Bright Bird

BRIGHTBIRD.COM

SAYARI

Sabotage at Sea: Tracing Russia's Shadow Fleet Through Corporate and Trade Data

JUNE 2025

Executive Summary

With its recent 17th round of sanctions on Russia, the EU has cast a spotlight on the country's "shadow fleet" — a network of aging oil tankers illicitly transporting oil in circumvention of the G7's price cap and, as recent events suggest, serving as a vector for hybrid conflict and sabotage. The targeted sanctions underscore the importance of corporate and maritime records in identifying the true beneficiaries and operational controllers of these vehicles. Apparent sabotage actions by shadow fleet vessels in the Baltic and North Seas earlier this year have escalated concerns, revealing how these operations could significantly impact European security and economic stability.

This assessment reflects a collaborative effort between Bright Bird and Sayari. By combining expansive corporate and trade records with deep investigative expertise, this partnership has uncovered operationally critical insights into the evolving nature of hybrid threats, sanctions evasion, and the inherent reputational risks driven by the shadow fleet's activities and its opaque networks.

Operational Risk Indicators

The complex networks uncovered in this assessment reveal recurring patterns that can serve as early warning indicators for stakeholders in maritime logistics, insurance, energy, and infrastructure security. These include:

- Shared physical or corporate addresses across multiple vessel managers, especially in key jurisdictions (including well-known secrecy jurisdictions) like the UAE, Marshall Islands, Cyprus, or Panama.
- Rapid turnover of commercial managers or ISM managers, particularly when linked to previously sanctioned entities.
- Inconsistent vessel histories — including gaps in Automatic Identification System (AIS) data, sudden flag changes, or long periods of registry under flags of convenience.
- Recurrent links to sanctioned entities.
- Use of intermediary companies to receive or ship Russian crude oil, especially in jurisdictions with weak transparency standards.

Flagging these indicators during compliance reviews, due diligence, or port inspections can help organizations avoid entanglement in state-enabled hybrid operations and reduce both reputational and operational exposure.

Background and Methodology

Unraveling the networks behind Russia's shadow fleet is inherently difficult. These vessels often operate under flags of convenience and with opaque ownership structures, minimal insurance, and affiliations across jurisdictions that resist scrutiny. In practice, this makes it extremely difficult for claimants to recover costs related to damage, oil spills, or rescue operations — and nearly impossible to hold operators accountable when sabotage or surveillance is suspected.

Sanctions lists reflect the challenge:

- The EU currently lists 342 vessels (264 tankers), following the latest sanctions package.
- The U.S. lists 470 vessels (143 tankers, most suspected shadow fleet participants).
- The UK has sanctioned 73 vessels.

However, there is no comprehensive or universally accepted definition of the shadow fleet, complicating both enforcement and risk assessments. This ambiguity allows actors to operate in a grey zone between legality and strategic subversion.[1]

To pierce this veil, Bright Bird and Sayari combine complementary capabilities. The Sayari Graph platform links maritime, trade, and corporate data to reveal operational overlaps, entity relationships, and commercial patterns. Bright Bird's geopolitical and behavioral analysis interprets these connections through the lens of intent, state strategy, and hybrid threat modeling.

This fusion enables identification not just of the vessels and their owners, but of the patterns of behavior, ownership obfuscation, and risk indicators that define shadow fleet operations. It also allows for operationally relevant insight — moving from raw data to action-oriented intelligence.

The *Eventin* Case

As one example, the Panama-flagged *Eventin*, which was secured by German authorities in January 2025 after the vessel temporarily lost maneuverability, was carrying Russian crude oil and is believed to be a member of Moscow's shadow fleet. Using maritime records, Sayari was able to identify its registered owner, Laliya Shipping Corp, located in the United Arab Emirates. Its only disclosed address, however, is in care of the *Eventin*'s commercial manager, Vaigai Lines, which is registered at an address in Ajeltake, Marshall Islands — an address that Sayari previously linked to multiple shadow fleet vessel registered owners, among other companies.[2]

Use of trust or company service providers (TCSPs) in secrecy jurisdictions is not inherently illegal, though many shadow fleet vessels are registered to owners in the Marshall Islands. Sayari maritime data identified a second Vaigai Lines address that is in care of a company called Koban Shipping LLC, the *Eventin*'s previous commercial manager, suggesting close association between Vaigai and Koban.

