Deloitte.

Navigating Sanctions

Understanding circumvention techniques, involved countries and challenges for financial institutions regarding Russia

June 2024

Overview

This white paper aims to enhance awareness among European financial institutions about general sanction circumvention strategies employed globally. It provides an updated overview as of June 2024, reflecting the evolving landscape of sanctions. This includes the recent 13th EU sanctions package implemented in February 2024, which focuses on further restricting Russia's access to military technologies, particularly components used for drones. By bolstering risk management and ensuring adherence to international sanctions, the paper supports financial institutions to safeguard the integrity of the global financial system and mitigate inadvertent non-compliance risks linked to sanctions. The EU sanctions are complex, fast-changing and unique, for instance through their extraterritorial effect. The journey continues now with the 14th package of sanctions against Russia, which has been approved by the EU member states on June 20, 2024, and potentially more to come...

EU Sanction Lists[1]

- Approx. 1,700 individuals
- Approx. 420 organisations

Blocked Russian Central Bank Reserves[2]

- EU: Approx. €200 billion
- EU, other G7 countries and Australia: Approx. €300 billion

Impact on Russian Economy in 2023 (World Bank)[3]

- GDP drop by 0.2%
- Imports increased by 4.1%
- Exports dropped by 4.6%

Impact on Russian Banking System Worldwide[4]

- Bank assets under sanctions: 70% of total assets
- SWIFT exclusion: 10 Russian banks

Sanction Circumvention Techniques

Our recent research shows that the sanction circumvention techniques of Russian sanction objectives can be categorized into three main groups:
01. Financial transactions,
02. Trade activities, and
03. Ownership structures.

01. Financial Transactions

This section explores Russia's evolving circumvention tactics in response to growing financial sanctions. It covers traditional methods like using an Intermediary Company and the SPFS alternative to SWIFT, as well as emerging systems such as Virtual Currency and Dark Net transactions.

Sanction circumvention in financial systems can be achieved through four primary methods.

Intermediary Company

The first method involves using the conventional payment system by using intermediary companies, often exhibiting money laundering patterns. According to a joint alert issued by FinCEN and BIS in May 2023, newly identified red flags indicate potential sanctions evasion. These include:

1. Payments for defense or dual-use products from newly established companies in non-GECC countries after February 24, 2022, or from new customers trading specific HS code products after incorporating post-February 24, 2022, in non-GECC (Global Export Controls Coalition) countries.
2. Existing customers receiving certain HS code exports for the first time after February 24, 2022, or non-U.S. customers significantly increasing orders of specific HS code exports post-February 24, 2022.
3. Transparency issues and unusual behaviours, such as customers refusing or unable to provide details about end users, intended use, or ownership. This also includes transactions involving smaller payments from the same foreign end user to multiple suppliers of dual-use products.
4. Unusual business practices, such as parties listed as ultimate consignees that are not typical consumers (e.g., financial institutions, mail centers), or significant overpayment for commodities compared to market norms.[5]

A company establishes a new entity in a third country not bound by EU sanctions. The company then makes a payment to this new entity, which subsequently transfers the funds to the EU.

1. https://www.consilium.europa.eu/en/policies/sanctions-against-russia/ (as of June 19, 2024).
2. https://www.consilium.europa.eu/en/infographics/impact-sanctions-russian-economy (as of October 2023).
3. https://www.consilium.europa.eu/en/infographics/impact-sanctions-russian-economy (as of October 2023).
4. https://www.gtai.de/de/trade/russland/zoll/eu-sanktionen-gegenueber-russland-811200#toc-anchor--29 (as of June 19, 2024), https://www.consilium.europa.eu/en/policies/sanctions-against-russia/ (as of June 19, 2024).
5. https://www.bis.doc.gov/index.php/documents/enforcement/3272-fincen-and-bis-joint-alert-final-508c/file (as of June 19, 2024).

SWIFT Alternatives

The second method involves the usage of the newly established Financial Messaging System of the Bank of Russia (SPFS) as an alternative to SWIFT. In 2014, when facing lighter SWIFT sanctions due to the Annexation of Crimea, Russia rapidly developed The Financial Messaging System of the Bank of Russia (SPFS) to fortify its domestic payment system. This alternative to SWIFT, with around 10,000 members, served as a preventive measure in anticipation of potential global SWIFT restrictions.[6] Concurrently, Russia diversified its financial infrastructure by shifting foreign reserves away from the USD and establishing stronger ties with the Chinese Cross-Border Interbank Payment System (CIPS), capable of settling international claims in RMB. The use of alternative payment systems gained further prominence when certain Russian banks were recently excluded from the global SWIFT system as well as international financial institutions and intermediaries being under watch for the facilitation of transfers to/from Russia.

