March 2023
Geoff Huston

Submarine Cable Resilience

I have on my desk a rather small tube. It's a little under 2cm in diameter, 6 cm long, and looks like it's made from a dull white polycarbonate material. At the end I can see a copper inner tube, and inside that another polycarbonate layer, and then a smaller steel tube that holds a thin steel thread and some fibre optic cables. There are no layers of steel jacketing, nor any other additional wrapping at all. This is a small section of a fibre optic submarine cable that is laid on the deep-sea floor. It has no protection because at extreme depths there is little in the way of hazards to the cable other than water itself. Shipping anchors and fishing equipment do not usually scour the very deep-sea floor. The only perils at this depth are related to underwater seismic activity such as submarine landslides. This is a calculated risk for cables at such depths, in that seismic-related activity is infrequent enough, and extremely difficult to protect against in any case, so that the cable operator relies on performing repairs if such an event occurs. For cable stretches in shallower waters where there is fishing activity or other forms of shipping activity near a port then the common practice is to wrap the cable in additional layers of spun steel cables. This steel cable wrapper doesn't make the cable impervious to all possible events, such as being snagged by an anchor from a very large vessel, but it helps. And it you really want to minimise the risk of accidental snagging of the cable, then you use a trenching tool to bury the cable into the sea floor, if the sea floor is ploughable.

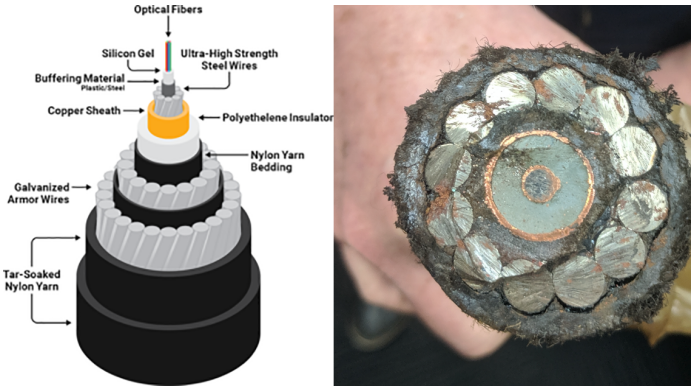

Figure 1 – Cross-section of a submarine fibre cable

But while such measures can help in ensuring integrity of the cable service in shallow waters, they are not absolute, and cable outages still occur in shallow waters. At the end of January Vietnamese Internet service providers reported that the Asia-America Gateway cable and the Asia Pacific Gateway cable went offline. The Asia Africa Europe 1 cable was also experiencing disruption near Hong Kong and the Intra-Asia cable was experiencing problems near Singapore. That somewhat coincidence of outages impacted four out of the five subsea cables that are used to connect the Vietnamese ISPs to the larger Internet.

Subsea cables take weeks or even months to repair. A repair ship needs to position itself near the cable fault point, raise the cable and splice on a repair segment and drop it all back into the water. If the cable was cut, then it needs to repeat this process on the other side of the break. Such specialised ships and their crews are typically contracted to provide a repair service to a number of cables at once, and when multiple faults occur there may be some delay to get an individual cable repaired.

During this repair delay the fifth and final cable servicing Vietnam, the Singapore-Vietnam leg of SMW-3 was also operating in a degraded mode as of 22 February (https://e.vnexpress.net/news/news/vietnam-s-last-functional-undersea-cable-now-malfunctioned-4573176.html) (Figure 2).

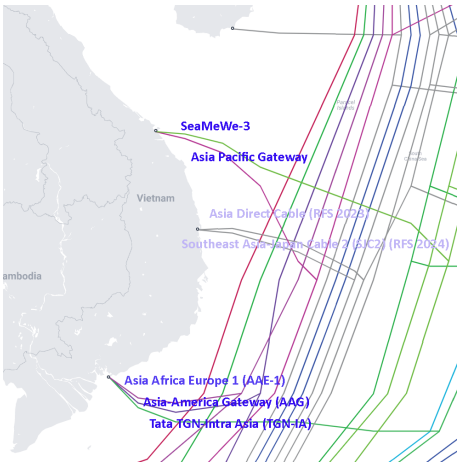

Figure 2 – Cables that service Vietnam (from Teleglobe)

The South China Sea is relatively shallow and there is a considerable amount of maritime traffic as well as fishing fleets, so some level of shipping-related incidents on these subsea cable systems should not be unexpected. However, to experience faults on all five separate cable systems is unusual. And the local area is not without its political overtones because of the conflicting political claims of sovereignty over various parts of the South China Sea (https://en.wikipedia.org/wiki/Territorial_disputes_in_the_South_China_Sea).

Taiwan is also experiencing similar subsea cable problems. The Matsu archipelago, which lies close to mainland China, is connected to the island of Taiwan through two operational subsea cables. In late February it was reported that one of these cables was damaged by a Chinese fishing boat, while the other was damaged by an unknown marine freighter. (https://www.theregister.com/2023/02/21/taiwan_vietnam_submarine_cable_outages/)

This is apparently the 27th time one of Matsu's internet cables have been cut in the past five years, which, again, is an unusually high level of cable disruption. Yes, the Taiwan strait is shallow, with a depth of around 60m between Tawian and the Matsu islands, and there have been periods of sea floor dredging in the area a few years back, in addition to the normal levels of fishing and merchant marine activity in the Strait. Even so, that's a very high outage incident rate.

