Gilat Defense

www.gilat.com

White Paper

Cybersecurity Challenges in SATCOM

Release Date: 25 May 2025

Introduction

Satellite Communications (SATCOM) is a critical enabler of modern defense and governmental operations, facilitating secure, reliable, and resilient connectivity in diverse environments. However, as cyber threats continue to evolve, SATCOM networks face growing vulnerabilities to jamming, eavesdropping, spoofing, and cyberattacks. Addressing these challenges requires a robust cybersecurity framework that is grounded in comprehensive and detailed Enemy Course of Action (COA) Analysis - like the methodologies applied in other defense sectors - integrated within SATCOM solutions to safeguard sensitive data and ensure operational continuity.

Cybersecurity Challenges in SATCOM Systems

The increasing reliance on SATCOM for military and critical communications exposes it to several cybersecurity threats:

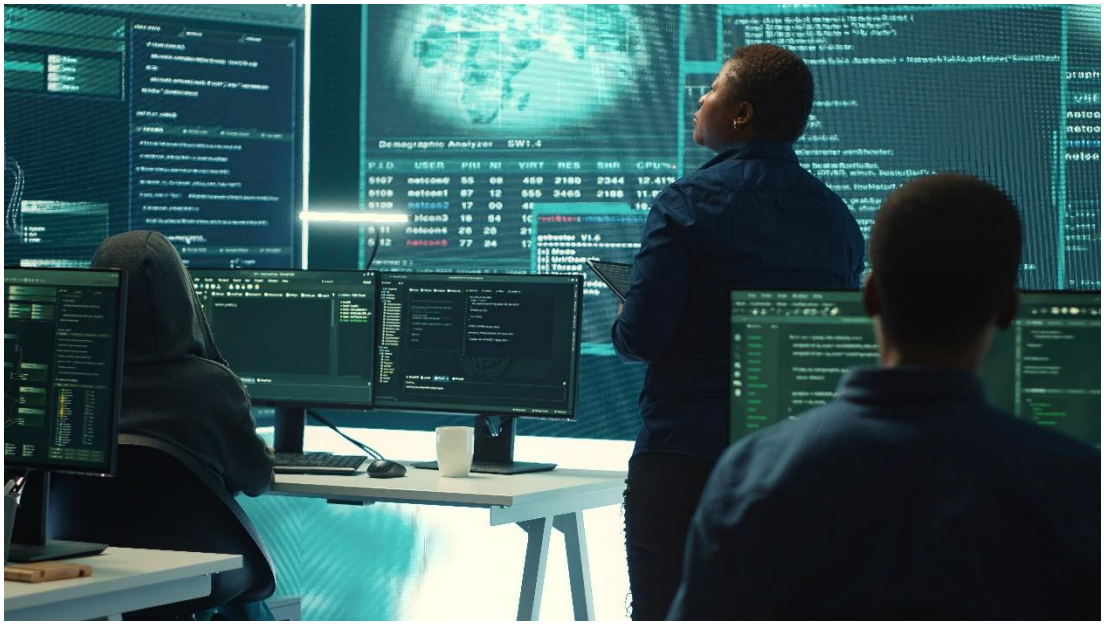
- **Jamming and Signal Interference:** Adversaries use electronic warfare (EW) techniques to disrupt satellite signals, leading to degraded performance and potential loss of connectivity.
- **Eavesdropping and Spoofing:** Unauthorized interception of SATCOM signals can compromise classified communications, while spoofing attacks can mislead operators with falsified data.
    - *Eavesdropping:* SATCOM signals, if not properly encrypted, can be intercepted by adversaries, leading to the extraction of sensitive or classified information. This vulnerability is particularly concerning for military operations and critical infrastructure communications. Advanced signal interception techniques allow attackers to listen to satellite transmissions. Making encryption and secure transmission protocols is vital for protection.
    - *Spoofing:* Attackers can inject fraudulent signals into a SATCOM network, misleading receivers with manipulated data. This can result in unauthorized commands being executed, misinformation spreading across command centers, or disruption of critical decision-making processes. GPS spoofing, for instance, can cause navigation errors for military units or unmanned systems. Effective countermeasures include authentication protocols, signal integrity verification, and GPS independent operation.
- **Cyber Intrusions and Malware:** SATCOM networks, like terrestrial networks, are susceptible to hacking, malware injection, and cyber espionage, potentially leading to service disruption or data theft.
- **Lack of Encryption and Secure Protocols:** Some legacy SATCOM systems lack modern encryption protocols, making them vulnerable to unauthorized access and cyber threats.