For instance, in June 2024, OFAC updated the Specially Designated Nationals and Blocked Persons List (SDN List) for five Russian financial institutions. The updates include: 1) Promsvyazbank Public Joint Stock Company: Beijing (China), Bishkek (Kyrgyzstan), and New Delhi (India); 2) State Corporation Bank for Development and Foreign Economic Affairs Vnesheconombank: Beijing (China) and Mumbai (India); 3) Sberbank: Beijing (China) and New Delhi (India); 4) VTB: New Delhi (India), and Beijing and Shanghai (China); 5) VTB Capital Holdings Closed Joint Stock Company: Hong Kong (China).[7] Foreign financial institutions with substantial USD transactions or exposure should implement enhanced due diligence (EDD) for high-risk goods, services, or entities in high-risk jurisdictions. All parties involved must provide detailed documentation on the origin of goods, end-users, and intended use.
The EU Commission proposes that financial institutions maintaining correspondent accounts for foreign financial institutions are required to establish appropriate, risk-based enhanced due diligence frameworks. These frameworks should include policies, procedures, and processes designed to assess and mitigate the inherent risks associated with these relationships, including the processing of wire transfers, international trade settlements, remittances, and cross-border payments.[8]

6. https://cyberft.com/about/comparison (as of July 2023).
7. https://home.treasury.gov/news/press-releases/jy2404 (as of June 19, 2024).
8. https://finance.ec.europa.eu/system/files/2023-12/guidance-eu-operators-russia-sanctions-circumvention_en.pdf (as of June 19, 2024).

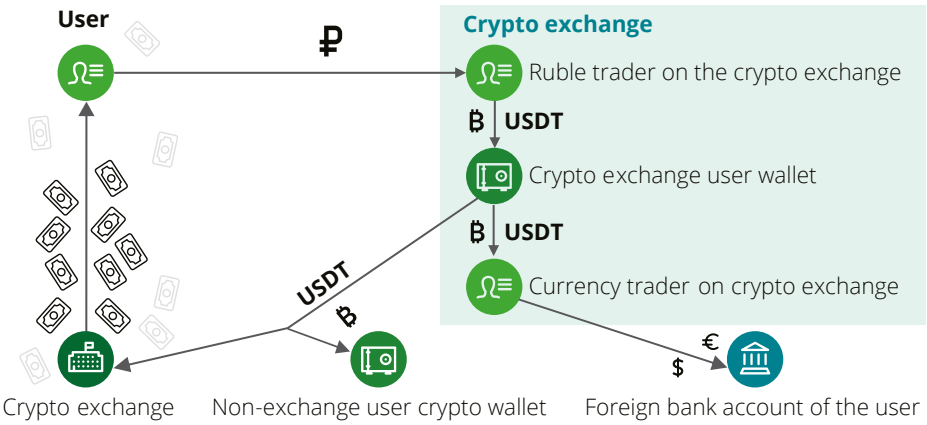
Virtual Currency

Additionally, the SWIFT ban may drive increased virtual currency use to evade financial sanctions. For example, Garantex, a virtual currency exchange established in 2019 in Estonia, primarily operates in Moscow. Known transactions involving Garantex reveal associations with illicit actors and darknet markets, totaling over $100 million. In April 2022, the U.S. Department of the Treasury imposed sanctions on Garantex, citing its participation in ransomware activities linked to Russian criminal groups, leading to its inclusion in the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals (SDN) list.[9]