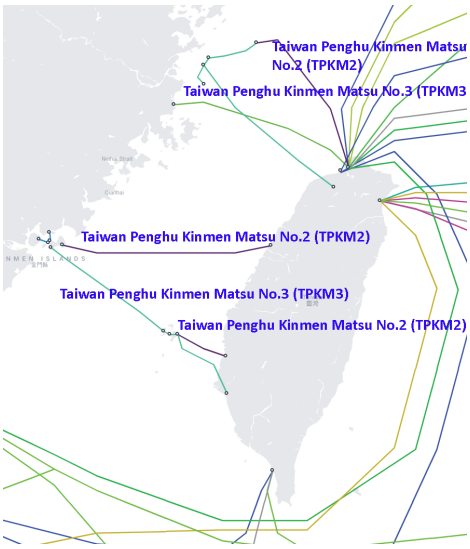

Figure 3 – Cables that service the Kinmen and Matsu Islands (from Teleglobe)

What are the options for connectivity when the existing cable systems are subject to such frequent disruptions?

The response from Vietnam is to plan to install more cables (https://e.vnexpress.net/news/news/vietnam-to-own-three-undersea-cables-by-2025-information-ministry-4570649.html). These are branching connections to the Asia Direct Cable, and Southeast Asia-Japan Cable 2, with a Vietnam landing point midway between the two existing cable landing points.

While it may look like an attractive option to connect to nearby Hong Kong, there is the issue of the ongoing tensions between the United States and China. The US is apparently no longer approving landing rights on any US territory for cable systems that also have landings in China or Hong Kong, forcing large-scale content enterprises such as Alphabet and Meta to concentrate on Singapore as a regional data centre hub for their services. However, the entire South China Sea itself is now considered to be a high risk route by the United States and the most recent high capacity Asian cables that have ownership that includes Google and Meta, namely Bifrost and Echo, both have routes that completely avoid the South China Sea, including Taiwan and Vietnam (Figures 4, 5)

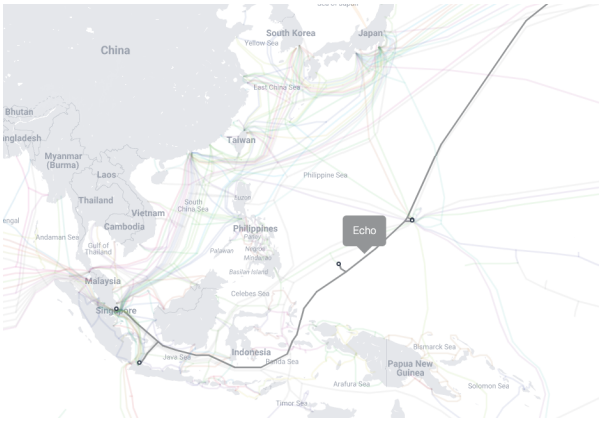

Figure 4 – Google Echo cable route (from Teleglobe)

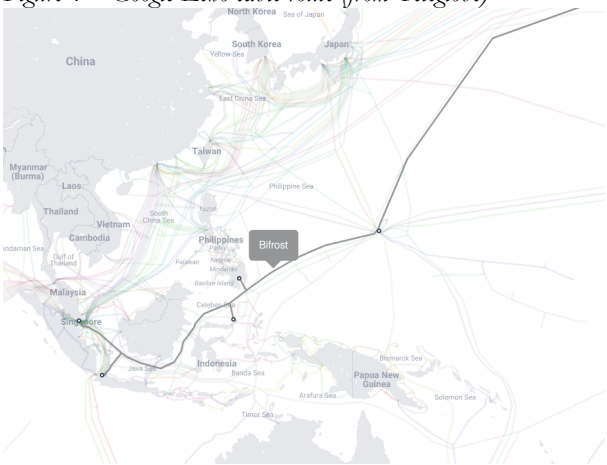

Figure 5 – Bifrost cable route (from Teleglobe)

This form of deliberate disruption of communication has a rich history.

On the 5th of August 1914, a few hours after the UK declared war on Germany a British vessel severed five German overseas underwater cables, which passed from Emden through the English Channel to Vigo, Tenerife, the Azores and the USA.

This cut direct German communications to outside Europe, most significantly to the United States, forcing their traffic to use alternate cable paths that were readily intercepted, as they passed through the UK.

The US entered the war against Germany in 1917 largely because of the interception of the "Zimmermann" telegram which offered an alliance between Mexico and Germany and support for a Mexican attack on the US. The encrypted telegram was transmitted by cable to Copenhagen and then to London for onward transmission over the UK/US transatlantic cables to Washington. The interception and decryption of the Zimmermann telegram was a direct outcome of the earlier cable-cutting activity.