1 Baltic Sea: the security risk posed by Russia's shadow fleet," Bundeswehr, February 26, 2025, https://www.bundeswehr.de/en/baltic-sea-russia-s-shadow-fleet-5892544.

2 This separate analysis is available upon request.

At least nine Marshall Islands-registered companies list addresses in care of Koban. Of these, at least five served as commercial managers for Panama-flagged vessels, including *Eventin*, the now-sanctioned crude oil tanker that German authorities encountered in January.

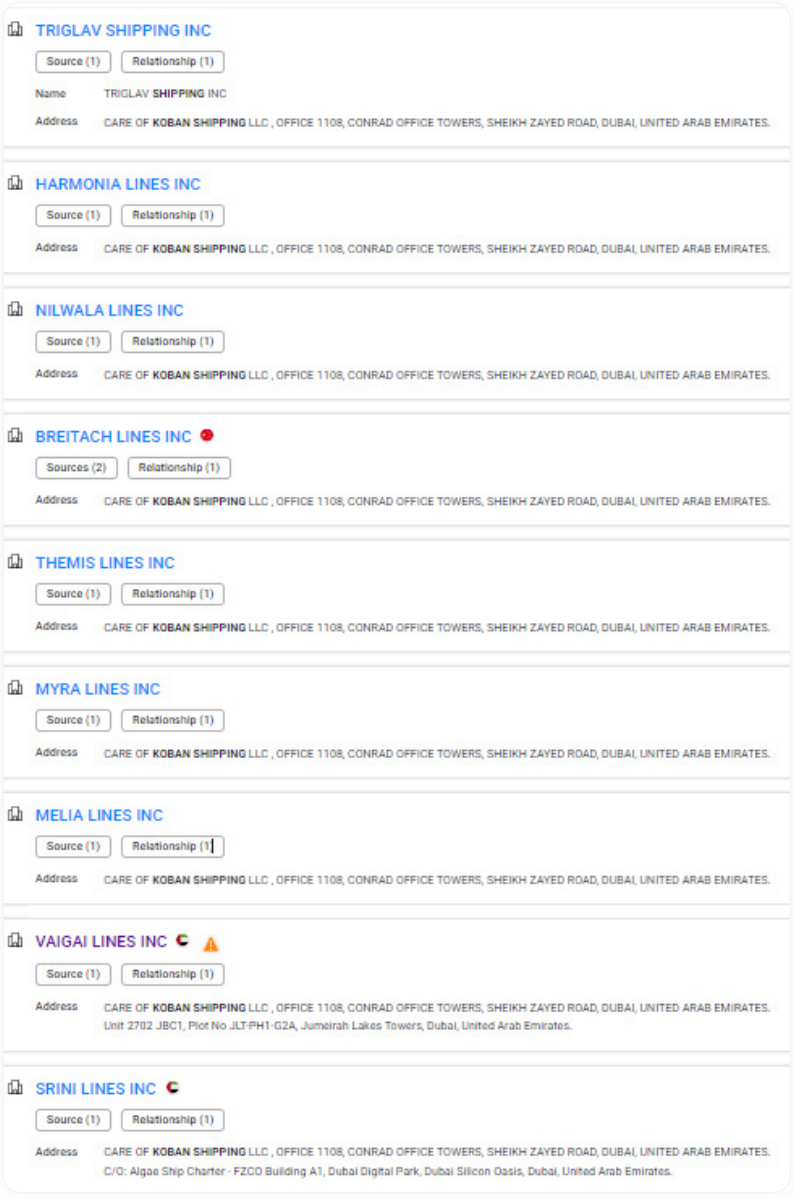

Fig. 1: *Sayari data listing companies that share addresses in care of Koban Shipping LLC.*

These vessels previously shared an ISM manager, an Emirati company called Wanta Shipping LLC-FZ, located in the same office tower in Dubai as Koban. Sayari analysis indicates that Wanta Shipping LLC-FZ has served as ISM manager for at least 22 vessels, all crude oil tankers, at least three of which are known shadow fleet participants (including the *Eventin*). While the other 19 vessels have not been sanctioned, they have a higher potential for connections to the shadow fleet given these associations. For example, one such vessel, *Guanyin*, previously listed its commercial manager as SUN Ship