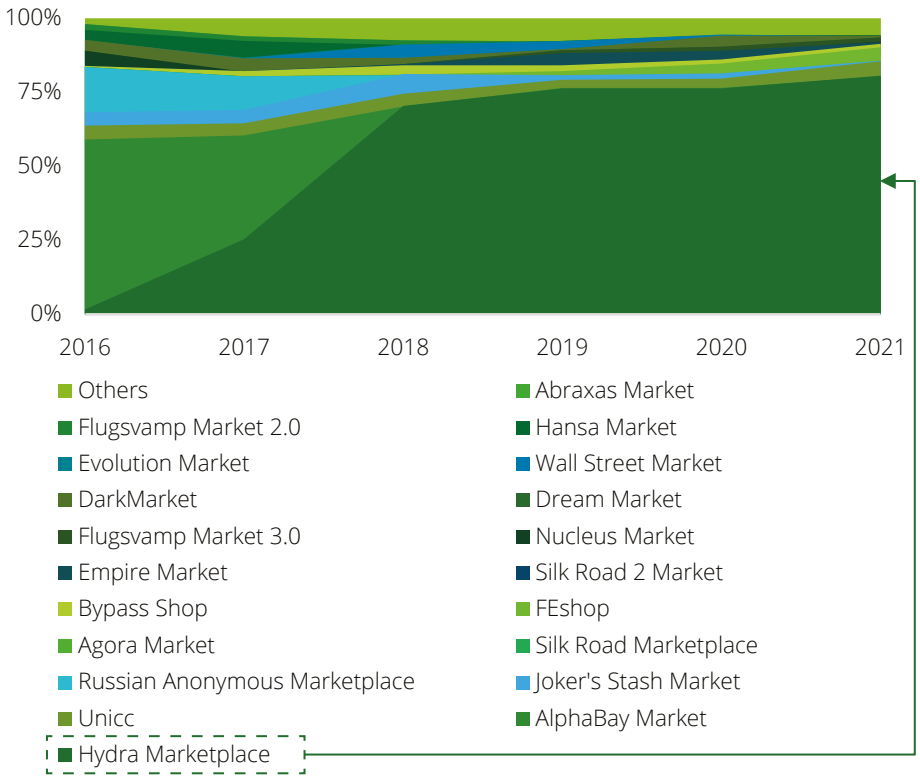
Dark Net

In Dark Net marketplaces, virtual currency is frequently preferred for transactions due to its perceived anonymity and untrace ability. For example, Hydra, launched in 2015, was the largest global dark net market, providing various illicit services. OFAC's investigation uncovered $8 million in ransomware proceeds transiting through Hydra's virtual currency accounts, predominantly from major ransomware variants. Hydra contributed to approximately 86% of illicit Bitcoin received by Russian virtual currency exchanges in 2019. In 2020, Hydra's revenue soared from under $10 million in 2016 to over $1.3 billion, driven by its ties to Russian illicit finance. A joint operation by German and U.S. law enforcement agencies shut down Hydra's Germany-based server in April 2022.[10]

These alternative systems intricately connect to SWIFT systems, posing challenges in tracing funds and enabling their integration into global financial systems.



Procedure: Virtual Currency Use to Bypass SWIFT Bans –
Steps: 1) Register on crypto platforms. 2) Use "P2P-trading" for individual transactions. 3) Select a seller, initiate the transaction. 4) Transfer RUB to the seller's account. 5) Upon money confirmation, the seller releases crypto to the counterparty's account. 6) Withdraw to a third-party wallet or sell for USD/EUR.[11]



The chart from the 2022 Crypto Crime Report by Chainalysis illustrates the significant impact of Hydra in the realm of illicit online transactions. Hydra is distinct for its size, Russian focus, and variety of offerings related to drugs and fraud-related goods and services.[12]

9. https://home.treasury.gov/news/press-releases/jy0701 (as of June 19, 2024).
10. https://home.treasury.gov/news/press-releases/jy0701 (as of June 19, 2024).
11. https://gaodawei.wordpress.com/2023/01/19/2022-how-crypto-gets-russian-dirty-money-abroad/ (as of June 19, 2024).
12. https://www.spiceworks.com/it-security/security-general/news/darknet-marketplace-hydra-dismantled/ (as of June 19, 2024).

02. Trade Activities

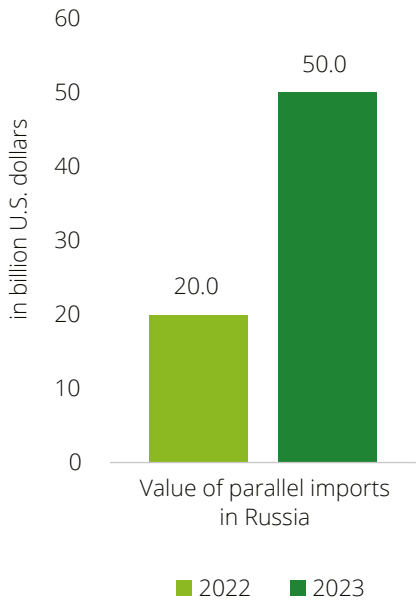
As a result of the impact of sanctions, critical parts of Western technology remain inaccessible to Russian military force, while also impacting its ability to generate export revenue through conventional trade channels. To address these challenges, several strategies have been employed, including the Parallel Import, Dual-Use Goods, Shadow Fleet and Luxury Metals.

