ROSA & ROUBINI
ASSOCIATES

Policy Compass

Russia's Shadow War and Putin's Forever War

By

Noel Therattil

29 January 2026

Noel Therattil

Russia's Shadow War and Putin's Forever War

29 January 2026

Table of Contents

Rosa & Roubini Associates Ltd is a private limited company registered in England and Wales (Registration number: 10975116) with registered office at 75 King William Street, London EC4N 7BE, United Kingdom.

For information about Rosa&Roubini Associates, please send an email to info@rosa-roubini-associates.com or call +44 (0)20 7101 0718.

***Analyst Certification**: I, Noel Therattil, hereby certify that all the views expressed in this report reflect my personal opinion, which has not been influenced by considerations of Rosa & Roubini Associates' business, nor by personal or client relationships. I also certify that no part of our compensation was, is or will be, directly or indirectly, related to the views expressed in this report.*

***Disclaimer**: All material presented in this report is provided by Rosa & Roubini Associates-Limited for informational purposes only and is not to be used or considered as an offer or a solicitation to sell or to buy, or subscribe for securities, investment products or other financial instruments. Rosa & Roubini Associates Limited does not conduct "investment research" as defined in the FCA Conduct of Business Sourcebook (COBS) section 12 nor does it provide "advice about securities" as defined in the Regulation of Investment Advisors by the US SEC. Rosa & Roubini Associates Limited is not regulated by the FCA, SEC or by any other regulatory body. Nothing in this report shall be deemed to constitute financial or other professional advice in any way, and under no circumstances shall we be liable for any direct or indirect losses, costs or expenses nor for any loss of profit that results from the content of this report or any material in it or website links or references embedded within it. The price and value of financial instruments, securities and investment products referred to in this research and the income from them may fluctuate. Past performance and forecasts should not be treated as a reliable guide of future performance or results; future returns are not guaranteed; and a loss of original capital may occur. This research is based on current public information that Rosa & Roubini Associates considers reliable, but we do not represent it is accurate or complete, and it should not be relied on as such. Rosa & Roubini Associates, its contributors, partners and employees make no representation about the completeness or accuracy of the data, calculations, information or opinions contained in this report. Rosa & Roubini Associates has an internal policy designed to minimize the risk of receiving or misusing confidential or potentially material non-public information. We seek to update our research as appropriate, but the large majority of reports are published at irregular intervals as appropriate in the author's judgment. The information, opinions, estimates and forecasts contained herein are as of the date hereof and may be changed without prior notification. This research is for our clients only and is disseminated and available to all clients simultaneously through electronic publication. Rosa & Roubini Associates is not responsible for the redistribution of our research by third party aggregators. This report is not directed to you if Rosa & Roubini Associates is barred from doing so in your jurisdiction. This report and its content cannot be copied, redistributed or reproduced in part or whole without Rosa & Roubini Associates' written permission.*

