IS YOUR CLOUD BEING TAPPED?

The Security Case For Dark Fiber Between The World's Data Centers

BY SVANTE JURNELL

Today's world runs on data that is being stored and processed in data centers around the world that were for the most part not even conceived of when the world's current international fiber backbones were built. The need for bandwidth between these data centers is enormous, pushing the capacity of existing backbones to their limits and calling for ever more fiber to be deployed and lit.

However, the explosion in traffic volumes is not the only factor driving the need for more fiber. In this article, I'm going to discuss one of the drivers behind the need for more long-haul dark fiber between data centers which is not about the growing traffic volumes per se, but about the separate, equally pressing, need for enhanced security and integrity of the world's networks.

In other words, I would like to shift our attention away from bandwidth for a moment, and instead present some of the ways that the growing awareness, and well-founded concerns, about security-related issues are fueling demand for a greater volume of physical fiber strands on long-haul stretches than what can be accounted for by the sheer increase in traffic. I will also present some of the ways that my own company, Eastern Light, is thinking about these issues and how we are working with them in practice.

EASTERN LIGHT'S FOCUS ON SECURE LONG-HAUL DARK FIBER LINKS

Eastern Light is a Swedish independent company that builds, owns, and operates its own long-haul dark fiber infrastructure in northern Europe, for the express purpose of providing dark fiber connections end-to-end between major data centers in the region. Our speciality is to deliver fully-spliced fiber links all the way from a customer's equipment in one data center in one country the most efficient way to the customer's, or a cloud provider's, equipment in another data center in another country. Our customers are mostly operators and hyperscalers, who install and operate their own active equipment on top of the dark fiber they purchase from us, but increasingly they are also other kinds of organizations with exceptional demands on their data networks. Most of our customers have massive capacity needs, and their reasons for demanding their own dedicated dark fiber, rather than lit capacity, are related to quality, performance, and cost-efficiency. However, we are seeing that the security aspect of controlling one's own fiber is increasingly coming to the forefront, and this aspect is significant for a much wider array of companies and organizations than those with the largest capacity needs.

THREE SECURITY ARGUMENTS FOR DARK FIBER

Most fundamentally, having your own dark fiber onto which you install your own active equipment of your own choosing allows you to have full control and insight into every piece of equipment that your traffic travels through. Aside from the benefits of quality and performance as well as commercial and operational independence, this is crucial in terms of cybersecurity, since it's the only way to ensure

that your traffic doesn't pass through equipment that contains backdoors or that is compromised in any other way.

Secondly, modern state-of-the art encryption technologies – such as optical-layer encryption, which provides both the most secure, most practicable and most cost-efficient encryption solutions of today, as well as tomorrow's quantum encryption – require that one is in control of the physical transmission medium. In other words, one must have one's own dedicated dark fiber all the way between the end points.

A third reason to want to have one's own dark fiber on a certain stretch, rather than lit capacity, is that it gives you insight – in more or less detail, depending on who you're purchasing your fiber from – into the actual geographical position of the physical cable that carries your traffic. This is important in order to ensure full physical separation from other cables for redundancy reasons, but also in order to be able to identify instances where the cable may be vulnerable to unauthorized outside tampering, which I will expand upon in a moment.

THREE WAYS FOR A CABLE OWNER TO PROTECT YOUR FIBER'S INTEGRITY

Even as purchasers of dedicated dark fiber take full control of all of their own active equipment, it's still the job of the cable owner to minimize the risk for outside interference at the optical level, i.e., the risk of unauthorized tapping of the actual light somewhere along the length of the fiber. In this respect, all dark fiber links are not created equal, and at Eastern Light we have worked to address these issues in several different ways. Here I will briefly describe three of our approaches to managing this type of security risk, two of which serve to prevent tapping in the first place, and one which deals with how to detect tapping that is already ongoing or underway.