Parallel Import

This scheme often involves small-scale foreign firms in some third countries that acquire goods, which are no longer officially available on the sanctioned market and such re-export them to sanctioned countries without the right holders' permission, bypassing trade controls. The Ministry of Industry and Trade of the Russian Federation has published a list of goods allowed for parallel importation, which includes 56 groups of goods, consisting of critical products like warships, spare parts needed for railways and auto components as well as consumer goods like electronics and household appliances, clothing, footwear, and cosmetics.[13] Such routing makes it challenging to identify breaches due to passing through neutral jurisdictions and the exhaustion of intellectual property rights.

The EU introduced measures to address parallel imports in the 12th package. The "No Russia Clause" prohibits EU exporters from re-exporting sensitive goods and technology to Russia, even when sold to third countries. Additionally, the EU has created a list of Common High Priority sanctioned goods, to which businesses should apply due diligence, and which third countries must not re-export to Russia. The list is divided into four tiers containing a total of 50 Harmonized System (HS) codes for dual-use and advanced technology items sanctioned under the Russia Sanctions Regulation. These items are involved in Russian weapons systems used against Ukraine, including the Kalibr cruise missile, the Kh-101 cruise missile, the Orlan-10 UAV, and the Ka-52 "Alligator" helicopter.[15]

The 13th package has introduced further restrictions on parallel imports or enhanced existing measures. For instance, the new listings include a Russian logistics company, LLC Novelco, involved in parallel imports of prohibited goods to Russia.[16] Financial institutions need to stay updated on evolving sanctions regulations and maintain robust screening procedures to identify potential parallel import activities that violate sanctions.[17]



In March 2022, Russia legalized parallel imports due to Western sanctions over the Ukraine invasion. From mid-June 2022 to the end of 2023, the value of these imports was estimated at $70 billion[14]

13. https://www.russia-briefing.com/news/russia-legalizes-parallel-imports.html/ (as of June 22, 2022).
14. https://www.statista.com/statistics/1347702/russia-parallel-imports/#:~:text=The%20value%20of%20parallel%20imports,to%20the%20end%20of%202023. (as of June 19, 2024).
15. https://neighbourhood-enlargement.ec.europa.eu/news/eu-adopts-12th-package-sanctions-against-russia-its-continued-illegal-war-against-ukraine-2023-12-19_en (as of June 19, 2024).
16. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02014R0269-20240223 (as of June 19, 2024).
17. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_963 (as of June 19, 2024).