Management (D) Limited, a UAE-domiciled company, sanctioned by the EU for enabling Russia's war effort in Ukraine as part of the Russian state shipping company PAO Sovcomflot, establishing a potential link between the network of vessels formerly associated with Wanta Shipping LLC-FZ and Russia.[3]

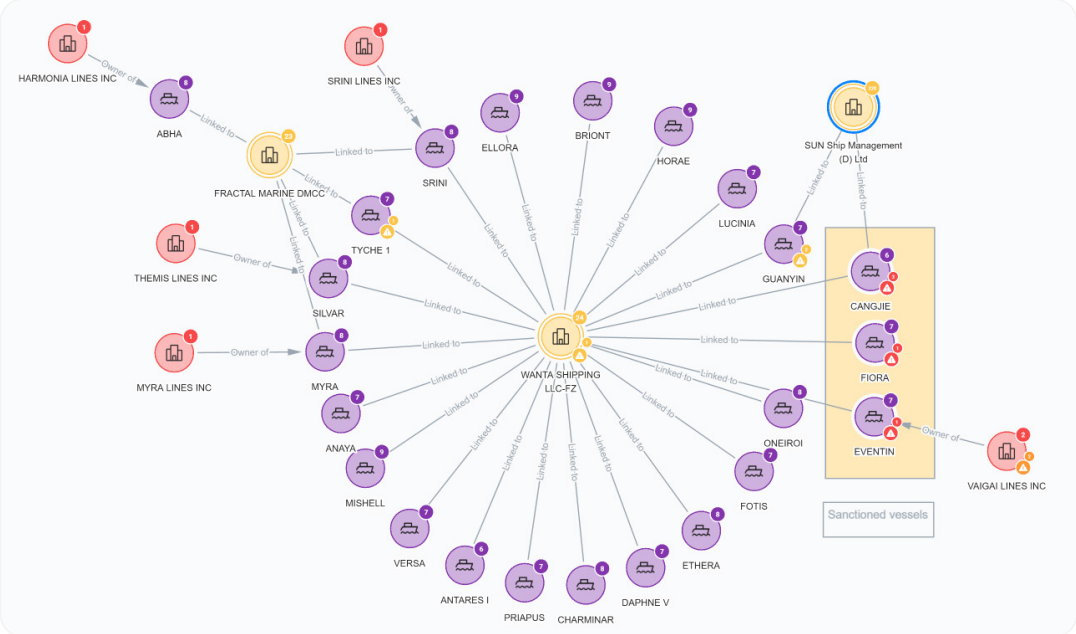

Fig. 2: Sayari Graph network visualization showing companies in red as listed addresses in care of Koban Shipping. These previously served as commercial managers for at least five vessels that shared links to Wanta Shipping LLC-FZ, previously listed as their ISM manager. Two other vessels sanctioned for shadow fleet-related activity also were associated with Wanta Shipping. At least two of the vessels in this network, including the sanctioned Cangjie*, had also prior commercial manager links to SUN Ship Management (D) Ltd.*

Marshall Shipping LLC

Koban Shipping is an alias of UAE-registered Marshall Shipping LLC (alternatively, "Marshal" Shipping LLC), according to Emirati corporate records. These records provide insight into Marshall Shipping's two beneficial owners, Malihah Mohammed Ramadan Ahmed and Ekaterina Rakhbarmadani.

Ekaterina Rakhbarmadani, a Russian national according to Emirati records, is also a minority shareholder (49%) in a UAE-based company called Petrochemix General Trading LLC. Petrochemix has a history of shadow fleet activity, trading oil on behalf of Iran in evasion of sanctions in 2017.[4]

3 EU Sanctions Dubai-Based Inheritor of Sovcomflot's Fleet," *The Maritime Executive*, February 27, 2023, https://maritime-executive.com/article/eu-sanctions-dubai-based-inheritor-of-sovcomflot-s-fleet.

