

How AI Drives Fiber Network Expansion

Gary M. Weiner, Founder Apriori Network Systems

AI isn't just about big models — it's about **massive volumes of distributed data and compute**. That demand propagates across **four layers** of the network:

1. Data Center Interconnect (DCI)

- AI clusters are built using **tens of thousands of GPUs**, often spread across **multiple data centers**.
- These require **ultra-low-latency, ultra-high-throughput** fiber between facilities.
- Vendors: Infinera, Ciena, Arista — with fiber underneath, often from Corning, Sumitomo, etc.

2. Metro + Long-Haul Backbone

- AI workloads move across **regions**, between co-location hubs and hyperscaler sites (Google, Meta, Microsoft).
- This drives **terabits per second** of traffic across thousands of miles.
- Fiber networks get **densified** and **diversified** to handle it (hence Zayo, Lumen, etc.).

3. Edge AI / 5G-AI Fusion

- As inference moves closer to users (edge compute), there's a need for **local fiber loops** to link edge nodes, towers, and microdata centers.
- This happens in **metro areas** — often in MTUs or real estate tied to ISPs like Pilot or Stealth.

4. Last-Mile and Intra-Building

- Fiber from basement MMR to AI-driven tenant systems (finance, defense, biotech, etc.).
- Here's where **Apriori lives** — where hyperscalers *don't* protect data and security gets sloppy.

Why Fiber Makers may be (Still) Missing the Point on Security

Wendell Weeks is right: AI is pushing fiber demand through the roof.

But here's the blind spot:

Corning and others have remained focused on fiber volume, not on fiber security.

They are selling bandwidth; low loss / bend radius; Multi-Core Fiber capacity and Quantum-compatible, low-dispersion fiber

The fiber makers are selling nothing at all on eavesdropping or fiber-tap resistant, privacy over fiber, data confidentiality or physical-layer integrity.

Why?!

- Because it's not their job and outside of the U.S. Government, no one is asking for it...yet! Fiber makers view physical-layer security as the domain of encryption (MACsec, TLS, etc.).
- Fiber makers, by virtue of the sizable demand for fiber, serve the hyperscalers, who assume that their campuses and cables are safe from tampering.
- And most of all, there is zero public accountability. The industry isn't regulated to prevent fiber tapping. NSA, CIA, and CISA have not required it — ye

The Apriori Network Systems Opportunity

This is exactly where Apriori Network Systems enters the arena, a group of like-minded friends, associates, and a group of the fiber optic, telecom engineering visionaries, Internationally recognized Optical Fiber Conference Keynote speakers, Bell Labs Fellows and real engineering leaders, helped enrich the approach taken over a patient decade of research, demonstrations and now, ramping up initial pre-production at a time when:

“Everyone’s scaling fiber. No one’s securing it.”

“AI query data is more sensitive than emails — and no one’s protecting it at the physical layer.”

Apriori’s approach is:

- Non-encryption based and no latency added.
- Intrinsic, not retrofitted or encased in metal conduits or armored jacket, but can be if deemed essential, but most cost effective and efficient, naked.
- Effective in short links inside buildings, risers, and edge facilities
- Compatible with QKD & legacy fiber....it is single mode, multi-core
- And covers Layer 1, where MACsec does not, but they both work effectively, together and I go into this further below.

Ignoring this threat is the liability. If we do not catch on to this, others will.