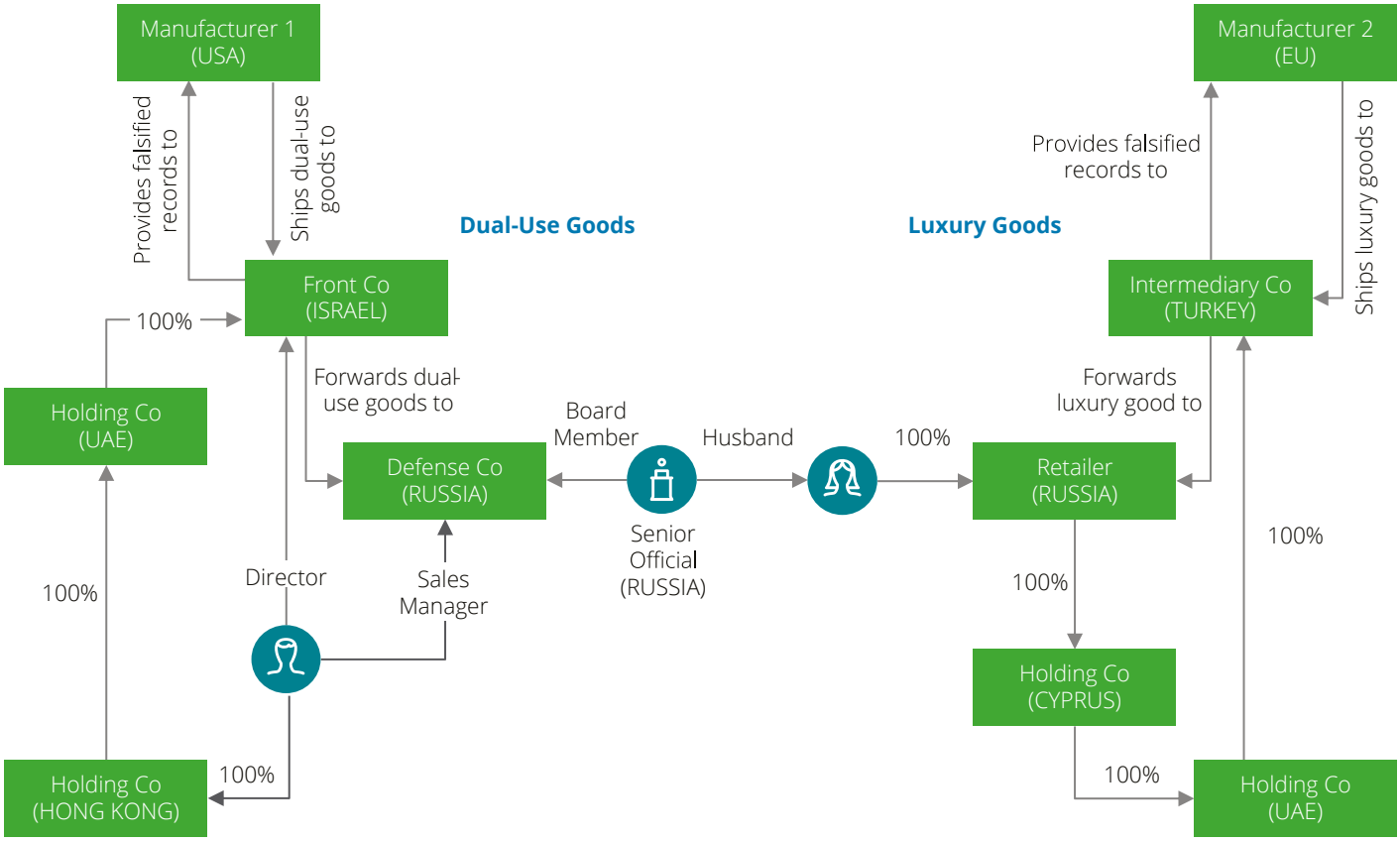
Dual-Use Goods

The 13th package highlights the frequent use of dual-use goods for circumvention. These goods are used by concealing the end-user, final destination, or end use. Common dual-use items in Russian military force include drones, encryption devices, semiconductors, and thermographic cameras. Customs face challenges in determining compliance, requiring knowledge of both the Harmonized System (HS) and the Export Control Classification Number (ECCN), and a robust analytical methodology.

The EU revised Appendix I of Regulation (EU) No. 2021/821 (EU-Dual-Use-VO), governing the export, brokerage, technical support, and transit of dual-use goods. The Conversion Directory (Umschlüsselungsverzeichnis) correlates customs tariff numbers with list item numbers from the EU Dual-Use Regulation, outlining criteria for examined goods. The Federal Office for Economic Affairs and Export Control (BAFA) is responsible for implementing the EU regulations in Germany and handling export license applications. Germany additionally considers the Export Control List to ascertain authorization needs for dual-use goods. The latest version can be found in the Bundesanzeiger.[18]