4 Ships Exporting Iranian Oil Go Dark, Raising Sanctions Red Flags," *Fox Business*, July 6, 2017, https://www.foxbusiness.com/features/ships-exporting-iranian-oil-go-dark-raising-sanctions-red-flags.

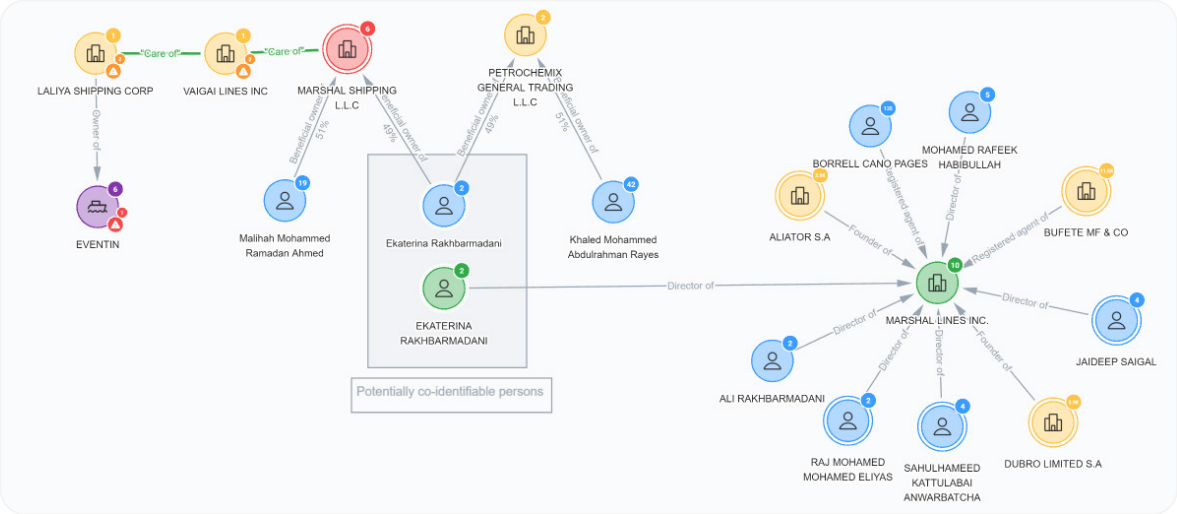

Fig. 3: *Sayari Graph visualization. By combining Panamanian corporate and maritime ownership data with Emirati corporate data, Sayari was able to link Ekaterina Rakhbarmadani, a beneficial owner of known shadow fleet operator Petrochemix General Trading LLC, with both* Eventin *and Panaman-registered Marshal Lines Inc., itself potentially associated with other shadow fleet actors.*

According to social media posts, Ekaterina Rakhbarmadani is married to an Iranian shipping manager named Ali Rakhbarmadani.[5] After living in Iran and then Russia for years, Ali received an offer of employment from an "Arab shipping company," after which it appears they moved to Dubai.[6]

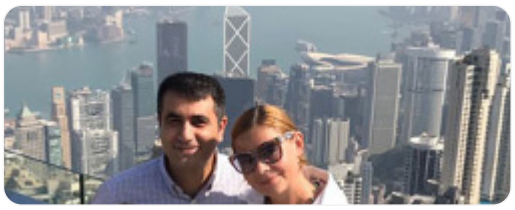

Fig. 4: *Ali and Ekaterina Rahbarmadani, undated social media post.*

Ekaterina Rakhbarmadani also appears in Panamanian corporate records as of August 2024 as director and president of a Marshal Lines Inc. registered in that country. Ali Rakhbarmadani, her husband, is also listed as an officer of that company, along with four other individuals.

Indications were found suggesting potential links — or at least favorable disposition toward — the Russian regime. An Instagram post from the portal PERSONO features her receiving an award from the magazine, stating that she received a letter of appreciation from the Russian State Duma in 2021 "for her high level of professionalism and competence in the field of modernization, improving the quality and popularizing online education in the Russian Federation, as well as for her active public engagement."[7]

5 Favorite Bride of the East - Ekaterina Rahbarmadani," *Bomónd*, July 19, 2020, https://persono.ru/blog/lifestyle/ekaterina_rahbarmadani_assali4ka/ (Russian site).

