MIND THE GAP -Â A SUPPORTING ANALYTICAL PAPER

By Robin Ashby, Rapporteur, High North Observatory

The First Act of the First World War

At 5am on 5 August 1914, less than twenty-four hours after Britain declared war on Imperial Germany, the cable ship CS Alert slipped out of Dover and began cutting. Within hours she had severed five transatlantic telegraph cables connecting Germany to the world — to North America, to Africa, to the wider global communications network on which the Kaiser's empire depended. It was the first British military act of the Great War, executed before a single soldier had crossed the Channel, before a single naval gun had fired in anger.

The officer who ordered it understood something that took the rest of the world a century to relearn: that the cables lying on the seabed are not infrastructure. They are strategic arteries. Cut them and you do not merely inconvenience an adversary. You blind them, isolate them, and begin the long work of strangling them.

A hundred and eleven years later, on Christmas Day 2024, the oil tanker Eagle S — registered in the Cook Islands, loaded with Russian crude, and assessed by Finnish authorities as part of Russia's shadow fleet evading Western sanctions — dragged its anchor across the seabed of the Gulf of Finland for almost 62 miles, cutting the Estlink 2 power cable connecting Finland and Estonia along with four telecommunications lines. Finnish Prime Minister Petteri Orpo was celebrating Christmas with his family when an urgent call from the Border Guard shattered the holiday.

The cable carried electricity. It carried data. It carried military communications. Its repair would take more than seven months. The wheel had come full circle. The seabed is a battlefield again.

What Lies Beneath

The scale of modern dependence on subsea infrastructure is poorly understood by the general public and inadequately appreciated even in defence circles. Ninety-nine per cent of the United Kingdom's digital communications are now supplied by undersea cables. Globally, these small fibre-optic cables are responsible for carrying 99 per cent of global internet data traffic, facilitating connection and communication worldwide. Every financial transaction, every military communication, every intelligence feed that does not travel by satellite — and most do not — travels by cable. The SWIFT interbank system, the London foreign exchange markets, NATO command communications, the logistics networks of every major Western military: all of it flows along unprotected equipment lying on the ocean floor.

For the United Kingdom specifically, the vulnerability is acute. As an island nation dependent on maritime trade for over 90 per cent of its imports by volume, and now dependent on subsea cables for the overwhelming majority of its digital life, the seabed is not an abstraction. It is the connective tissue of national existence. Energy interconnectors carry electricity from Norway and France. Gas pipelines carry fuel that heats homes and powers industry. Telecommunications cables carry the data flows on which the City of London's financial centre depends.

A sustained, coordinated attack on this infrastructure would not merely be a military inconvenience. It would, within days, begin to destabilise civilian life in ways that no conventional military strike against defended targets could easily replicate. This is precisely why the seabed has become a theatre of competition. Russia's Long Game: GUGI and the Mapping of the West Russia's interest in subsea infrastructure is not a post-2022 improvisation. It reflects a strategic tradition that never paused even during the darkest years of the 1990s when the surface fleet rusted and the ground forces disintegrated.

Even during the Soviet Union's fall, as its military was atrophying and its funding collapsing, Moscow never stopped investing in submarine warfare and developing techniques to map and potentially sabotage adversaries' subsea critical infrastructure. The instrument of this programme is the Main Directorate of Deep-Sea Research — known by its Russian acronym GUGI. NATO's intelligence chief has described it as "a euphemism for a paramilitary structure,

very well-funded, that is mapping out all of our cables and our energy pipelines," equipped with research ships and miniature submarines operating beneath them. GUGI's base at Olenya Guba on the Kola Peninsula — whose defences have been significantly strengthened in recent years, with a new barrier erected across the mouth of the bay — sits at the heart of Russia's northern bastion.

GPS jamming in the area is so intensive that tracking even ordinary civilian ships past the Olenya Guba inlet is impossible. The most visible instrument of GUGI's above-water operations is the research vessel Yantar. Between October 2023 and November 2024, eleven Russian naval and non-military vessels conducted a sustained presence in Britain's maritime area, including near Ireland. When Yantar resumed long-range operations in November 2024, its voyage included stops in waters off northern Norway where it loitered over two cables supplying data and communications to Svalbard, before descending into the North Sea and the English Channel and up to the Irish Sea — where it attracted the attention of RAF maritime patrol aircraft and Royal Navy warships.

