Commentary

In hybrid warfare, acts like the sabotage of internet cables can be devastating, but are hard to prove and prevent, says Ian Li from the S Rajaratnam School of International Studies.

File photo. The C-Lion1 submarine telecommunications cable is being laid to the bottom of the Baltic Sea by cable ship Ile de Brehat on Oct 12, 2015. (Photo: Lehtikuva/Heikki Saukkomaa/via Reuters)

This audio is generated by an AI tool.

SINGAPORE:Two undersea fibre-optic communications cablesin the Baltic Sea were severed within 48 hours of each other in November. Europe is on alert, with suspicions surrounding Russia’s involvement.

For many, this was a clarion call over thethreat of hybrid warfareand a reminder of the vulnerability of undersea cable networks – something the Asia Pacific knows all too well, as home to one of the world’s greatest concentrations of undersea cables.

But determining whether the Baltic Sea incidents arepart of a wider Russian hybrid warfare campaignlinked to the Ukraine war is less straightforward. This is not helped by the fact that there is much ambiguity about what hybrid warfare means.

Hybrid strategies seek to combine individual tools that can be potent on their own but achieve exponentially greater effects when employed together. Ultimately, hybrid warfare is an amorphous term, and like cuisine, each actor’s version has its own unique flavour – and recipe.

Western analysts often label Russia's actions as hybrid warfare. However, it is not a term used by the Russians. Rather, it operates under the framework of New Generation Warfare, which blends various instruments, specifically of a non-military nature, to achieve objectives.

Regardless of what it is called, Russia has placed greater reliance on its unconventional toolkit to gain inroads in the Ukraine war. Despite recent territorial gains in east Ukraine, its military is far from achieving a decisive breakthrough, tying down a significant portion of its conventional fighting force.

Indeed, when one considers the wider spate of sabotage and disinformation activities against NATO countries, and Russian efforts to gain influence in the Global South through information operations, the shades of a broader hybrid strategy begin to emerge, designed to erode Western cohesion and support for Ukraine. The result is a two-pronged assault in both the political and military spheres that could potentially cripple Ukraine's war effort.

Nonetheless, while it is clear that Russia is waging some form of hybrid warfare against Ukraine, and by extension its Western allies, it does not necessarily mean that the cable incidents were part of it.

Russia is not even the only possible culprit, given the likelihood that the damage was caused by aChinese vessel, the Yi Peng 3, which tracking sites said had sailed over the cables around the time they were cut.

A similar incident occurred in October 2023, when two undersea cables and a gas pipeline were damaged by the trailing anchor of a Chinese vessel. Despite initial denials of responsibility, Chinese authorities acknowledged 10 months later thatHong Kong-flagged ship NewNew Polar Bearcaused the damage by accident.

Unfortunately, without perpetual surveillance, it is difficult to establish intentionality, or even attribution, in such incidents. And given the stakes involved, states are unlikely to risk escalation unless guilt can be proven beyond all reasonable doubt.

Given the vastness of the Earth's oceans, and the sheer number of undersea cables, securing the global network in its entirety is impossible. Furthermore, many cables run through international waters, where there is no effective regime to hold potential culprits accountable.

Undersea cables are vital to the functioning of the internet, and while it cannot be conclusively proven that the cable incidents in the Baltic Sea were malicious, they provide a glimpse of how similar acts of sabotage could be employed as part of a hybrid strategy.

For example, in 2023,two undersea cables connecting Taiwan with its Matsu islandswere cut by Chinese non-naval vessels, disconnecting 14,000 people from the internet for 50 days. While there was no evidence that this was a deliberate act on China's part, it is not hard to see how such an incident

might support military operations in the event of war.

The Asia Pacific and its many cables is a fertile hunting ground for would-be hybrid actors. For example, the Straits of Malacca is a critical chokepoint for the region's undersea cables, responsible for providing data connection between Asia, India, the Middle East and Europe, and with its relatively shallow waters, run a high risk of incidents. Should an incident occur there, the impact on regional connectivity would be significant.

While there are no easy solutions, several measures can be adopted to mitigate the threat. The first is for the international community to establish a working regime that governs responses to undersea cable sabotage, and to strengthen multilateral monitoring and repair capabilities. The undersea cable ecosystem is after all a shared global resource.

The second is for states to build communications resilience, acquiring backup sources for internet services and essential communications networks, such as satellite-based and microwave systems, and local fibre-optic networks. While such options provide only a fraction of the connectivity afforded by undersea cables, they will help partially alleviate the impact of a communications blackout.

Finally, borrowing from the hybrid warfare playbook, countermeasures can be adopted in other areas to deter potential sabotage – by addressing key vulnerabilities to strengthen overall resilience, a potential target becomes less attractive for hybrid actors to act against. For example, building social cohesion would allow a country to weather the effects of an incident, while a strong military provides an essential backstop against opportunistic attacks.

After all, if hybrid warfare represents a holistic form of attack, the defence must be just as expansive.

Ian Li is an Associate Research Fellow with the Military Studies Programme at the Institute of Defence and Strategic Studies, S Rajaratnam School of International Studies (RSIS).

Stay updated with notifications for breaking news and our best stories

Get WhatsApp alerts

Join our channel for the top reads for the day on your preferred chat app