6 Ali Rakhbarmadani's LinkedIn profile states that he has been a self-employed "shipping specialist" since 2019. However, he also appears in open source websites as vice president of Mairin Shipping and Management Consultancy DMCC in Dubai.

7 Persono Awards (@persono_awards), Instagram photo, Septemer 13 2023, https://www.instagram.com/p/CxJXU3mLPnD/.

This analysis was unable to find independent evidence of such an award. However, recognition from an element of the Russian government while living in Dubai suggests that Ekaterina Rakhbarmadani maintained notable public engagement with Russian government entities.[8]

By combining maritime records connecting the *Eventin* to Laliya, address and corporate records from the UAE, and Panamanian corporate records, Sayari was able to identify this network, additional derogatory datapoints, and other entities that, based on their close association with actors linked to the *Eventin*, may be associated with shadow fleet activity as well.

The *Eagle S* Case and the Black Pearl Energy Trading Network

In December 2024, Finnish authorities seized the *Eagle S*, a Cook Islands-flagged crude oil tanker sailing from St. Petersburg to Port Said, Egypt, on suspicion it had damaged the Estlink2 undersea cable running between Finland and Estonia.[9] While there is little publicly available information on the ship's registered owner, UAE-based Caravella LLC FZ, the company shares its address at the Meydan Hotel in Dubai with about a dozen companies, most of them trading firms, including Conrad Management Company LLC FZ and Black Pearl Energy Trading LLC.

Fig. 5: Eagle S[10]

Both of these companies were sanctioned by the US in January 2025 for enabling Russia's war effort in Ukraine. They are linked to a Latvian national named Aleksejs Halavins, described in open source reporting as a key figure in Russia's efforts to bypass the oil price cap using the shadow fleet and by OFAC as a "prolific buyer of above-price cap Russian oil since 2023."[11] [12] Halavins is also connected to Russian

8 Ekaterina Rakhbarmadani has also appeared in interviews with various Russian media outlets online as a business owner in industries far removed from maritime logistics (e.g. "creative workshops" and nail salons). This lack of relevant background in spite of her corporate associations with shipping-related entities may indicate that she served as a nominal executive, possibly benefitting from connections with parts of the Russian establishment.

9 Eagle S owners could abandon tanker, lawyer says," *Lloyd's List*, January 15, 2025, https://www.lloydslist.com/LL1152236/Eagle-S-owners-could-abandon-tanker-lawyer-says.

10 Gary Dixon, "Court orders seizure of dark fleet tanker suspected of cutting undersea cables," *Tradewinds News,* January 22, 2025, https://www.tradewindsnews.com/tankers/court-orders-seizure-of-dark-fleet-tanker-suspected-of-cutting-undersea-cables/2-1-1767916.

11 Andrey Zayakin, "Our flag means cash: The Latvian trader abetting Russia's billion-dollar oil sanctions evasion," *The Insider*, September 24, 2024, https://theins.ru/en/corruption/274795.

12 Treasury Intensifies Sanctions Against Russia by Targeting Russia's Oil Production and Exports," Press Releases, U.S. Department of the Treasury, January 10, 2025, https://home.treasury.gov/news/press-releases/jy2777.

national Mikhail Silantiev, former head of Promsyrioimport, according to The Insider.[13] Promsyrioimport, a Russian state-owned enterprise, was sanctioned by OFAC in 2018 for facilitating shadow fleet shipments of Iranian oil to Syria. Halavins was potentially also involved in sponsoring Promsyrioimport employees seeking resident permits in the UAE, according to The Insider.

