



China and the Iranian and Russian shadow fleets

Marcin Przychodniak

China is using the “shadow fleets” of Russia and Iran to import cheaper crude oil and liquefied natural gas (LNG). This maritime network includes some vessels owned by PRC-based companies, some of which have been linked to hybrid sabotage operations, including in the Baltic Sea. They draw on the experience of Chinese ships from attacks on Taiwan’s critical infrastructure. Countermeasures by EU and NATO countries against China’s involvement in “shadow fleet” operations should include, among other things, more frequent inspections of Chinese ships, as well as the exchange of experience with Taiwan.

The term “[shadow fleet](#)” refers to vessels used by Russia (at least 700 vessels), Iran (approximately 400), and Venezuela (until January of this year) to transport crude oil, petroleum products, and LNG. They are characterised by opaque ownership structures, insurers sourced from outside the G7, manipulation of positioning systems, and STS (ship-to-ship) transfers intended to conceal the origin of the cargo and circumvent price caps. The vessels are also used for sabotage and reconnaissance operations targeting critical infrastructure. The People’s Republic of China is the main recipient of crude oil and LNG, as well as a frequent country of origin for the companies that own the ships and their crews.

Economic significance. For China, the Iranian and Russian “shadow fleets” offer a means of acquiring raw materials at reduced prices. While not critical to China’s overall supply chain, this approach yields short-term benefits and also serves as a tool for cooperating with supplier nations to circumvent sanctions imposed by the G7 and its partners.

No official data is available on imports to China via the “shadow fleet”; however, estimates by the analytics firm Vortexa indicate that in 2025, China imported approximately 1.5–2 million barrels of sanctioned oil per day from Russia. On an annual basis, this accounted for approximately 18% of China’s imports. According to data from Kpler, approximately 1.67 million barrels per day were imported from Iran. In total, in 2025, the “shadow fleet” was estimated to account for approximately 25% of oil supplies to China. The scale of LNG supplies is more difficult to determine. Bloomberg’s estimate is that in 2025, this source

provided just under 2% of China’s imports, mostly from the sanctioned Russian Arctic LNG2 project to the Chinese terminal in Beihai.

To process crude oil, the authorities of the People’s Republic of China have established a network of smaller, privately-owned refineries located in Shandong province. Known as “teapots” due to the shape of their distillation columns, there are approximately 150 in total, with enough processing capacity to handle 70% of all crude oil imported by China, and they are also responsible for refining most of the sanctioned crude oil imports. Their importance grew after 2013, when they obtained licenses and quotas for the import and processing of high-sulphur crude oil from Iran and Venezuela. The Chinese authorities’ control over these companies, beyond imposing import limits and granting licenses, is manifested, among other things, through capital ties with state-owned enterprises (PetroChina, Sinopec) and the use of financial instruments (including loans to selected entities and the regulation of payments in yuan).

Many of the tankers in the Iranian and Russian “shadow fleets” are owned by companies from China and Hong Kong (though few vessels actually sail under those flags), and are manned by Chinese crews, including the captains. It is estimated that among the ships in the Iranian “shadow fleet”, the two main places of registration for the vessel owners are China and Hong Kong. According to Ukrainian intelligence data from 2026, the Russian “shadow fleet” is believed to include 26 vessels flying the Chinese flag (primarily from Hong Kong). Accurately identifying the origin of the vessels and their owners is difficult, both due to the

complex ownership structure of the companies and the frequent falsification of data.

Countermeasures and Sanctions. Some vessels linked to China have been detained by Baltic Sea region countries for illegal activities, and their owners have been subject to US and EU sanctions. At least four such incidents have been recorded to date, including the tanker *Boracay/Pushpa*, owned by a Hong Kong-based company, which was detained by French authorities in September 2025 on suspicion of illegally transporting oil from Primorsk to India, as well as involvement in disrupting operations at Danish airports through drones launched from the vessel. As the French lacked the legal grounds to detain it long-term, the ship resumed its voyage after a few days. However, in March of this year, its Chinese captain was sentenced in absentia by a French court to one year in prison for refusing to hand over documents and allow an inspection of the ship. Another tanker—the *Jin Hui*, sailing under a false Syrian flag and previously managed by entities based in Hong Kong—was detained in May 2026 by the Swedish Coast Guard due to its unclear legal status and the illegal transport of Russian oil. The ship’s Chinese captain was arrested by Swedish authorities, and his case is still pending.

