

FINANCIAL TIMES – 27 MARZO 2025

Subsea sabotage puts European power at risk

di Elisabeth Braw

The writer is a senior fellow at the Atlantic Council and an adviser to Disruptive Industries, a threat intelligence company

A spectre is haunting international waters: the spectre of modern life suddenly ceasing because critical subsea cables have been severed.

Along the seabed lie thousands of kilometres of interconnectors that transport electricity between countries, between mainlands and islands, and between offshore installations and the mainland.

These wires are both easy to damage and more difficult and expensive to repair than fibre optic communication cables. That makes them a prime target for acts of sabotage.

Many incidents involving undersea installation damage appear intentional. National politicians such as German defence minister Boris Pistorius have publicly suggested as much.

On Christmas Day, for example, the Estlink 2 power interconnector in the Gulf of Finland stopped working, along with several communication cables.

An oil tanker called Eagle S, seen passing over the cable at the time, was seized by Finnish police and coastguard officers shortly after the cable was disconnected. Finnish authorities suspect the tanker is part of Russia's "shadow fleet" of vessels used to bypass oil sanctions and that it used its anchor to deliberately cut the cables.

But proving intentional sabotage is difficult. Earlier this month Finland released the tanker, although the investigation continues.

Problems distinguishing between deliberate damage and negligence complicates repairs. Standard insurance is null and void for any damage that is the result of a "warlike act".

It is no surprise that Estlink 2's owners — Fingrid and Estonia's Elering — say they will sue the Eagle S's owner, though they may have difficulty tracking that owner down.

Like other cables recently damaged in the Baltic Sea and off the coast of Taiwan, the Estlink 2 stretches along the seabed, buried by a protective layer of soil. It transmits electricity from Estonia to Finland.

In recent years interconnectors have grown significantly in both length and number. Energy companies are installing more cables to link offshore energy fields, including wind farms, with onshore facilities. They are also attempting to use the cables to reduce energy imports from hostile nations.

Interconnectors look like fibre optic cables, but they're far bulkier and more difficult to repair. They do not operate in pairs and most lack the ambulance service that fibre optic cables typically enjoy in the form of repair vessels under contract to mend damage.

Operators are therefore relying on a small pool of repair ships to assist them, Richard Goldring, a longtime consultant to undersea cable insurers, tells me. "That means the outage times are much longer. In the North Sea, you could look at three months. In places with fewer resources, it could be up to nine months."

A severe shortage of repair vessels adds to the delay. Estlink 2's owners struggled to find a repair ship and crew.

Power outages caused by severed cables could have disastrous effects, says Neil Roberts, secretary of the maritime insurance sector's Joint War Committee. "If shops are unable to process transactions, for example, it is easy to imagine almost immediate social difficulties as people may be unable to buy food or fuel."

Extended outages are expensive for operators too. Every day that an interconnector is not working, the operator loses money. "If the repairs cost you €20mn these days, you'd be doing well, but insurers now see claims of closer to €40mn," Goldring says.

High-tech subsea wires are a critical part of our infrastructure. Fibre optic cable attacks are a justifiable cause for concern but electricity interconnections are the vulnerability we should really worry about.