Fig. 6: *Aleksejs Halavins (L) and Mikhail Silantiev (R).*

In a 2022 interview, Halavins presented himself as general manager of a company named Sparta Shipmanagement while providing a Sparta Shipmanagement email on LinkedIn.[14] Sparta Shipmanagement is registered in Cyprus, sharing the same address as another company, Lagosmarine Ltd. OFAC sanctioned Lagosmarine Ltd. in January 2025 for serving as technical manager of a Russian shadow fleet vessel, as well as a number of suspected shell companies potentially linked to shadow fleet activity.[15]

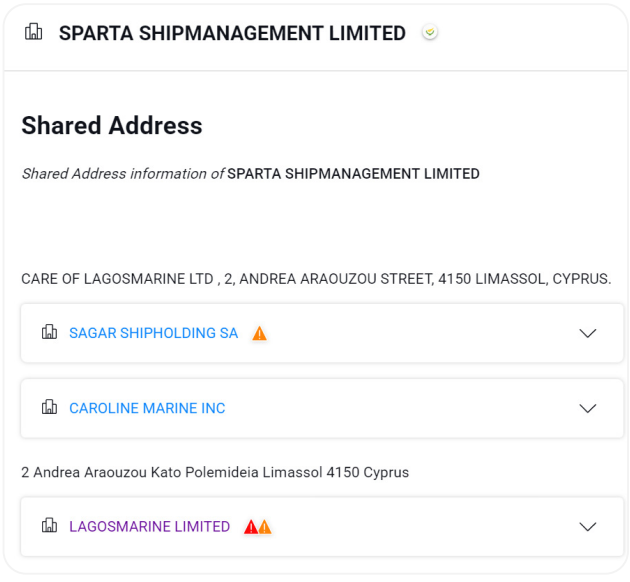

Fig. 7: *Sayari corporate data identified Lagosmarine Ltd. as an entity sharing the same Cyprus address as Sparta Shipmanagement Limited, connecting a company linked to Aleksejs Halavins with an OFAC-sanctioned shadow fleet operator.*

13 Zayakin, "Flag."

14 Beefeater (@Beefeater_Fella), "In a 2022 interview for YoungShip Cyprus, Halavins presented himself as the 'general manager,'" X post, September 28, 2024, https://x.com/Beefeater_Fella/status/1840142812341272908.

15 Zayakin, "Flag."

Both companies are associated with the same Greek national, Dakis Mavroudis, current CEO of Cyprus-based TMS Group, which specializes in "international activities in the marine, offshore, and energy industry." (*sic*) [16] According to records analyzed by The Insider, vessels associated with Lagosmarine, including the sanctioned *Sagar Violet*, regularly navigated between Russian ports and ports in India and China along the exact routes used to move oil sold to Dubai-based companies linked to Halavins.[17]

