PL
DELIVERING SEAMLESS CONNECTIVITY WITH CableLabs
THE AI FACTORY BACKBONE WITH NOKIA
NAVIGATING NIS2 SUPPLY CHAINS
INTEGRATING INTENT-BASED NETWORKS
TRANSPARENT ENTERPRISE SERVICES
THE FIBER RESURGENCE
UNIFIED NETWORK SECURITY
AI & HYBRID NETWORKS
LIQUID COOLING & STRANDED POWER
DESIGNING SELF-HEALING NETWORKS
NETWORK TRANSFORMATION

www.pipelinepub.com
Volume 22, Issue 3

NIS2 and the New Reality for Interconnection: What US Carriers Need to Know About Supply Chain Transparency

By: Brandon Ross

The new EU network security directive, NIS2, has brought with it a fundamental change in how digital infrastructure is expected to operate, shifting the balance from passing compliance to proactive, provable resilience. At its heart there is a demand for visibility that goes far deeper than anything European carriers have been required to demonstrate before. Operators must know, and be able to *show*, how traffic moves through their networks, which suppliers sit inside critical paths, and where interconnection occurs.

This is a far cry from the old days when IP transit was treated as an acceptable black box. Under NIS2, the lack of transparency that was traditionally baked into long-haul routes, third-party dependencies, and multi-operator transit chains is no longer acceptable. That means visibility is no longer just a nice-to-have layer to give operators an added element of control – it's a fundamental necessity that will change how networks need to be architected from the ground up.

For US carriers with transatlantic business, this carries some immediate implications. Even if domestic regulatory frameworks remain more permissive, operators serving European customers or transporting European traffic will "inherit" the transparency obligations that NIS2 now enforces. Traffic paths that traverse European areas, even briefly, will simply fall under a different level of scrutiny. Architectural decisions that were once based on cost and convenience now have to consider traceability, auditability, and supplier accountability as a minimum. It's a sensible piece of legislation, particularly when you consider the multi-million-dollar disruption that can be caused by outages or security issues cascading through supply chains due to a single, hidden dependency.

NIS2 may be a European directive, but its ripple effects are unmistakably global, and they point to a new era in which interconnection strategy is inseparable from regulatory compliance and competitive positioning.

NIS2’s supply chain impact: new depths of visibility

NIS2 is recasting digital infrastructure as a regulated supply chain in which every dependency must be identified, validated, and monitored. Where previous frameworks concentrated on internal systems and security controls, the new directive forces operators to map the full ecosystem that keeps their services running, including upstream carriers, data center partners, cloud interconnects, and any external provider that touches critical traffic.

Companies must now understand which functions are essential, how failures propagate, and where single points of failure may be hiding. And in order to do that they will require a level of observability that exposes pathways as well as the contractual and operational relationships that hold those pathways together. Put simply, it means that interconnection, which was historically a technical footnote or a way to boost speed and control, is now an important compliance tool.

There’s a cultural angle to all of this too. By its nature, NIS2 elevates business continuity and resilience to the boardroom, requiring executives to demonstrate that they understand how traffic moves through their infrastructure and which suppliers influence service availability. The directive makes clear that resilience can’t be achieved without architectural clarity, and that operators must be able to explain, at any time, where data flows and which entities handle it along the way. While data sovereignty was once a geopolitical question, now it's a question of compliance.

The limitations of traditional transit

Since the Internet first became mainstream, businesses have had the luxury of using regular IP transit to move traffic without thinking too hard about what happens in between. Those who wanted an extra element of security, speed, or control always had the option of directly interconnecting with relevant networks (also known as peering), but it was far from a necessity for the average enterprise.

The public Internet may have been sufficient a couple of decades ago, but data – and our dependency on it – has grown a lot since then, not to mention escalating threat levels and geopolitical tensions. Routes shift, intermediaries appear and disappear, and packets may cross borders or operators without anyone noticing or even *needing* to notice. Under NIS2, that’s not possible. Opaque routing and multi-layered carrier chains make it almost impossible to show precisely where traffic travelled or which suppliers were involved. When an auditor asks for a clear picture of a path, giving them a start point and end point is no longer an acceptable answer. Carriers need to be able to see the full picture of what route their data is taking.

Operators are now naturally rethinking their connectivity architecture. Direct peering and dedicated interconnection hubs give carriers something transit never could – *visibility* and *control*. They know where links land, who sits on the other side, and how traffic will behave under load or failure. When a regulator, customer, or internal team asks for proof of a traffic path, they can provide it without digging through layers of unknown upstream networks. It’s a way of shrinking the unknowns inside the network and bringing transparency back into the operator’s hands.

Automation and optical innovation as enablers of audit-ready networks

As operators take on more responsibility for proving how their networks behave, automation becomes less of an efficiency play and more of a survival mechanism. Manual record-keeping and ad hoc processes can’t keep pace with the level of detail NIS2 expects. Automated provisioning, topology discovery, and telemetry give carriers a living map of their infrastructure rather than a static diagram that’s outdated the moment someone makes a change. When routing shifts or capacity scales, automation creates a digital trail that shows what happened, when, and why. It reduces the guesswork that often surrounds network events and turns day-to-day operations into something that can be explained clearly during an audit.

Optical innovation is playing its part as well. Deployments such as Nokia's 800G-ZR+ single-lambda optics simplify the transport layer by consolidating what once required multiple components into far cleaner, more predictable links. With fewer elements in the chain, there are fewer suppliers to track and fewer points of uncertainty when mapping dependencies. Combined with automation, this forms a foundation where transparency is baked into the network’s DNA, giving carriers a more straightforward path to compliance and a clearer story to tell when regulators come knocking.

Why US carriers need to act

Even though NIS2 is an EU directive, its reach doesn’t stop at the union’s borders. Any US carrier transporting European traffic, hosting EU workloads, or serving customers with operations in the region will be expected to meet the same standards of dependency visibility and operational clarity. In practice, that means questions about traffic paths, supplier chains, and interconnection decisions will increasingly surface in transatlantic contracts and RFPs. A route that briefly enters European territory, a data center operating under EU jurisdiction, or a partner based in an EU member state can all bring NIS2 expectations into play.

There is an upside though – carriers who adapt early will gain a crucial advantage. As European enterprises and cloud providers tighten their procurement rules, they will prioritize partners who can demonstrate clean interconnection paths, predictable routing, and well-documented supplier dependencies. Transparent infrastructure will become a unique selling point, especially as traffic demand surges and others fail to keep up. So rather than viewing NIS2 as someone else’s regulatory burden, US carriers have an opening to position themselves as dependable, audit-ready partners for customers operating across both markets. Resilience and clarity will determine who wins business in 2026 and beyond.