Chinese refineries and oil terminals receiving crude from the “shadow fleet” are subject [to sanctions](#) imposed by [the EU, the US, and the United Kingdom](#). In 2025, the US imposed the first such restrictions on refineries in the PRC purchasing crude from Iran, as well as on recipients of crude from Russia’s Rosneft and Lukoil. The EU included one of the “teapot” refineries in its 19th sanctions package in October 2025. That same month, Chinese authorities announced a suspension of purchases from Russian oil producers by state-owned refineries, but at the same time increased purchase limits for the “teapot” refineries. In May of this year, China suspended loans to sanctioned refineries, but at the same time, it prohibited them from complying with [US sanctions](#)—the first such decision in history.

The security dimension. China’s involvement in the activities of the “shadow fleet” is also part of its cooperation with Russia and Iran in the context of rivalry with the US. This position serves to support the political interests of actors such as those of the Cuban government (a Chinese ship carrying Russian oil attempted to break the US blockade of the island in March of this year), or [Iran in its conflict with the US and Israel](#).

Chinese vessels have concrete experience of sabotage operations, based on operations [against](#) Taiwan. Primarily involving cargo ships causing damage to undersea cables by dragging anchors, there have been several dozen attacks by China since 2023. In June 2026, the first verdict in such a case was handed down—a Taiwanese court sentenced a Chinese captain to three years in prison.

China is applying this experience in the Baltic Sea. In October 2023, the container ship [New Polar Bear](#)—owned by a company from the People’s Republic of China and flying

the Hong Kong flag—was sailing from Shanghai to St. Petersburg via Kaliningrad when its anchor damaged a gas pipeline, a fibre-optic cable connecting Finland and Estonia, and a fibre-optic cable between Sweden and Estonia. The vessel was not detained, but Finnish authorities recovered the anchor at the scene of the incident. The Chinese captain was arrested in May of this year in Hong Kong, but on charges of causing an accident. Proceedings in this case are currently underway in Hong Kong. Similarly, in November 2024, the bulk carrier *Yi Peng 3*, owned by a company from China, was alleged to have damaged telecommunications cables running between Finland and Germany, and between Sweden and Lithuania. It was detained by the Danish Navy but refused to return to Sweden. After a month of negotiations, China agreed to allow Denmark, Germany, Sweden, Finland, and Lithuania (with the participation of Chinese representatives) to conduct an inspection; however, the inspection failed to produce evidence of sabotage. The vessel was allowed to sail away, and Sweden, Denmark, and Finland’s investigation was closed due to a lack of cooperation from the Chinese side.

Conclusions and Recommendations. China’s participation in the operations of the Russian and Iranian “shadow fleets” allows it to procure cheap crude oil and LNG from sanctioned countries. This practice is politically and economically advantageous, while also requiring minimal investment. China’s involvement boosts the Russian and Iranian state budgets, and thus also supports their military-industrial complexes. Though not actively part of the “shadow fleet” (they do not transport oil or LNG and do not operate in the grey zone), some vessels sailing under the Hong Kong flag are commanded by Chinese nationals and cooperate with Russia by providing support for sabotage operations in the Baltic Sea.

To counter the negative effects of China’s activities on European countries, Taiwan’s experience of Chinese operations could prove useful. This could be an important area of cooperation with NATO and the European Union. This includes elements such as a greater focus on monitoring and intercepting Chinese vessels that violate sanctions, as well as information-sharing about their actions. There is a need to expand monitoring infrastructure (including hydrophones) to detect sabotage and effectively attribute responsibility, as well as to conduct patrols by deploying units with these capabilities, such as maritime drones. Legislative initiatives that increase the costs of liability for sabotage—including those enabling the confiscation of ships, their equipment, and cargo—are also important. EU sanctions imposed on Russia should take into account the involvement of Chinese entities in “shadow fleet” activities by imposing further restrictions on Chinese refining companies as well as shipowners. It is worth considering cooperation between the EU and states such as the US, South Korea, and Japan to restrict the expansion of the “shadow fleet” and block its vessels from accessing maritime services.