Noel Therattil

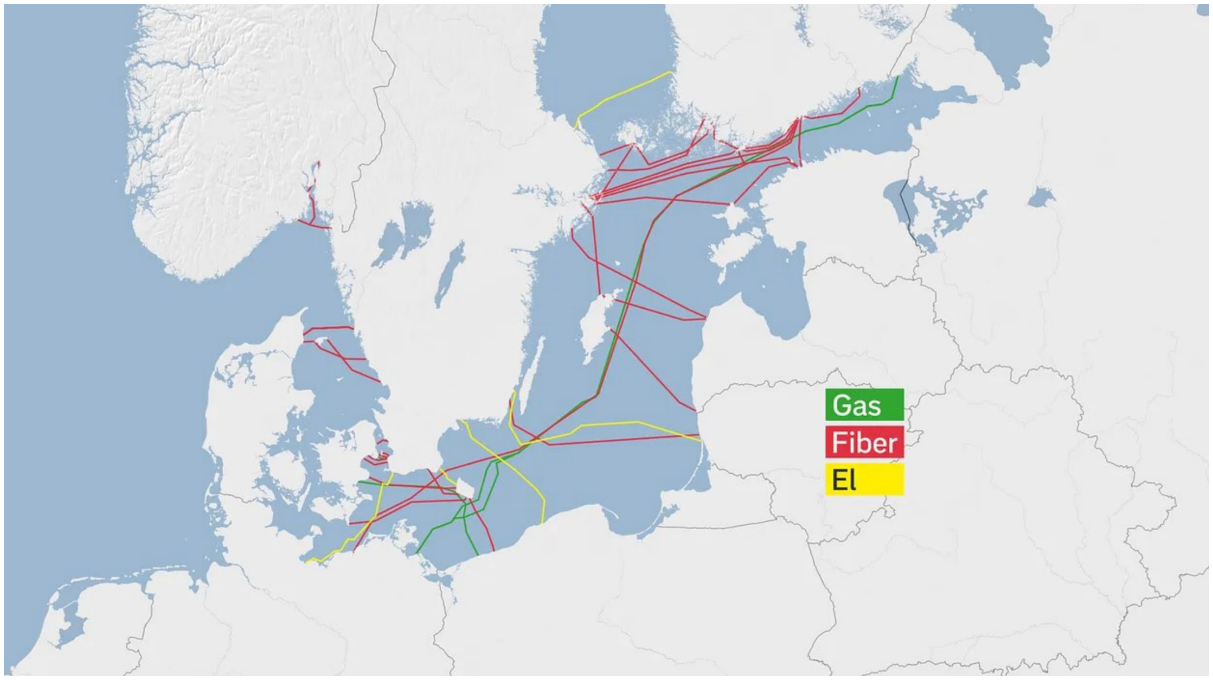
Russia's Shadow War and Putin's Forever War

29 January 2026

Executive Summary

- Through shadow warfare Putin seeks to keep NATO engaged in a 'forever' war at minimum cost.
- Russia's shadow warfare is based on deploying unattributable tactics, low cost high impact operations, and 'gig and platform model' to tap into opportunistic elements.
- Europe and NATO are failing to address Russia's shadow warfare and create strategies for non-conventional conflict. The release of the Fitburg is a quintessential example of this.
- Attack on subsea cables, airports, train and logistics hubs reflect Europe's soft underbelly both in peace time and war time.

Key Picture: Overview of the infrastructure cutting across the Baltic Sea



Source: Infratsructure Cutting

The Fitburg: More Than a Ship

The Baltic Sea is increasingly regarded by regional governments and NATO as a testing ground for grey-zone pressure. Grey zone actions are disruptive acts that impose costs and send political signals without crossing the red line.

The Fitburg

Across Europe, there have been disruptive drone activity around airports, sabotage or interference with railways and energy pipelines, and cyber operations against critical services. Finland's detention of the cargo ship Fitburg is one such case. On 31 December 2025, Finnish authorities seized the vessel after they found damage to a

submarine telecommunications cable between Finland and Estonia. Associated Press has reported that at least 11 Baltic cables have been damaged since October 2023. This explains why even single events now trigger heightened alert. The strategic shadow cast by these incidents is the Nord Stream 1 and 2 explosions of September 2022, which demonstrated that undersea infrastructure can also become a target, with major geopolitical and economic consequences.

Investigators in the Fitburg case consider the incident a serious crime and suspect anchor dragging as a key factor; reports also mention that the cable was damaged within Estonia's exclusive economic zone. Finnish customs checked the cargo for possible sanctions breaches, showing how subsea incidents can quickly escalate into broader enforcement action. For decision-makers, critical infrastructure exposure and inability to attribute responsibility is enough to drive heightened security postures and policy action.

Objectives of Russia's Grey Zone Warfare

Putin seeks to establish a forever war across Europe. The end is not victory but rather to keep NATO bogged down, raise the financial cost of peace, and maintain a climate of uncertainty where Russia holds the cards. Putin seeks to do so without crossing NATO's red lines.

