RFA Proteus monitors the Yantar, back in November 2024

Picture credit: Crown Copyright

MARITIME VULNERABILITY

Alexander Lord *examines the potential threat to undersea infrastructure as Russian interest in foreign waters increases*

The recent deployment of the Russian 'spy' ship the *Yantar* through the English Channel has sparked fierce debate and concern over Russian activities in European waters. Officially designated as a 'research vessel', the *Yantar* is among the most advanced of Russia's reconnaissance ships and is frequently shadowed by NATO navies whenever it puts to sea. The ship's recent movements in early 2025 are just the latest deployment since the full-scale invasion of Ukraine, after which we have seen a sharp uptick in Russian maritime activity in Northern European waters. So, the question remains: what are these Russian 'spy' vessels doing in our waters and what threat do they pose to Europe's maritime security?

A number of investigations since 2022 have tracked Russian naval and civilian vessels operating in and around Northern European waters. Numerous European naval intelligence services have warned of 'suspicious' Russian activities in their respective waters. Russian 'spy' and civilian vessels have been tracked loitering in highly sensitive areas where critical underwater infrastructure is located, including in the North, Baltic and Irish seas. These investigations have identified a clear pattern of behaviour, which strongly indicates that the Russian Navy is likely conducting a systematic reconnaissance and mapping operation of critical offshore infrastructure across European waters.

For example, in 2023 the Russian 'oceanographic research ship' the *Admiral Vladimirsky* undertook a tour across Northern European waters, sailing throughout the North and Baltic seas. A joint Danish, Finnish, Norwegian and Swedish investigation into the Russian deployment concluded that the vessel was part of a wider effort to survey critical offshore infrastructure, likely including wind farms, undersea telecommunication and other cables and gas pipelines. The vessel was likely attempting to understand how they are connected and identify potential vulnerabilities. The vessel had been identified sailing near Danish and other European critical infrastructure, with its Automatic Identification System (AIS) turned off. However, intercepted radio communications confirm that it was sending its location to a naval base in Russia throughout its journey.

According to Norwegian intelligence chief Nils Andreas Stensones, Russian reconnaissance vessels like the *Yantar* and the *Admiral Vladimirsky* send information gathered during their operations to an intelligence system in Russia. This intelligence can then be accessed by the Main Directorate of Deep-Sea Research (GUGI), a dedicated special naval intelligence command that oversees the mapping of Western infrastructure on the seabed. GUGI strategic operations have ramped up across Northern European waters since the full-scale invasion of Ukraine. Growing reports of damage to undersea infrastructure is leading to concerns that these Russian reconnaissance and mapping operations are facilitating more deliberate sabotage operations.

Prospects of a peace deal in Ukraine are growing in 2025, but so are the risks of a Trans-Atlantic split. As such, Moscow's efforts to deter European states from backing Ukraine will only increase in importance this year. Russia is likely to use reconnaissance operations, cyber attacks, disinformation campaigns and, potentially, sabotage as part of this effort. Such a strategy aims to illustrate to European decision makers and the public at large that their support for Ukraine comes at a price.

Russian strategists have often focused on the concept of 'imposing costs' as a form of deterrence and to achieve Russia's geopolitical objectives. This concept sees Russia use the full range of its military (and some non-military) capabilities to convince an adversary that the costs outweigh any advantages in undermining Russian interests. Moscow's extensive maritime surveillance and underwater naval capabilities are a key part of this strategy; and the Kremlin is likely to leverage the Russian Navy to threaten (or directly impose) significant costs on Russia's potential adversaries in the maritime domain. Maritime assets (including undersea energy pipelines and telecommunication cables) remain economically and militarily vulnerable – making them an attractive target.

Ultimately, the activities of the *Yantar* and other 'spy' vessels are highly likely aimed at providing the Kremlin with a range of credible options to escalate, should it wish to do so. By mapping European critical infrastructure, the Russian Navy is likely attempting to identify potential vulnerabilities to exploit during an escalation or to warn adversaries. If the Kremlin is determined to remind Europe that supporting Ukraine carries costs, then maritime grey zone operations, including espionage as well as sabotage, will likely remain highly credible (and plausibly deniable) options.

The *Yantar* is merely the most famous Russian 'spy' vessel. The Russian Navy has deployed a number of surface and submarine assets that are capable of not only mapping Europe's critical undersea infrastructure, but also of potentially sabotaging or directly attacking it. Over the last two years, numerous states have reported damage to critical undersea energy pipelines and telecommunication cables throughout the Baltic Sea; but there is still fierce debate as to whether this damage was accidental or deliberate. Numerous investigations have found that poor weather conditions, faulty equipment or human error have been responsible for this damage. However, there are numerous other cases which remain unresolved – with the prospect of deliberate sabotage at the forefront of many nations' concerns.

In November 2024, a fault was detected on the C-Lion1 fibre optic cable that runs under the Baltic Sea between Finland and Germany. On the same day, Lithuanian-based telecommunications provider Telia Lietuva reported that another undersea cable connecting Lithuania and Sweden, which intersects with the C-Lion 1 cable, was also cut. More recently, on 21 February 2025, Swedish police confirmed that the C-Lion 1 cable had been damaged once again, and were conducting an investigation into "suspected sabotage". While it remains unclear whether these incidents were accidental, German Defence Minister Boris Pistorius stated that he suspects the 2024 incident was an act of hybrid sabotage, though he refrained from attributing blame.