If these disruptions to submarine cable services are accidental, then more cables, coupled with perhaps greater levels of steel cladding and laying the cable in a ploughed trench, sounds like a reasonable response to the problem. But what if these disruptions are deliberate acts of sabotage? How can a nation state protect its communications capabilities in the face of deliberate acts of disruption? If you want to use an alternative to undersea cables, then you need to look at radio-based communications.

Microwave point-to-point services can be used to span distances of up to 150km, and it has been used in many situations as a cost-effective medium capacity service. Parabolic antennae can help in focussing the radio signal between the two points. Such point-to-point radio services have been used for many decades and operate well for medium to large bandwidth requirements. But they are not immune from deliberate third-party efforts to disrupt the signal and jamming can occur if the disruptor can inject a radio signal that interferes with the microwave carrier. However, the biggest limitation of microwave is the line-of-sight distance limit. If the distance to span is greater than 150km then the options tend to head skyward into high bandwidth satellite-based communications.

Data circuits over satellite have been used by the Internet for decades and can certainly be used for long distance infrastructure. Australia made extensive use of such circuits in the 1990's while awaiting the completion of higher speed trans-Pacific submarine cables, and while the additional delay in the circuit to pass the signal up to the satellite and back is less than ideal, they can be used to span hemispheric distances. Can these geostationary satellite data services be deliberately disrupted? Unfortunately, various forms of signal jamming are likely to be effective. If the disruptor can direct a high power signal to the satellite's transponder at the same frequency as the service bearer, then it's likely that the circuit will be disrupted.

What about using Low Earth Orbit communications satellites instead of Geostationary Orbit satellite services? It's an option for certain cases, and today the O3B and Starlink services are available in many parts of the world. Starlink appears to be concentrating on the retail sector, while O3B appears to be concentrating on the communications needs of the business and government sectors. These LEO services are typically simple relay services, in that the client and the earth station need to be located in the same "cell" covered by the satellite as it passes overhead. This smaller footprint has its advantages and disadvantages: it's possible to achieve high capacity from the satellite service and do so with low delay. The limited footprint of each satellite transponder means that any effort to jam the radio signal needs to be located close to the user or the earth station.

There are two additional considerations that relate to LEOs. The first is the use of inter-satellite links in the second generation of Starlink satellites. This makes some forms of radio jamming more challenging, in that the two "ends" of the LEO connection do not need to be geographically nearby. It also potentially extends the coverage and range of a LEO connection, but here the details of this relay-based service are still forthcoming from Starlink, so this topic of inter-satellite signal switching and the way this alters the characteristics of the Starlink LEO service are still a matter of speculation.

The second consideration is also a speculative exercise, about how many other operators may launch LEO satellite constellations.

This is a complex question, as it brings in a number of questions of exactly how high "up" do you need to get to shift from the national sovereignty over the atmosphere] above a national locality to the area of "space law", which, according to a 1967 treaty ratified by over 100 countries asserts the principle that "outer space" is not subject to national appropriation by claim of sovereignty. The only wrinkle here is that the countries that participated in the drafting of the treaty could not agree of an exact definition of where this so-called "outer space" begins. Some countries advocate a 100km altitude, some appear to favour a slightly lower point at 80km while others appear to favour 160km.

The point here is that operators of LEO constellations do not require universal national approval to operate in outer space. Any national approvals that they gather relate to the earth links that they operate, and it's the negotiations over these earth links that apparently dominate the considerations of economic viability of a LEO service. But there are no overall restrictions, national or treaty based, that inherently limit what nation states and enterprises may do in "outer space". If you have access to a launch vehicle that can get your payload into "outer space" then there are no other limitations on what you may choose to do with these space craft in outer space. As the Iridium project found out some decades ago, the major hurdle here is getting the national spectrum approvals to bring the signal back to earth!

Joining Starlink and O3B are Amazon, who has announced plans to launch its Kuiper constellation with some 3,200 satellites in orbits at between 590km and 630km and a long-running series of reports of a Chinese LEO project with up to 12,000 such LEO satellites.

With such a large number of satellites being added to these low Earth orbital planes, each operator's plans for handling the satellites once their operational life is completed are an important consideration. There has been a longstanding conversation about the issues of space debris and a chain-reaction where a critical level of debris at a given altitude could potentially cause a run-away effect by colliding with other satellites, creating more debris, and so on. Once these orbital planes are polluted with debris, they are unusable for all, and for extended periods of time.

So yes, radio-based systems are an alternative to cable-based services, but they are by no means immune from attempts to disrupt the service from a determined and well-resourced adversary. It's more a case of trading one set of vulnerabilities and risks for another set. Our communications systems are fragile, and absolute assurances of integrity of such services, whether they are based on cable or radio, are extremely challenging to engineer into the system. It's simply not feasible to build a high-capacity accessible communications infrastructure if we also need to consider its resilience in the face of a well-resourced and determined adversary. If we can't construct communications infrastructure components that are completely impervious to all efforts to disrupt them, then pragmatically all that's left to us are the mechanisms to bind nation states into positions of common forbearance through international treaties, however unsatisfying that may sound.

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

Author

Geoff Huston AM, B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net