International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

Satellite Communication Cybersecurity

Vinod Varma Vegesna

Independent Researcher

Vol. 7 No. 7 (2025): IJSTC

Abstract

Satellite communications (SatCom) are integral to global telecommunications, navigation, national security, and critical infrastructure. Recent years have shown a sharp rise in cyber-attacks and interference that target space assets, ground infrastructure, and radio links — exposing vulnerabilities across the SatCom ecosystem. This paper reviews the architecture of satellite systems, develops a threat taxonomy, surveys real-world incidents, analyzes technical and organizational vulnerabilities, synthesizes defensive measures (technical, operational, and policy), and proposes research directions and best-practice recommendations. Key references include recent surveys and authoritative guidance such as NIST IR 8270 and industry reports. NIST Publications+2MDPI+2

Keywords

Satellite communications, SatCom, space cybersecurity, GNSS spoofing, jamming, supply chain, NIST IR 8270, Viasat KA-SAT, attack surface, resilience.

1. Introduction

Satellites and their supporting systems form a globally distributed cyber-physical system that supports telecommunications (broadband/VSAT), broadcast, Earth observation, positioning (GNSS), and command-and-control for space vehicles. Because satellites bridge terrestrial networks and the space domain, they inherit classic cyberspace threats while also facing domain-specific interference and physical-kinetic risks. In the 2020s the number and diversity of space

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

actors expanded rapidly (mega-constellations, commercial ground stations, hosted payloads), increasing complexity and attack surface. Recent attacks and interference incidents demonstrate the sector's practical insecurity and the need for systemic cybersecurity improvements. Via Satellite+1

---

2. SatCom Architecture and Attack Surface

A typical communications satellite system comprises three logical segments:

- **Space segment:** the satellite bus and payload (transponders, processors, payload software, on-board computers, telemetry & telecommand (TTC) systems).
- **Ground segment:** Telemetry, Tracking & Control (TT&C) stations, Mission Control, Network Operations Centers, ground gateways, and user terminals (VSATs, user modems).
- **Space–ground link (radio links):** Uplink/downlink RF channels, satellite-to-satellite links, inter-satellite crosslinks, and GNSS signals. ScienceDirect+1

Each segment brings specific vulnerabilities:

- **Space segment vulnerabilities:** outdated or unsigned on-board software, insecure serial/maintenance ports, weak command authentication, and insufficient isolation between payload and bus functions.
- **Ground segment vulnerabilities:** exposed ground station networks, weak patch management, third-party service dependencies, and supply chain insertion risks.
- **Link vulnerabilities:** jamming, spoofing (GNSS and timing), unencrypted links, poor authentication at terminals, and RF intercepts.

---

3. Threat Taxonomy

We categorize threats into **confidentiality**, **integrity**, and **availability (CIA)** and into **cyber-only** and **mixed cyber-physical** attack types.

3.1 Confidentiality

- Eavesdropping on unencrypted telemetry, control channels, or user data streams.
- Compromise of ground station networks to exfiltrate keys, engineering data, or user payloads.

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

3.2 Integrity

- Tampering with telemetry/telecommand (TTC) commands or payload configuration.
- GNSS spoofing to manipulate timing/position data used by networks or vehicles.

3.3 Availability

- RF jamming and denial of service against user terminals or TT&C frequencies.
- Targeted malware attacks that disrupt ground infrastructure (e.g., modem bricking, gateway shutdown). Real incidents demonstrate large-scale outages. Via Satellite+1

3.4 Supply-chain & Insider Threats

- Compromise during manufacturing, firmware supply chains, or via third-party ground service providers — a growing concern as the number of manufacturers and integrators grows. Recent industry assessments highlight disparities in threat intelligence and supply-chain risk management. The White House

---

4. Representative Incidents & Case Studies

4.1 Viasat KA-SAT (2022)

In February 2022, a cyber incident affecting the KA-SAT network disrupted thousands of customer modems across Europe and impacted services including critical infrastructure. Reporting and analyses connected the attack to exploitation of vulnerabilities in modems and management systems, resulting in mass denial of service and long service outages. This incident catalyzed industry awareness and responses to SatCom cyber risk. Via Satellite+1

4.2 GNSS Jamming and Spoofing (Baltic Sea & maritime)

States and non-state actors increasingly use GNSS jamming/spoofing to conceal ship movements and interfere with navigation. For example, Finland detected GNSS jamming and spoofing incidents in the Baltic Sea that disrupted navigation systems and AIS reports. These incidents show how link interference can create safety and security hazards for navigation and time-sensitive systems. Reuters

