PRD & Teardown for Starlink 2026

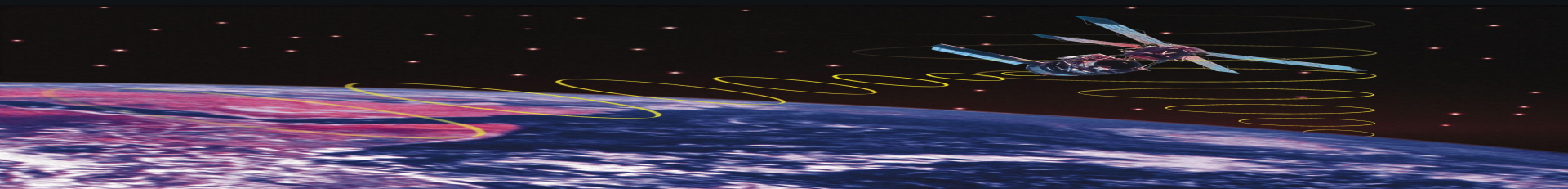
Control Plane Resilience

M.A. Watkins, TPM, BA, Consultant © 2025
mattwatkins.io

For company info: https://starlink.com/

Introduction

“Starlink is the world's most advanced satellite constellation using a low Earth orbit to deliver broadband internet capable of supporting streaming, online gaming, video calls and more…As the world’s leading provider of launch services, SpaceX is the only satellite operator with the ability to launch its own satellites as needed. With frequent, low-cost launches, Starlink satellites are constantly updated with the newest technology…Leveraging SpaceX’s deep experience with both spacecraft and on-orbit operations, Starlink's advanced satellites are produced and operated in Redmond, Washington and Starlinks Kits for customers are manufactured in Bastrop, Texas, all to deliver high-speed, low-latency internet all around the world” (https://starlink.com/technology).

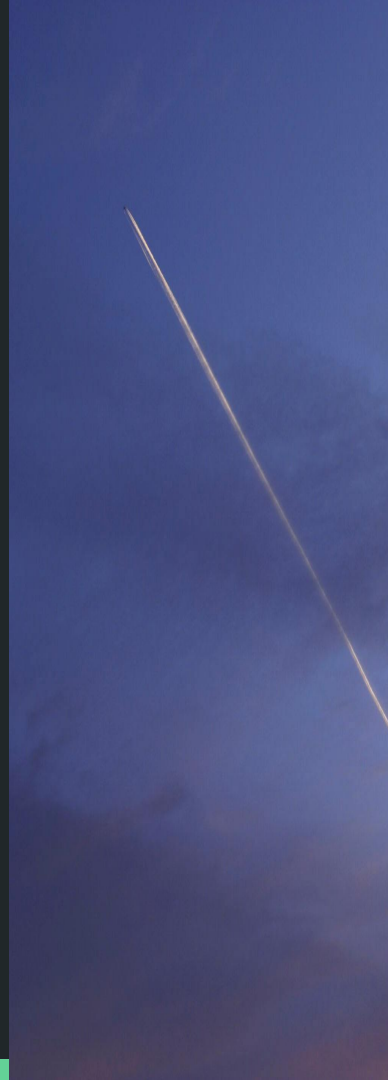


Problem

On January 8, 2026, a massive military-grade electronic warfare (EW) operation in Iran targeted the LEO constellation, causing up to 80% packet loss in urban centers like Tehran.

The event exposed the fragility of terminal-to-satellite handshakes when GPS is spoofed and command frequencies are "drowned out" by state-backed jammers.

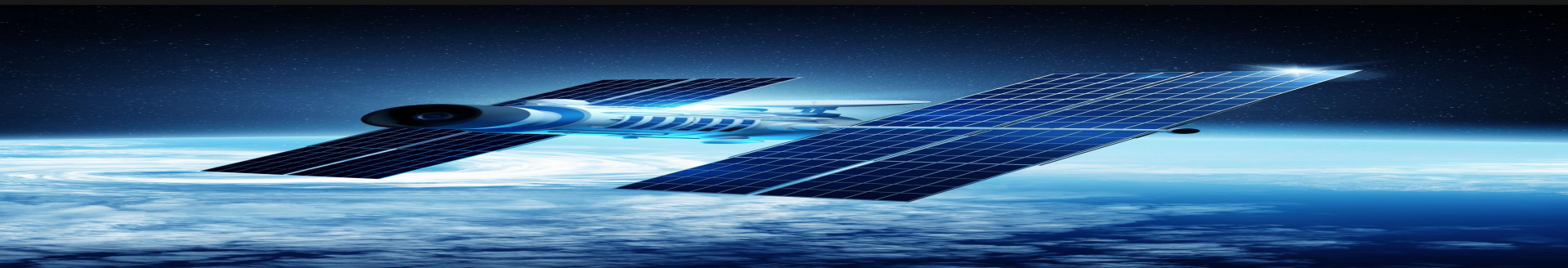
This incident serves as a case study for technical teardown, and need for a product solution for the company to resolve the problem.