Firstly, Eastern Light owns and controls – and has exclusive access to – all physical cables as well as all canalization in its network. In other words, when Eastern Light provides a dark fiber link between two locations, the fiber is, along its entire length, located inside Eastern Light's own cables deployed inside Eastern Light's own ducts. Furthermore, the ILA sites which the cable passes through along the way are also fully owned by Eastern Light, and no one – neither customer nor supplier – is ever granted access to these spaces unescorted, but all work is required to be done in the constant presence of Eastern Light's own staff. Together, these rules and routines make it exceedingly difficult for an unauthorized party to gain the sort of physical access to a fiber that would be necessary for deploying an optical tapping device.

Secondly, another security-enhancing factor to Eastern Light's dark fiber links is that there are no connectors or traditional ODFs anywhere. All our fibers are fully spliced end-to-end all the way to the customer's equipment. The original reason for this was to maximize performance and eliminate risk for undesired reflections from connectors which can damage transmission equipment but having as few connectors as possible is also crucial from a security perspective. For someone who wants to attach a tapping device to a fiber, it's easiest to do it in conjunction with an existing connector.

Our third approach concerns how to find out whether optical tapping has already occurred or is underway. If someone, despite prevention efforts, succeeds in placing an optical tapping device along a fiber stretch, this may be very difficult to detect. It is certainly true that any device that taps light from a fiber will, by definition, cause an additional light loss which will have an effect on the measurement results of regular OTDR testing, but such loss may very well be small enough to appear as nothing but a normal splice within the acceptable limits, and therefore not give any reason for suspicion.

For someone who wants to attach a tapping device to a fiber, it's easiest to do it in conjunction with an existing connector.

That is, unless there›s a way to compare such measurement results side by side with historical measurements of the very same link, all the way back to when the cable was first deployed. In that case, any discrepancy in the data between different measurements made at different points in time (such as the sudden appearance of a splice that did not use to be there), can, in the absence of a satisfactory explanation (such as time-stamped documentation of the work that would have produced such a splice), be an indication that there may have been an instance of unauthorized interference with the fiber, and that there is a cause for further inspection.

DEMAND A "FIBER INTEGRITY AUDIT TRAIL"

For this reason, Eastern Light has developed the concept "Fiber Integrity Audit Trail". This means that we do regular fiber measurements to measure technical performance as usual, but in addition we also provide side-by-side comparisons with historical measurement data for the same stretch, along with any relevant documentation of the work that has

been done on the link over time, in order assure our customers and ourselves of each link's sustained integrity.

CONCLUSION

The increasing need for long-haul dark fiber links, for reasons of security and control, means that the world's backbones need to be upgraded with cables with much higher fiber counts than today, irrespective of how much traffic can be squeezed through each fiber.

For the data centers of the world, the increasing demand for customer-specific end-to-end dark fiber links all the way between different data centers, means that they will need to take a closer interest in how the world's backbones are built. It will not be sufficient to note that one has a large number of operators present in one's data center providing great connectivity on the lit capacity layer, but one will need to ensure that there are enough physical dark fiber pairs available all the way between one's various data centers across the globe, in order to be able to satisfy one's customers' need for unbroken fiber all the way from their own equipment in one data center to their own equipment in another data center in a different country.

The challenge to get this in place is significant, but what is at stake is nothing less than the security and integrity of the networks that make up the central nervous system of our modern world, and Eastern Light is committed to continuing its untiring work in contributing to this important development. **STF**

SVANTE JURNELL *is the co-founder and CEO of Eastern Light and is a pioneer within fiber optic infrastructure in the Nordic region. In 1995, he co-founded the telecom and internet operator Utfors which built the first large-scale private fiber network in Scandinavia, and in 1999 he co-founded fiber infrastructure company IP-Only, for which he was the CEO for ten years. He now heads Eastern Light, which operates its own independent sea cable system in the Baltic Sea and builds entirely new and independent long-haul fiber infrastructure across northern Europe for the purpose of providing end-to-end dark fiber connections between major data centers in the region.*