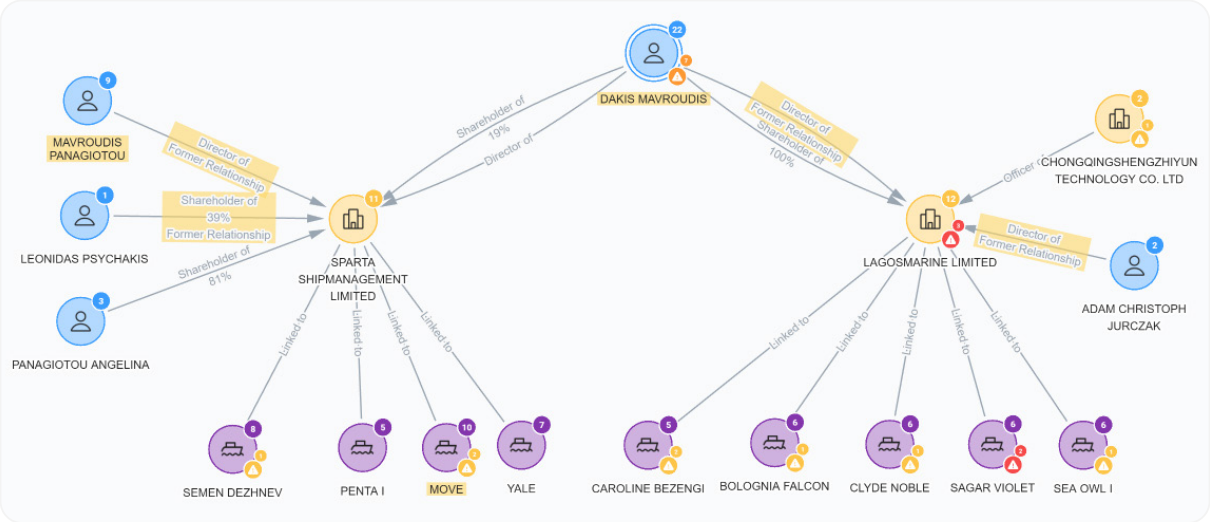

Fig. 8: *Sayari Graph visualization linking Sparta Shipmanagement Ltd., of which Aleksejs Halavins claimed to be general manager, with Lagosmarine Ltd. Both companies share the same Cyprus address and are linked via Greek national Dakis Mavroudis, according to Cypriot corporate records. International maritime records link both companies to several oil products tankers. Some of these vessels are sanctioned for shadow fleet activity, suggesting others may pose similar risks.*

Returning to Black Pearl Energy Trading LLC FZ, Sayari Graph reveals that Black Pearl received at least 30 shipments of "crude oil 'Russian export mixture'" from PJSC Surgutneftegaz (a Russian oil major sanctioned by the U.S., EU, UK, Australia, New Zealand and Japan for shadow fleet activity) between September 2023 and December 2023, according to Russian trade records. Black Pearl received these shipments at ports in India, the UAE, and China, all well-established hubs for shadow fleet activity. Due to inconsistent availability of some Russian trade records, it is plausible that this trade activity continued past December 2023.

16 TMS Group, LinkedIn profile, https://www.linkedin.com/company/tmsgroupeu/.

17 Zayakin, "Flag."

Shipments Received

Arrival Date	Supplier	HS Code	Product Description
2023-12-18	PJSC "SURGUTNEFTEGAZ"	2709.00	CRUDE OIL "RUSSIAN EXPORT MIXTURE", DENSITY AT 20°
2023-12-18	PJSC "SURGUTNEFTEGAZ"	2709.00	OIL "RUSSIAN EXPORT MIXTURE", DENSITY AT 20°C IS NO
2023-12-18	PJSC "SURGUTNEFTEGAZ"	2709.00	CRUDE OIL "RUSSIAN EXPORT MIXTURE", DENSITY AT 20°
2023-12-18	PJSC "SURGUTNEFTEGAZ"	2709.00	OIL "RUSSIAN EXPORT MIXTURE", DENSITY AT 20°C IS NO
2023-12-01	PJSC "SURGUTNEFTEGAZ"	2709.00	CRUDE OIL "RUSSIAN EXPORT MIXTURE", DENSITY AT 20°
2023-12-01	PJSC "SURGUTNEFTEGAZ"	2709.00	CRUDE OIL, DENSITY AT 20°C: 845.9 KG/M3, SULFUR CON

Fig. 9: *Sayari trade data depicting shipments of Russian-export crude oil from U.S. and EU-sanctioned PJSC Surgutneftegaz to Black Pearl Energy Trading LLC FZ. Sayari trade data captures consignor/consignee, countries of origin/arrival, as well as detailed information regarding shipments' Harmonized System codes and shipment descriptions, allowing for product-level analysis of potentially-illicit trade flows.*

Pivoting to Indian trade records, Sayari Graph shows that throughout 2024 (and subsequent to the above received shipments), Black Pearl Energy Trading shipped Russian-sourced crude oil to at least four companies, three of them in India. In the years since the conflict in Ukraine began, India has emerged as a significant importer of Russian crude oil, including oil shipped by the shadow fleet. Indian refineries process the oil into diesel and gasoline for further distribution to global markets.[18] The later dates of these shipments are further indication that Black Pearl Energy Trading continued to receive Russian crude well after 2023 and may still today.

Buyers (4)

Direct Buyers of BLACK PEARL ENERGY TRADING L.L.C-FZ

Buyer	Buyer Country	Number of Shipments	Top HS Codes	Latest Shipment
HINDUSTAN PETROLEUM CORPOR... 20	United States, United Arab Emirates, Australia, Ecuador, India	18	2709.00 — Crude petroleum oils 18	2024-10-10
HPCL-MITTAL ENERGY LIMITED	India	3	2709.00 — Crude petroleum oils 3	2024-11-26
BHARAT PETROLEUM CORPORATLTD 55	India, United States, Singapore, Canada	2	2709.00 — Crude petroleum oils 2	2024-11-28
CNERGYICO PK LIMITED 3	Pakistan, United Kingdom	1	2709.00 — Crude petroleum oils 1	2024-04-05