Strategic Vision and Roadmap

The 2026 jamming crisis serves as the technical catalyst for Starlink’s business and product shift from a centralized Control Plane to a federated, autonomous Mesh Architecture.

Starlink’s Product Life Cycle is defined by its role as critical sovereign infrastructure, necessitating an SDLC that prioritizes electronic warfare (EW) resistance and autonomous failover.



Product Strategy: GPS-Independent Handshaking

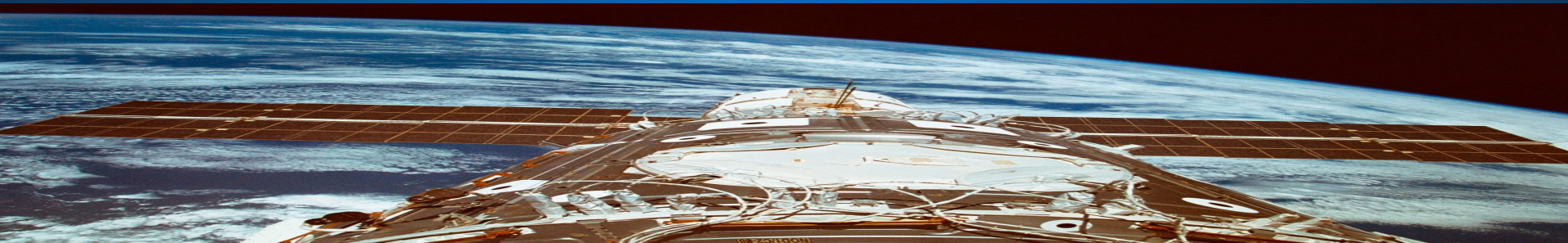
- ➔ Implementation: Update terminal firmware to include Vision-based Positioning or Inertial Navigation Systems (INS).
- ➔ Implementation of A/B Boot firmware to allow instant recovery if an update is corrupted by signal interference.
- ➔ Goal: Allow terminals to predict satellite positions using cached orbital data (ephemerides) instead of relying on external GPS signals, which are the primary target of state-level jamming.

Tech Architecture: Federated Mesh

- Implementation: Transition the Control Plane from a centralized global logic to Federated Regional Clusters.
- Goal: Ensure that a topological collapse in one region (like Iran) cannot be used as a testbed to cascade failures into other regions. This localizes the impact of electronic warfare.
- Updates are sandboxed by region, ensuring a compromised or jammed control cluster in one hemisphere cannot crash the global constellation.

Conclusion: New Product Model

- Implementation: Launch a high-tier subscription for government and NGO clients that includes Hardened Terminals with integrated frequency-hopping software-defined radios (SDR).
- Goal: Monetize the need for survivalism over speed, transforming a technical vulnerability into a premium revenue stream for critical infrastructure users.
- To-Be Goal: Achieving 99.9% uptime even under active wide-spectrum jamming through automated survival mode



References

Doffman, Z. (2026, January 11). “Kill switch”—Iran shuts down Starlink internet for first time. *Forbes*. https://www.forbes.com/sites/zakdoffman/2026/01/11/kill-switch-iran-shuts-down-starlink-internet-for-first-time/

Kan, M. (2026, January 12). Iran appears to be jamming Starlink amid protests. *PCMag*. https://www.pcmag.com/news/iran-appears-to-be-jamming-starlink-amid-protests

The Kenyan Wallstreet. (2026, January 12). How Iran revealed that Starlink is not invincible: Forensic analysis of LEO network vulnerability. *The Kenyan Wallstreet*. https://kenyanwallstreet.com/how-iran-revealed-that-starlink-is-not-invincible/

NetBlocks. (2026, January 8). Iran internet blackout metrics: Nationwide 98% connectivity drop. *NetBlocks*. https://netblocks.org/reports/iran-internet-blackout-metrics-january-2026/

Safai, B. (2026, January 13). An ecosystem of smuggled tech holds Iran’s last link to the outside world. *The Guardian*. https://www.theguardian.com/world/2026/jan/13/iran-internet-starlink-smuggled-tech-jamming