Keeping Europe bogged down

The series of cutting of undersea cables represents a larger tacit of grey zone warfare being deployed by Russia. Both at sea, on land, and in the air, Russia has resorted to grey zone warfare as a cost effective means of pinning down European forces and resources even as Russia itself is bogged down in Ukraine. For instance, in the Baltic sea, cases of damage to sealink were reduced to nil as soon as NATO deployed additional ships and aircrafts to the areas. In Poland, as part of operation Horizon, nearly 10,000 troops may be tied down in operations to prevent the sabotage of rail lines and logistic hubs. Similarly, in the air, NATO air forces have been kept on alert to combat Russian drones and balloons. These drones have disrupted flight operations as far as France. Their presence not only impinges on the sovereignty of European states but also tests NATO's capability to identify, shoot, and track Russian drones. Importantly, it keeps NATO forces occupied for low cost and low risk. Other attacks, such as arson and package bombs require domestic security services to remain on perpetual high alert.

Catch 22

Grey zone warfare also reflects the helplessness of European states. Russian action is enough to provoke costly defensive actions but yet is not destructive or attributable enough to invoke article 5 of the NATO charter. Concomitantly, European countries are still figuring out how to deal with grey zone warfare.

Prior to the seizing the Fritzburg, Finland has also seized a Russian Oil tanker the *Eagle S* for causing damage to the Estlink-2 power cable . The case fell apart because a Finnish court held that the matter could only be dealt with under the UNCLOS and that only the home countries of the accused sailors could prosecute them. Further, the UNCLOS does not explicitly permit warships of non-flag states to interdict vessels on the high seas solely on suspicion of cable damage, reinforcing the importance of evidence and jurisdictional limits. Legally, anchor-dragging is a significant and well-documented cause of cable faults, which keeps plausible deniability in play even when a pattern of incidents raises suspicions.

Further, Russia has adopted a 'gig economy model' where saboteurs are paid through crypto currency and communication takes place on platforms such as telegram. For Russia this keeps costs low for high 'returns', traceability and attribution becomes difficult, and allows Russia to tap into opportunistic elements and local extremists.

Addressing Russia's Shadow War

Incidents like Fitburg matter less for the immediate outage and more for how they force decision-makers to act under uncertainty. Viewed in context, it resembles a playbook: low-visibility disruption in domains where

attribution is hard, and response is slow—whether at sea, in cyberspace, or against surface transport and energy networks.

Future Policy Moves

European policymakers have increased focus on cable security after Russia's 2022 invasion of Ukraine and subsequent undersea infrastructure incidents. Meanwhile the UK parliamentary scrutiny has highlighted that managing subsea disruptions in crises is challenging due to fragmented protection, attribution, and recovery efforts across actors and jurisdictions.

In the short term, the most probable scenario is that operational responses will be driven by tools that function even when intent is unclear: criminal investigation, boarding, inspection, and compliance enforcement. The immediate goal is to reduce harm before intent can be established. In the current scenario, Finland's National Bureau of Investigation seized the vessel on suspicion of damaging a subsea telecommunications cable, and Customs detained the cargo while investigating a potential sanctions offence.

In the medium term, the most likely scenario is the hardening of posture and the institutionalisation of protection. NATO's Baltic Sentry and the EU's workstream on cable resilience points towards more routine surveillance, coordination, and faster repair planning, supported by a shift from policy guidance to operational mechanisms. In other areas, this generally shifts from informal alertness to established resilience measures—more routine monitoring, clearer protocols, and quicker recovery capacity—because deterrence relies on reducing the benefits of disruption.

In the long term, the risk is a securitised seabed baseline where routine faults are consistently viewed through a strategic lens. This is the same strategic drift around airports, railways, pipelines, and digital services. Further, UNCLOS provides a legal foundation by recognising the right to lay cables and requiring states to enact laws criminalising culpable damage or injury to cables. However it does not address enforcement challenges at sea. Due to this, Europe's deterrence approach is likely to rely less on interdiction at sea and more on deterrence-by-denial by improving surveillance and maritime situational awareness, hardening networks, and building rapid repair capacity so that disruption yields fewer strategic gains. In this regard, NATO and the EU emphasise "deterrence" as a key mechanism in response to destabilising acts.

