THE WASHINGTON POST – 20 APRILE 2026

A critical internet infrastructure lies vulnerable at the ocean floor

di Elena McGovern e Daniel Silverberg

Daniel Silverberg and Elena McGovern are managing directors at Capstone, a policy advisory firm.

The war with Iran may have focused the United States' attention on the Middle East, but the conflict is putting a critical component of global infrastructure at heightened risk far from the Strait of Hormuz.

More than 500 fiber-optic cables run along the ocean floor and carry more than 95 percent of global data and voice call traffic, enabling trillions of transactions in daily commerce. These cables are largely unmonitored, inadequately protected and increasingly targeted. Britain's Defense Ministry recently reported a "30% increase in Russian vessels threatening UK waters in the past two years."

What a patient adversary could do to these cables is plain to see. In November 2024, two fiber-optic cables in the Baltic Sea went dark within hours of each other. One linked Sweden and Lithuania, the other Finland and Germany. A Chinese bulk carrier, the Yi Peng 3, had sailed directly over both around the time each was cut. The next month, a Russian shadow fleet tanker called the Eagle S dragged its anchor for nearly 60 miles across the Gulf of Finland, severing an electricity interconnector and four more communications cables.

U.S. and European intelligence agencies said the lines may have been damaged due to poorly maintained vessels, even as Finnish authorities seized Eagle S and charged its officers with "aggravated criminal mischief." Nevertheless, the incidents exposed a major vulnerability should an adversary treat the ocean floor as a battlefield.

China has developed technology capable of cutting cables at depths exceeding 4,000 meters, far deeper than the average depth of the Baltic Sea, where much of northern Europe's critical infrastructure rests.

The artificial intelligence build-out and Europe's clean energy plans are compounding this vulnerability. AI companies are spending trillions of dollars on chips, power grids and hyperscale computing facilities while leaving their underwater nervous system essentially undefended. Europe's plan to build a wind farm amounting to the largest "clean energy reservoir" in the North Sea depends on undersea cables crossing the same waters where Russia — with every incentive to keep Europe addicted to its oil — has already demonstrated a willingness to act.

In the U.S., the response has been woefully inadequate. Responsibility to protect cables is fragmented across more than 14 entities, none with the authority or resources to act decisively. Congress should designate a single entity — most logically the U.S. Navy — to own this mission. Effectively countering the threat requires rapid response protocols and investments in expanding the cable repair fleet and underwater monitoring.

The Iran conflict has made this threat more acute. Tehran wages asymmetric warfare — drones, mining the Strait of Hormuz, proxy attacks — that follows the same logic as cutting a cable: maximum disruption, with disproportionate cost to the target.

Europe has begun to act. NATO launched Baltic Sentry in January 2025, deploying frigates, maritime patrol aircraft and naval drones across the Baltic Sea. Norway and Britain followed in December with a joint agreement to patrol and protect undersea infrastructure, including the energy cables connecting offshore Norwegian wind farms to British power grids. In February, the European Union committed 347 million euros through 2027 for subsea surveillance systems, autonomous monitoring platforms and rapid repair capabilities.

Finally, NATO's commitment to spend an additional 1.5 percent of gross domestic product on defense-related infrastructure — on top of 3.5 percent for traditional military spending — signals that European governments are serious about protecting critical networks, including cables.

That commitment creates commercial opportunity. Companies operating at the intersection of maritime technology, energy infrastructure and defense stand to benefit from E.U. — and eventually U.S. — procurement of underwater robotics manufacturers, acoustic sensor developers, autonomous submarine systems and satellite-based maritime surveillance platforms. Norway's Kongsberg Gruppen, one of Europe's largest defense companies, is consolidating its defense and underwater technology divisions and expanding operations into the U.S. around precisely this mission.

The cables carrying the AI revolution and Europe's renewable energy transition share the same ocean floor and the same absence of protection. Governments and companies that recognize this will be best positioned to shape the standards, secure the routes and capture the contracts that a serious protection regime will require. The ones that don't will find their ambitions severed at the seabed.