Britain has reported that Russian naval activity around UK waters has increased by 30 per cent in the past two years. This is not espionage for its own sake. Russian mapping of the seabed can be seen as a task in line with preparations for war with NATO. With detailed surveys, it will be possible to identify parts of the networks where maximum damage could be inflicted if attacked — offshore substations, clusters where multiple power cables connect, junctions where gas pipes meet. A precise map of Western undersea infrastructure, compiled in peacetime, becomes an order of battle for Day One of a conflict.

The fishing trawler has proved as useful to this programme as the research ship. The vessel Melkart-5, owned by a Russian fishing company within the Norebo Group, has repeatedly shown behaviour inconsistent with fishing activities, including regular presence close to Norwegian critical infrastructure and military sites, and highly unusual navigation in the immediate vicinity of a subsea cable in the Norwegian North Sea, crossing it multiple times immediately before the cable was severely damaged.

A Russian-crewed vessel, the Silver Dania, was detained by Norwegian authorities in Tromsø in January 2025 on suspicion of damaging an undersea cable linking Latvia and Sweden. In June 2025, a further Russian-crewed trawler was observed sailing at normal speed before deliberately slowing directly above a Scandinavian subsea cable. The Cold War intelligence trawler — a familiar sight for those old enough to remember them lurking off Scottish fishing ports, or hearing radio stories — has returned in updated form.

The Chronicle of Damage: 2022–2026

The incidents have accumulated with a frequency that makes the word "coincidence" implausible. Here is the record: Nord Stream 1 and Nord Stream 2, built across the Baltic Sea by Gazprom to carry gas to Germany, were damaged in explosions in September 2022. Responsibility remains disputed and legally contested, but the act demonstrated that major infrastructure could be attacked with strategic effect and limited immediate attribution. In January 2022 and again in April 2021, cables connecting the Norwegian archipelago of Svalbard to the mainland were severed. Russian trawlers were known to be sailing in the damaged cable at the time, but no conclusive findings were made. A cable connected to Norway's Evenes Air Station — a military facility — was cut in August 2022. Norwegian authorities declared the damage "intentional and calculated."

In October 2023, the Hong Kong-flagged vessel NewNew Polar Bear severed the Balticconnector gas pipeline linking Finland and Estonia by dragging its anchor, cutting telecoms cables on the same voyage before heading to a port near St Petersburg. China initially denied involvement; ten months later it admitted the vessel was Chinese, attributing the destruction of a major gas pipeline to "bad weather." In November 2024, the BCS East-West Interlink cable connecting Lithuania and Latvia and the C-Lion1 fibre-optic cable connecting Finland and Germany were cut near-simultaneously in the Baltic. German Defence Minister Boris Pistorius called it an act of sabotage. The Chinese-flagged Yi Peng 3 was held in the Kattegat while European officials sought access; it eventually sailed without a conclusive public finding.

On Christmas Day 2024, the Eagle S cut Estlink 2 and four data cables. Finland responded decisively — boarding the vessel from a helicopter, the first time European authorities had boarded a shadow fleet vessel. The Estlink 2 was not repaired until early August 2025, an outage of more than seven months. The repair cost ran to hundreds of millions of euros. The cost of maintaining the Eagle S under arrest proved so high that Finland ultimately had to release the vessel — the arrest guarantee alone was one million euros, with additional costs of hundreds of thousands per month. Russia had discovered, perhaps deliberately, that the economics of seizure favour the aggressor. In December 2025, Finnish police seized a further cargo vessel en route from Russia on suspicion of sabotaging an Elisa telecoms cable across the Gulf of Finland. By that point approximately ten subsea cables had been cut in the Baltic since 2022, with seven of those cuts occurring between November 2024 and January 2025 alone.