Conclusion

The question that NATO now faces is how to maintain effective deterrence against Russia's shadow war strategy. Will it be an offensive or defensive deterrence? Can NATO retaliate in kind by engaging in low intensity non conventional warfare? As European states struggle to meet military expenditure they are simultaneously also beginning to awaken to the reality of an unreliable US to its west.

NOTES

[1] Sauli Niinisto, (2024) *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, European Commission.

[2] Associated Press. (2025, January 28). *At least 11 Baltic cables have been damaged in 15 months, prompting NATO to up its guard*.

[3] Associated Press. (2026, January 2). *Police in Finland arrest 2 members of cargo ship's crew in connection with damage to undersea cable*.

[4] Reuters. (2026, January 12). *Finnish police release Russia-linked ship held in cable sabotage case*.

[5] Este, J. (2025, October 16). *Putin's forever war against the West*. The Conversation. Retrieved from https://theconversation.com/putins-forever-war-against-the-west-267679

[6] *A rash of Baltic cable-cutting raises fears of sabotage.* (2026, January 6). *The Economist*. Retrieved from https://www.economist.com/europe/2026/01/06/a-rash-of-baltic-cable-cutting-raises-fears-of-sabotage

[7] Harper, J. (2025, November 19). *Poland launches Operation Horizon as sabotage threats rise*. *Anadolu Agency*. Retrieved from https://www.aa.com.tr/en/europe/poland-launches-operation-horizon-as-sabotage-threats-rise/3748288

[8] France24. (2025, December 5). *France takes anti-drone measures after flight over nuclear sub base*. France24. Retrieved from https://www.france24.com/en/live-news/20251205-france-takes-anti-drone-measures-after-flight-over-nuclear-sub-base

[9] Fillingham, Z. (2025, June 5). *Russia's gray zone warfare campaign in Europe*. Geopolitical Monitor. Retrieved from https://www.geopoliticalmonitor.com/russias-gray-zone-warfare-campaign-in-europe/

[10] Associated Press. (2025, August 11). *Finland charges officers of Russia-linked ship that damaged undersea cables*. PBS NewsHour. Retrieved from https://www.pbs.org/newshour/world/finland-charges-officers-of-russia-linked-ship-that-damaged-undersea-cables

[11] International Law Association. (2019). *Submarine cables and pipelines under international law* (ILA Report).

[12] International Cable Protection Committee. (2025, February 24). *Damage to submarine cables from dragged anchors*.

[13] Arak, P. (2025, November 20). *Russia's shadow war: How the Kremlin uses sabotage to wear down Europe*. Atlantic Council. Retrieved from https://www.atlanticcouncil.org/blogs/new-atlanticist/russias-shadow-war-how-the-kremlin-uses-sabotage-to-wear-down-europe/

[14] Besch, S., & Brown, E. (2024, December 4). *Securing Europe's subsea data cables*. Carnegie Endowment for International Peace.

[15] UK Parliament, Joint Committee on the National Security Strategy. (2025, September 19). *Subsea telecommunications cables: Resilience and crisis preparedness* (First Report of Session 2024–26).

[16] Besch, S., & Brown, E. (2024, December 4). *Securing Europe's subsea data cables*. Carnegie Endowment for International Peace.

[17] Finnish Police, National Bureau of Investigation. (2026, January 7). *The Fitburg vessel seized by the National Bureau of Investigation*.

[18] European Commission. (2024, February 21). *Recommendation on the security and resilience of submarine cable infrastructures*.

[19] NATO. (2025, January 14). *NATO launches "Baltic Sentry" to increase critical infrastructure security*.

[20] European Commission. (2024, February 26). *Commission Recommendation (EU) 2024/779 of 26 February 2024 on secure and resilient submarine cable infrastructures* (OJ L, March 8, 2024).

[21] International Institute for Strategic Studies. (2025, August 19). *The scale of Russian sabotage operations against Europe's critical infrastructure* (C. Edwards & N. Seidenstein, IISS Research Paper).

[22] United Nations. (1982). *United Nations Convention on the Law of the Sea* (arts. 112–115).

[23] NATO. (2025, January 14). *NATO launches "Baltic Sentry" to increase critical infrastructure security*