4.3 Malware and Espionage Using SatCom Infrastructure

Advanced persistent threat groups have long used satellite infrastructure as part of their operations. Historic analyses (e.g., Turla) show that adversaries have exploited satellite links as stepping stones for espionage and persistence inside networks. WIRED

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

5. Vulnerabilities — Technical and Organizational Analysis

5.1 Technical Weaknesses

- **Legacy systems and poor patch management:** long satellite lifecycles mean on-orbit systems often run outdated software with known vulnerabilities.
- **Insecure telemetry/telecommand (TTC):** weak or absent authentication and encryption for command channels permits spoofing or unauthorized reconfiguration.
- **Unencrypted payload/user links:** many consumer and enterprise satellite links still lack end-to-end encryption or appropriate key management at the edge.
- **Hardware and firmware supply-chain compromise:** third-party components may contain backdoors or vulnerable firmware that is hard to update in deployed satellites. ScienceDirect+1

5.2 Organizational Weaknesses

- **Fragmented regulatory landscape:** inconsistent standards between jurisdictions and insufficient sectoral critical-infrastructure designation complicate coordinated defense. Policy reports call for stronger frameworks and clearer lead agencies. Foundation for Democracy in Elections+1
- **Operational maturity variance:** startups and smaller operators sometimes lack mature cybersecurity processes or access to timely threat intelligence. Industry surveys highlight disparities in capabilities and information sharing. The White House

6. Defensive Measures and Best Practices

Security must be layered: cryptographic protections, secure engineering, operational practices, and policy.

6.1 Cryptography and Protocols

- **End-to-end encryption:** apply authenticated encryption for user payloads and, where feasible, for TTC channels. Use modern, post-quantum-aware key management planning (hybrid schemes during transition).
- **Mutual authentication:** devices (user terminals, ground stations) and space assets should use strong mutual authentication—hardware root of trust helps.

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

- **Secure boot & firmware signing:** satellite on-board systems should enforce signed firmware and secure boot to prevent unauthorized code. MDPI

6.2 Resilient Architectures

- **Segmentation and least privilege:** isolate TT&C networks, mission systems, and payload traffic; apply strict access controls.
- **Redundancy & graceful degradation:** design GEO/LEO constellations and ground infrastructure to survive link loss or node compromise without catastrophic system failures (multi-path communications, alternative routing).
- **Anti-spoofing & anti-jamming:** multi-antenna arrays, signal-authentication techniques (e.g., spreading codes, cryptographic authentication of navigation signals where possible), and adaptive frequency hopping or beamforming. Research on jamming/spoofing detection has matured — early detection is essential to mitigation. MDPI+1

6.3 Supply-Chain Security

- **Component provenance & attestation:** track hardware and firmware provenance, require vendors to provide attestations and secure update mechanisms.
- **Secure DevSecOps:** integrate threat modeling, static/dynamic analysis, and code signing into satellite software development lifecycles. NIST and other bodies recommend adopting tailored cybersecurity frameworks for commercial satellite operations. NIST Publications

6.4 Operational & Organizational Controls

- **Incident response playbooks:** satellite-specific IR plans, tabletop exercises, and cross-sector coordination (telecom, energy, maritime) are critical.
- **Threat intelligence sharing:** improved, declassified, actionable intel flows between government and industry; industry reports note current shortfalls and the need for standardized channels. The White House
- **Regulatory alignment and standards:** adoption of frameworks (CSF mapping to satellite workflows) and establishing critical-infrastructure designations where appropriate to prioritize protections and funding. NIST Computer Security Resource Center+1

---

7. Standards, Guidance, and Policy Landscape

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

- **NIST IR 8270 (2023):** provides a method to apply the Cybersecurity Framework to commercial satellite operations and prescribes outcomes and suggested controls. This is a key reference for operators seeking to mature their security posture. NIST Publications+1
- **Industry reports & white papers:** U.S. government and industry collaborations have produced recent perspectives on space system cybersecurity and gaps in information sharing (White House / industry perspectives, 2025). The White House
- **Calls for critical-infrastructure status:** policy analyses advocate designating space systems as critical infrastructure to ensure resilience and funding for cybersecurity improvements. Foundation for Democracy in Elections

---

8. Research Directions

Priority research areas include:

