execution, authenticated inter-satellite links, and dynamic re-tasking. Coalition interoperability should be enabled through federated identity and attribute-based access control frameworks. These capabilities align with emerging doctrines of space cyber resilience and contested space operations (Falco et al., 2024; Khan et al., 2024; RAND, 2024).

- Engineer cyber-informed autonomy and safe-mode logic to maintain spacecraft survivability and limit adversary command authority.

- Design constellation-level resilience: diverse ground access, inter-satellite crosslinks with authenticated routing, and re-tasking strategies to sustain mission coverage under partial compromise.
- Standardize coalition interoperability through shared cryptographic and identity frameworks while maintaining compartmentalization and least privilege.

8. Conclusion

Military dependence on satellites makes space systems high-value cyber targets. Recent incidents demonstrate that adversaries can generate strategic effects by compromising ground infrastructure and user terminals rather than engaging in kinetic anti-satellite actions (CyberPeace Institute, 2022). Effective satellite cybersecurity therefore requires an enterprise mission assurance posture: structured risk management, standards-based link security and key management, identity-centric architectures such as zero trust, and resilience patterns that enable continued operation and rapid recovery (CISA, 2024a; RAND, 2024).

This study provides an engineering-oriented framework for analyzing satellite cyber risk and translating that analysis into actionable defensive architectures. However, satellite cybersecurity remains an evolving field that requires continued interdisciplinary research combining space systems engineering, network security, and operational mission assurance. Future work should focus on improved telemetry-driven threat detection, formal verification of satellite command systems, and integration of cyber resilience mechanisms directly into spacecraft autonomy and constellation-level architectures.

Ethics declaration: This research did not involve human subjects and thus no ethical clearance was required.

AI declaration: AI was only used to assist in making Figure 1. I created an initial figure then requested that ChatGPT improve that figure.

References

British Broadcasting Corporation (2014) China accused of hacking into US weather system. [online] Available at: https://www.cbsnews.com/news/china-accused-of-hacking-into-u-s-weather-system/ (Accessed: 2 March 2026).

CCSDS (2020a) Space Data Link Security Protocol Extended Procedures (CCSDS 355.1-B-1). [online] Available at: https://ccsds.org/Pubs/355x1b1.pdf (Accessed: 22 December 2025).

CCSDS (2020b) Space Data Link Security Protocol Extended Procedures: Summary of Concept of Operations (CCSDS 350.0-G-1). [online] Available at: https://ccsds.org/Pubs/350x11g1e1.pdf (Accessed: 22 December 2025).

CyberPeace Institute (2022) Case study: Viasat attack. [online] Available at: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (Accessed: 18 December 2025).

CISA (2024a) Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment. [online] Available at: https://www.cisa.gov/sites/default/files/2024-06/Space%20Systems%20Security%20and%20Resilience%20Landscape%20-%20Zero%20Trust%20in%20the%20Space%20Environment%20%28508%29.pdf (Accessed: 23 December 2025).

CISA (2024b) Recommendations to Space System Operators for Improving Cybersecurity. [online] Available at: https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf (Accessed: 18 December 2025).

Falco, G., Boschetti, N., Viswanathan, A., Bailey, B., Maple, C., Kurt, G. K., ... & Yahia, O. B. (2024, July). Minimum requirements for space system cybersecurity-ensuring cyber access to space. In *2024 IEEE 10th International Conference on Space Mission Challenges for Information Technology (SMC-IT)* (pp. 78-88). IEEE.

Khan, S. K., Shiwakoti, N., Diro, A., Molla, A., Gondal, I., & Warren, M. (2024) Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions. International Journal of Critical Infrastructure Protection, 47, 100724. https://doi.org/10.1016/j.ijcip.2024.100724

NATO (2025) NATO's approach to space. Updated 30 July 2025. [online] Available at: https://www.nato.int/en/what-we-do/deterrence-and-defence/natos-approach-to-space (Accessed: 19 December 2025).

RAND (2024) Enhancing Space Mission Assurance to Cyber Threats: Findings and Recommendations for the U.S. Space Force (RR-A2319-1). [online] Available at: https://www.rand.org/pubs/research_reports/RRA2319-1.html (Accessed: 2 March 2026).

Satellite Today (2011) Report: Hackers interfered with Landsat-7, Terra AM-1 in 2007 and 2008. [online] Available at: https://www.satellitetoday.com/government-military/2011/10/31/report-hackers-interfered-with-landsat-7-terra-am-1-in-2007-and-2008/ (Accessed: 4 January 2026).

SentinelOne (2022) AcidRain: A modem wiper rains down on Europe. [online] Available at: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ (Accessed: 22 December 2025).

Space.com (2011) Hackers interfered with 2 US government satellites. [online] Available at: https://www.space.com/13423-hackers-government-satellites.html (Accessed: 2 March 2026).

The Aerospace Corporation (2023) Space Segment Cybersecurity Profile for National Security Systems (TOR-2023-02161 Rev. A). [online] Available at: https://sparta.aerospace.org/resources/TOR-2023-02161-RevA%20Space%20Segment%20Cybersecurity%20Profile.pdf (Accessed: 2 March 2026).

Union of Concerned Scientists (2025) UCS Satellite Database. [online] Available at: https://www.ucs.org/resources/satellite-database (Accessed: 2 March 2026).

Varadharajan, V., & Suri, N. (2024). Security challenges when space merges with cyberspace. *Space Policy*, *67*, 101600.

Viasat (2022) KA-SAT network cyber-attack overview. [online] Available at: https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/ (Accessed: 2 March 2026).

Willbold, J., Schloegel, M., Vögele, M., Gerhardt, M., Holz, T., & Abbasi, A. (2023, May). Space odyssey: An experimental software security analysis of satellites. In 2023 IEEE Symposium on Security and Privacy (SP) (pp. 1-19). IEEE.