

Opinion **Russian politics**

Putin knows that undersea cables are the west's Achilles heel

Moscow has invested in subsurface naval capabilities that hold the world's internet infrastructure at risk

EDWARD STRINGER



© Rory Griffiths/FT/AP

Edward Stringer NOVEMBER 4 2022

The writer is a retired RAF Air Marshal who was formerly director-general of Joint Force Development and director of operations at the UK Ministry of Defence

Late last month, the undersea cable that supplies internet to the Shetland Islands was cut in two places. Such incidents are usually accidents, but the presence of a Russian underwater research ship, and the recent trio of underwater explosions that severed the Nordstream gas pipeline, make Moscow sabotage far more plausible.

Ever since the collapse of the Soviet Union, the west has been able to luxuriate in security through technical superiority. Nato comprehensively outcompeted the Warsaw Pact. We excelled in aerospace technology and built superior submarines. The digital revolution, largely driven from Silicon Valley, further widened the gulf. The Five Eyes intelligence partnership, with eyes and ears in space, reigns supreme. But space and cyber space are increasingly being democratised and can now be accessed at low cost. Hostile powers have calculated that this is where they can attack Nato countries to great effect.

Few are aware just how dependent we are on a limited number of fibre-optic cables that form the internet's spine and electronically link our continents and islands. Currently 95 per cent of international internet traffic is transmitted by undersea cables; satellites, in comparison, convey very little. There are still only about 200 cables around the world – each the size of a large hosepipe and capable of data

cables around the world, each the size of a large hosepipe and capable of data transfers at about 200 terabytes per second. These cables — which carry an estimated \$10tn worth of financial transactions every day — come together at 10 or so international chokepoints, which are particularly vulnerable.

As the Ukraine invasion is reminding us, all wars are economic. Our adversaries have realised that being able to threaten the sanctity of our information and financial systems is a huge strategic advantage. And as Vladimir Putin has long known, the single, physical point of failure in the system that can be overtly threatened is undersea cables. Holding these at risk is a guaranteed way of driving a wedge between Kyiv and the west.

Initially Russian forces targeted energy supply, deploying drones and missiles against the Ukrainian power grid and turning off Nordstream's gas supply to Europe. When these measures were not immediately effective, the Kremlin upped the ante. Three unexplained explosions ripped apart Nordstream I's undersea pipeline off the coast of Denmark, and less than a month later, the Shetlands cable incidents occurred. It is almost certain that Russia blew the pipeline, but breaches of undersea cabling are much harder to attribute as they can be damaged accidentally by trawlers or earthquakes. Indeed this ambiguity helps Putin: he has reminded the west that he has the capacity to cut pipes and cables should he choose, while challenging them to prove that Moscow was responsible.

The problem for Nato and its allies is that the threat is not felt equally. Russia and China, the continental superpowers that are most hostile to the west, are more controlling of their territorial internet and are less reliant on cables linked across oceans, so are not as vulnerable. Even in the satellite age, geography matters.

And so Moscow has developed several naval capabilities to work at depths that Nato considered irrelevant or uneconomic. Russia's flotilla of quasi-military vessels includes specialist survey and support ships for unmanned submersibles and advanced bathyscaphes that can descend to even lower depths. One, the *Boris Petrov* scientific research ship, was tracked in the vicinity of the Shetland Isles cables when they were cut. Most impressive are the old nuclear submarines that have been revamped to act as mother ships to newer, smaller submarines. They are hard to detect and can place explosive charges on the ocean-floor ready for detonation months or years later.

China too is exploiting network vulnerability by muscling into the undersea cable market and offering to lay cables at preferential rates. This has become the nautical arm of the Belt and Road Initiative. Australia and New Zealand have both passed

legislation to prevent interfering with or loitering around undersea cable infrastructure. Canberra also took precautions by installing its own cable to the Solomon Islands.

Western Europe, by contrast, has been less vigilant about who makes or installs its cables. One who spotted this vulnerability early was the then backbencher MP Rishi Sunak, who wrote a paper in 2017 on the growing sabotage threat. Now he is prime minister and the risk has become a reality, will he invest in protective maritime and submarine capabilities as he recommended back then?

[Copyright](#) The Financial Times Limited 2022. All rights reserved.