1. **Lightweight cryptography for constrained space hardware:** ensuring strong cryptography with constrained CPU, memory, and power budgets on smallsats.
2. **Secure on-orbit update and rollback systems:** robust, authenticated update mechanisms and safe failover to prevent bricking or hijacking during updates.
3. **GNSS authentication and anti-spoofing at scale:** cryptographic authentication of navigation/time signals and networked detection algorithms.
4. **Telemetry anomaly detection with explainability:** ML methods for anomaly detection in TT&C and payload telemetry constrained by interpretability and false-positive control.
5. **Supply-chain risk quantification for hardware/firmware:** metrics and observability tools to assess provenance and tamper evidence. Recent literature emphasizes systematic surveys of attacks/defenses that can inform these research directions. MDPI+1

---

9. Recommendations (Operator & Policy)

For Satellite Operators

- Adopt NIST IR 8270 mapping to the CSF and implement prioritized controls (identity management, encryption, secure update, segmentation). NIST Publications
- Harden ground infrastructure: micro-segmentation, strong patch management, and vendor security assessments.

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

- Invest in multi-path communications and graceful failover to reduce service outages from link interference.

For Regulators & Governments

- Improve information sharing and declassification of actionable threat intelligence for the space sector. The White House
- Standardize minimum cybersecurity requirements for commercial space systems (e.g., TTC authentication, firmware signing) and consider critical infrastructure designation where appropriate. NIST Computer Security Resource Center+1

For Researchers

- Focus on deployable anti-spoofing techniques for GNSS and secure boot solutions for resource-constrained satellites. MDPI+1

---

10. Conclusion

Satellite communications are essential, but their growing complexity and interdependence expose them to diverse cyber threats. Recent incidents (e.g., KA-SAT), maritime GNSS interference, and ongoing espionage operations show real consequences for infrastructure, safety, and national security. Effective defense requires combining technical hardening (cryptography, secure firmware, anti-jamming), operational maturity (incident response, threat sharing), supply-chain controls, and policy alignment (standards and potential critical-infrastructure designation). Implementing the guidance in NIST IR 8270, adopting best engineering practices, and prioritizing research into domain-specific defenses will materially increase resilience. NIST Publications+2Via Satellite+2

References

The following references were used to prepare this paper — key sources are highlighted.

1. Scholl, M., et al., *Introduction to Cybersecurity for Commercial Satellite Operations*, NIST Interagency Report (IR) 8270, July 2023. NIST Publications+1
2. Kang, M., et al., *A Survey on Satellite Communication System Security*, Sensors (MDPI), 2024. MDPI
3. Tedeschi, P., et al., *Satellite-based communications security: A survey* (ScienceDirect), 2022. ScienceDirect

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

4. Radoš, K., et al., *Recent Advances on Jamming and Spoofing Detection in GNSS*, Sensors (MDPI), 2024. MDPI
5. SatelliteToday, *10 Defining Moments In Cybersecurity And Satellite In 2022* (Viasat/KA-SAT coverage). Via Satellite
6. University / policy pieces: *Looking to the skies: The importance of satellite cybersecurity* (USSC), Nov 2024. United States Studies Centre
7. White House / Industry, *Space System Cybersecurity — Industry Perspectives Report*, Jan 2025. The White House
8. Reuters, *Finland detects satellite navigation jamming and spoofing in Baltic Sea*, Oct 31, 2024. Reuters
9. Wired, *The Underground History of Russia's Most Ingenious Hacker Group (Turla)* — background on satellite linkage in espionage campaigns. WIRED
10. CSIS, *Significant Cyber Incidents* (timeline resource). CSIS
11. FDD / policy report, *Time to Designate Space Systems as Critical Infrastructure*, 2023. Foundation for Democracy in Elections
12. U.S. GAO, *NASA Needs to Fully Implement Risk Management*, GAO-25-108138, June 25, 2025. (Relevant for understanding programmatic cybersecurity risk maturity in large space projects.) GAO Files

---

Appendix A — Suggested Technical Controls (Checklist)

- Enforce signed firmware and secure boot.
- Mutual authentication for TT&C and ground systems; phased rollout of post-quantum hybrid keys.
- Encrypt telemetry and payload links end-to-end where feasible.
- Implement network segmentation and zero-trust principles across ground networks.
- Deploy GNSS spoof/jam detection and alternative timing sources.
- Maintain documented incident response, backups for operational data, and offline control paths.
- Conduct vendor security reviews and require SBOMs (software bill of materials) for onboard code.

International Journal of Science, Technology and Convergence (IJSTC)
ISSN: 2134-986X

Appendix B — Suggested Research Reading (select)

- Comprehensive surveys in Sensors (MDPI) on SatCom security and GNSS countermeasures (2024). MDPI+1
- NIST IR 8270 for mapping CSF to satellite operations.