The Legal and Strategic Trap

The pattern of incidents reveals a calculated exploitation of legal ambiguity that echoes the Svalbard dynamic described in the companion scenario paper in this series. International freedom of navigation limits what navies can do in international waters or even within their own exclusive economic zone. A vessel dragging an anchor — or claiming to drag an anchor — is difficult to intercept before the damage is done. Attribution takes months. Legal proceedings take years. The cable lies severed in the interim.

The use of third-country flagging compounds the problem. The Eagle S flew under a Cook Islands flag. The NewNew Polar Bear was Hong Kong-registered. The Yi Peng 3 was Chinese-flagged. Each case triggered different legal jurisdictions, different evidentiary standards, and different diplomatic sensitivities. The most significant legal breakthrough came when the Jaguar — previously flagged to Gabon, which revoked its registration the same day UK sanctions were issued — was boarded by Estonian warships under Article 110 of UNCLOS because it was sailing without valid registration. Estonia had found the legal crack in the wall. But the wall remains substantially intact.

The asymmetry is profound. Russia has its own vulnerabilities but is far less dependent on subsea infrastructure, so NATO has limited options to respond directly in kind. Western societies have built their economic and military communications on a physical layer that is largely undefended and extremely difficult to defend comprehensively. Russia has not.

The Response: Necessary but Insufficient

Western responses have accelerated since Christmas 2024. NATO Secretary General Mark Rutte co-hosted a Summit of Baltic Sea Allies in January 2025, launching the Baltic Sentry mission under Supreme Allied Commander authority, deploying frigates, patrol aircraft and naval drones to monitor the shadow fleet and protect critical seabed infrastructure. In December 2025, the United Kingdom and Norway signed a bilateral naval agreement — described as "historic" by Prime Minister Starmer — under which Britain will use Norwegian missiles for Royal Navy surface vessels, with joint operations from RAF Lossiemouth tracking Russian vessels in the North Atlantic. In February 2025, the EU released an Action Plan on Cable Security covering prevention, detection, response and deterrence. These are welcome steps. They are not yet sufficient.

Baltic Sentry covers the Baltic; the North Sea, the Norwegian Sea, and the approaches to the GIUK Gap present a surveillance and response challenge of far greater scale. The nine P-8 Poseidon maritime patrol aircraft available to the Royal Air Force — against a Cold War fleet of 46 Nimrods — are already committed to anti-submarine warfare tasking, surface surveillance, and Northern Fleet monitoring. Adding comprehensive subsea infrastructure protection to that task list without additional assets is arithmetic that does not balance.

The repair timescale problem has received insufficient attention. The gas grid in the Baltic area is not particularly well integrated with the rest of the European grid; limited sabotage to gas pipelines can have disproportionate effects on Baltic states. For the United Kingdom, whose electricity interconnectors to Norway and France carry a significant fraction of national grid capacity at peak demand, a sustained multi-cable attack timed to winter would not be a military inconvenience. It would be a national emergency.

Conclusion: The Seabed Does Not Change

In 1914, Britain's first act of war was to cut Germany's cables. The lesson taken by the Royal Navy was that communications infrastructure is a legitimate and high-value target, and that Russia absorbed the same lesson and has been acting on it for decades — through GUGI, through trawlers with unconventional navigation patterns, through research vessels that linger over military cable routes with their transponders off, and now through a shadow fleet of ageing tankers whose anchors have become precision instruments.

The seabed beneath the waters around the British Isles, the Baltic, the Norwegian Sea and the approaches to the GIUK Gap carries the connective tissue of Western economic and military life. It is largely unprotected. Its defence requires sustained investment in surveillance capability, legal frameworks that do not reward the aggressor's use of flag ambiguity, repair capacity that can respond within weeks rather than months, and the political will to intercept suspicious vessels before rather than after the damage is done.

The CS Alert knew what she was doing on the morning of 5 August 1914. The question is whether we have relearned that lesson before the next cable is cut — or only after.

This paper should be read in conjunction with Mind the Gap I–V, Zashchitnyy Kupol: Russia's Protective Three-Ocean Dome along the Northern Sea Route (Kupol-3), and the NMD Briefing Paper: Russia's Northern Military District — Losses, Attrition and the Path to Recovery. All published by the UK Defence Forum High North Observatory, March 2026.