The damage caused to undersea infrastructure in the Baltic has up until now seemingly been caused by largely rudimentary means; namely civilian vessels dragging their anchors (accidently or deliberately) along the sea floor. Ukraine likely possesses other sabotage capabilities that go beyond this, if it was indeed responsible for the Nord Stream sabotage in 2022 as current investigations indicate. However, the Russian Navy possesses significant and highly sophisticated capabilities to conduct complex, deep-sea sabotage operations that go far beyond such rudimentary methods.

> THE RUSSIAN NAVY CAN ESSENTIALLY ACTIVATE ANY CIVILIAN VESSEL TO SUPPORT ITS OPERATIONS

While Russia's land forces may be struggling in Ukraine, its underwater capabilities outside of the Black Sea have only grown since the invasion, and continue to pose a serious threat to European critical undersea infrastructure. For example, the commissioning of the Belgorod (K-329) submarine in July 2022 marked a major increase in Russia's undersea capabilities. The Belgorod is the largest operational submarine in the world and is specially designed to conduct deep sea operations and act as a mothership for unmanned underwater vehicles (UUVs). The Belgorod's nuclear-powered deep-diving midget submarine, known as a Deep-Sea Station (AGS), is capable of operating on the sea floor and damaging undersea infrastructure. These capabilities represent a significant threat in the event of future conflict with Russia, particularly in the North Atlantic and North Sea. There is limited evidence that Russia is using its naval assets to prepare for sabotage. However, if threat = capability x will, the prospect of a highly capable power with a pressing need to deter European support for Ukraine means these capabilities must be taken seriously.

Recent Russian activity has highlighted just how vulnerable Europe's critical undersea infrastructure remains to potential interference, espionage or sabotage. Given the ever-decreasing hull numbers available to European navies, and the vast expanses of waters that they need to protect, European capabilities to identify and combat potential sabotage operations are lower than they need to be.

Even in the relatively confined waters of the Baltic, which enjoy a significant coverage of NATO installations and concentration of naval vessels, Russian espionage operations have been extensive. In more open seas, such as Irish waters in the North Atlantic, the vulnerability is even more pronounced.

Around 75 percent of transatlantic cables pass through Irish waters, making it of critical importance to the global economy. However, due to the almost complete absence of any Irish maritime capability to protect these waters, and over-stretched Royal Navy capabilities, Europe's North-Western flank remains highly vulnerable. The *Yantar* has already been spotted loitering over concentrations of transatlantic cables in these critical waters on a number of occasions, raising concerns of other Russian activities that have gone, up until now, un-noticed.

NUMEROUS STATES HAVE REPORTED DAMAGE TO CRITICAL UNDERSEA ENERGY PIPELINES

Norway's intelligence chief Stensønes has highlighted mine laying as a particular vulnerability that's hard to counter, particularly given the potential use of civilian vessels as part of these sabotage/reconnaissance operations. It remains possible that operations by 'spy' ships such as the *Yantar* are allowing other Russian vessels, including submarines, to mine critical infrastructure in preparation for a potential future conflict with European states. Russia's latest maritime doctrine, published in 2022, confirmed that the Russian Navy can activate any civilian vessel to support its operations. This means that fishing trawlers and cargo ships can play an equally important role in Russian grey zone maritime operations. This will make it all the harder for NATO naval and intelligence services to identify and prevent potential preparations for sabotage.

Nevertheless, NATO and individual European states are taking this evolving threat seriously. The UK, for example, commissioned its first Multi-Role Ocean Surveillance (MROS) ship into the Royal Fleet Auxiliary (RFA) in 2023, the RFA *Proteus*. The vessel is specifically designed for deep-sea operations, and will prove an important capability to protect European waters. Meanwhile, in 2023, NATO created a new Critical Undersea Infrastructure Coordination Cell, a small but significant step in enhancing allied cooperation to counter the threat. Since then, the flurry of reported damage to critical infrastructure in the Baltic Sea, including damage to the Balticconnector underwater pipeline later in 2023, led NATO to launch its 'Baltic Sentry' mission in January 2025. Such operations will prove vital to enhancing security around Europe's highly vulnerable undersea infrastructure, but these vulnerabilities will, of course, require significant investment to mitigate.

Despite the extensive capabilities available to the Russians, prevailing diplomatic and military conditions in Ukraine make it unlikely that they have imminent plans to launch a large-scale attack designed to cripple Europe's underwater infrastructure. However, this could change. The plausible deniability of small-scale and relatively rudimentary undersea sabotage means it will likely remain an attractive option to the Kremlin in a bid to deter Europe.

Ultimately, the fact that Russian 'spy' ships and other vessels are likely mapping Europe's vulnerable infrastructure and potentially preparing the ground for attacks in the future should give us all pause for thought and underscore the necessity of potent maritime security capabilities that will ultimately keep us, and our highly interconnected energy and digital systems, safe ●

ALEXANDER LORD is Lead Europe/Eurasia Analyst at Sibylline, and is extremely knowledgeable on all aspects of the war in Ukraine. His analysis has been featured on BBC *Newsnight*, in the *Express* and a variety of other publications.

Russian 'oceanographic research ship' the Admiral Vladimirsky was part of a wider effort to survey critical offshore infrastructure and identify potential vulnerabilities

Picture credit: Ministry of Defence of Russia