Fig. 10: *Sayari trade data showing buyers of Russian crude oil from Black Pearl Energy. The dates of these shipments post-date those of Black Pearl's imports from shadow fleet participant Surgutneftegaz (sanctioned by the U.S., EU, and others), suggesting Black Pearl may be transshipping illicit Russian oil to global markets.*

18 Erika Burri, "India is buying lots of crude oil from Russia. Who really benefits?," NZZ, January 28, 2025, https://www.nzz.ch/english/india-is-buying-lots-of-crude-oil-from-russia-who-benefits-ld.1867852.

Conclusion

The shadow fleet's evolution reflects a strategic shift in Russian behavior from covert sanctions evasion to hybrid conflict. This trajectory aligns with Russian concepts of unconventional warfare, which frames warfare as a spectrum that blends military force with economic pressure, covert operations, and information manipulation. Within this framework, maritime logistics are weaponized not just to sustain oil revenues, but to conduct surveillance, sabotage, and psychological operations under a veil of commercial legitimacy. The targeting of undersea cables, port infrastructure, and offshore energy assets reveals a deliberate campaign to test and exploit vulnerabilities in European critical infrastructure, amplifying regional security risks far beyond the maritime domain.

At first glance, the use of flags of convenience and layered ownership across secrecy jurisdictions may appear impenetrable. But as this joint analysis demonstrates, this opacity can be unwound through rigorous, data-driven investigation. Sayari's maritime, trade, and corporate records, combined with Bright Bird's geopolitical risk lens, expose the networks behind these vessels — and the actors enabling them.

These findings also reveal how private commercial actors — insurers, port operators, shipping agents, and energy firms — may unknowingly be drawn into complex hybrid operations that serve adversarial state objectives. By identifying front company behaviors, common address registries, and management overlaps, stakeholders can move from reactive compliance to proactive threat detection.

The complex networks uncovered in this assessment reveal recurring patterns that can serve as early warning indicators for stakeholders in maritime logistics, insurance, energy, and infrastructure security. These include:

- Shared physical or corporate addresses across multiple vessel managers, especially in secrecy jurisdictions like the UAE, Marshall Islands, and Panama.
- Rapid turnover of commercial managers or ISM managers, particularly when linked to previously sanctioned entities.
- Inconsistent vessel histories — including gaps in AIS (Automatic Identification System) data, sudden flag changes, or long periods of registry under flags of convenience.
- Recurrent links to sanctioned entities, such as SUN Ship Management (D) Ltd., or previously identified actors like Petrochemix or Black Pearl Energy Trading.
- Use of intermediary companies to receive or ship Russian crude, especially in jurisdictions with weak transparency standards.

Flagging these indicators during compliance reviews, due diligence, or port inspections can help organizations avoid entanglement in state-enabled hybrid operations and reduce both reputational and operational exposure.

Bright Bird and Sayari's mission is to help clients stay ahead of such developments — by identifying behavioral risk indicators, providing forward-looking threat modeling, and ensuring that business decisions are informed by a fuller suite of authoritative records and risk insights. The integration of investigative methodology and platform-based data gives our clients not only awareness — but real advantage — in an evolving maritime threat landscape.

ABOUT BRIGHT BIRD

Bright Bird A/S is a Danish Strategic Risk Management Partner. Established in 2020, the company specializes in providing tailored risk assessments, operational planning and execution of mitigation strategies for clients operating in complex and high-risk environments.

To learn more, please visit brightbird.com >

ABOUT SAYARI

Sayari is the transparency company providing the public and private sectors with immediate visibility into complex commercial relationships. Drawing on a decade of innovation and support from industry-leading investors, Sayari delivers the largest commercially available collection of corporate and trade data as a dynamic, living model of global ownership and trade activity. Sayari's solutions harness this model to enable risk resilience, complex investigations, and clear-eyed business decisions.

Sayari is headquartered in Washington, D.C., and its solutions are trusted by Fortune 100 companies, financial institutions, and governments in over 35 countries.

To learn how Sayari powers safer global commerce, please visit sayari.com. >