Gilat’s SkyEdge II-c and SkyEdge IV Platforms Offer Advanced Modem Technology

To mitigate these challenges, Gilat SkyEdge platforms offer a comprehensive SATCOM cybersecurity framework that is grounded in a detailed Enemy Course of Action (COA) Analysis; this is similar to the methodologies applied in other defense sectors solution incorporating advanced waveform technology, compliance with cybersecurity regulations, and secure modem technologies. Key cybersecurity features include:

Advanced Waveform Technology*

- **Resilient Signal Processing:** Enhances resistance against jamming and interference by employing adaptive transmission techniques:
    - **Frequency Hopping:** Utilizes MFTDMA (Multi-Frequency Time Division Multiple Access) scheme, allocates resources in both frequency and time domains
    - **Burst Transmission:** All Return Traffic is transmitted in bursts, eliminating constant traffic from individual modems
    - **Return Adaptive Coding and Modulation (ACM):** Dynamically assigns symbol rates and modulation-coding schemes (modcods) based on traffic demand, modem capabilities, and channel configuration
    - **Very Low Signal-to-Noise Ratio (VLSNR) Operation:** Enables data transmission in negative SNR conditions, operates down to -15 dB using spread spectrum techniques
- **Optimized Spectral Efficiency:** Ensures maximum data throughput with minimal bandwidth consumption, reducing exposure to interference.
- **Enhanced Air Interface Resiliency (EAIR):** Provides enhanced protection for the M&C traffic sent over the DVB-S2X forward link. It protects it from interception, or the ability to view M&C traffic transmitted over the air, significantly bolstering the system's overall security posture.



IA-PRE Best Practices

- **Infrastructure Asset Pre-Assessment (IA-PRE) Program:** Bolsters the cybersecurity of Department of Defense (DoD) Commercial Satellite Communications (COMSATCOM) systems. The IA-PRE program preapproves commercial assets ranging from single satellites to end-to-end management service architectures. It meets the government and defense-level cybersecurity framework NIST 800-53 Rev. 5, to protect sensitive communications.
- **Secure Network Architecture:** Implements robust security mechanisms to prevent unauthorized access and cyber-attacks.
- Gilat SkyEdge II-c & SkyEdge IV are following the IA-PRE best practices recomendations

Advanced Modem Security*

- **TRANSEC (Transmission Security):** Encrypts transmission paths to prevent interception and unauthorized access.
- **COMSEC AES-256 Encryption:** Ensures end-to-end data payload encryption, protecting classified and sensitive information from unauthorized access and interception.
- **FIPS (Federal Information Processing Standards) Compliance:** Ensures cryptographic security measures align with federal cybersecurity regulations.
- **Anti-Tampering Mechanisms:** Implements hardware and software-level protection to prevent physical or cyber exploitation of terminals.
- **Embedded security:** Includes secure boot and digital signatures to allow safe OTA updates.
- **Audit Logging:** Documenting activity within the SATCOM system that may be used for SoC/SIEM systems to detect anomalies and for forensics.

Conclusion

Cybersecurity is a paramount concern in modern SATCOM networks, requiring advanced security measures to counter evolving threats. Gilat's SkyEdge II-c, SkyEdge IV and their advanced modem technology provide a resilient, secure, and high-performance solution that addresses these challenges through advanced waveform technology, IA PRE best practice capabilities, Security, COMSEC encryption. By integrating these cybersecurity enhancements, SkyEdge Platforms and Gilat's advanced modems ensure mission-critical SATCOM operations remain secure, reliable, and resilient against cyber threats.

* Availability of capabilities may vary by platform or modem