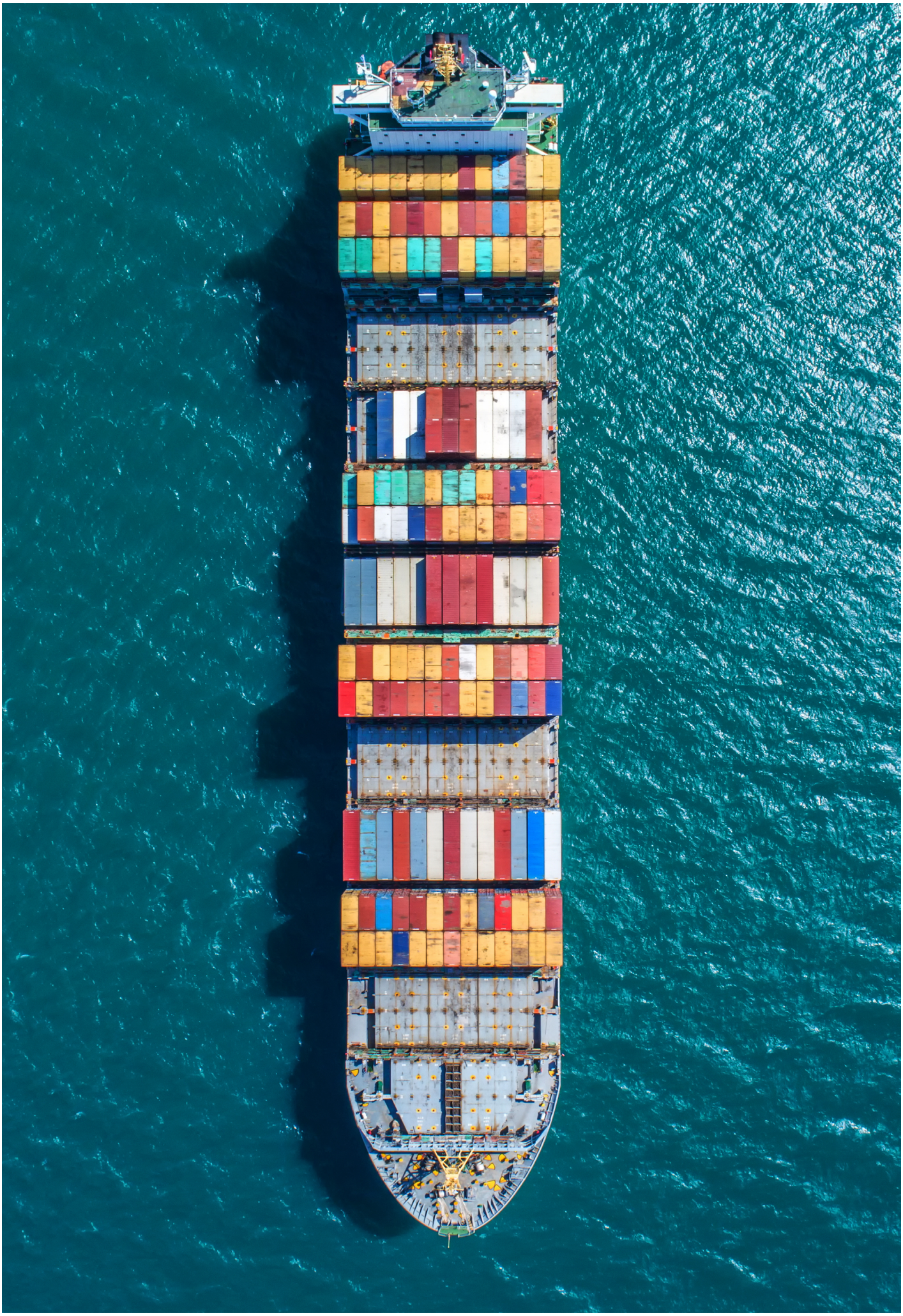
Building on the 12th package, the 13th package tightens controls on dual-use goods critical to Russia's military. It expands the list of advanced technology items, focusing on components for drone production, such as electric transformers, static converters, and inductors. Aluminium capacitors, used in missiles and communication systems, are now also restricted. In addition, the 14th package restricts the export of nine additional dual-use and advanced technology items like aerial amplifiers and microwaves. These measures aim to weaken Russia's military capabilities. Financial institutions should stay informed about these restrictions to identify transactions involving newly controlled items, referencing the updated EU Dual-Use Regulation and relevant press releases.[19, 20]

Procurement of Defense Items, Dual-Use Goods and Sensitive Technologies as well as Embargoed Luxury Goods*



* This is a fictional example. The jurisdictions mentioned in the above graph have been previously identified by western regulatory agencies as possible transshipment hubs.
Source ACAMS, Russia Sanctions Evasion: Key Methods and Techniques-part 1

18. https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Gueterlisten/gueterlisten_node.html (as of December 19, 2023).
19. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_963 (as of June 19, 2024).
20. https://neighbourhood-enlargement.ec.europa.eu/news/eu-adopts-14th-package-sanctions-against-russia-its-continued-illegal-war-against-ukraine-2024-06-24_en (as of June 2024).



Shadow Fleet

Since the 12th package, the EU reinforced the G7+ oil price cap by tightening scrutiny on tanker sales to third countries and introducing detailed attestation requirements to address the Shadow Fleet issue. Vessels altering navigation tracking while transporting Russian oil are also restricted from EU ports.

Public sources indicate Russia's Shadow Fleet includes the Gray Fleet (900 vessels) and Dark Fleet (1,100 vessels).[21] Gray Fleet vessels frequently switch flags, complicating sanctions compliance, while Dark Fleet ships often disable identification systems and use misleading practices. About 31% of the Gray Fleet and 20% of the Dark Fleet are registered in European countries, mainly Greece and Malta, with over 40% of the Dark Fleet registered in Hong Kong and UAE. China and India are top destinations, with most departure ports in Russia.[22]

It is crucial to screen International Maritime Organization (IMO) numbers for trade diligence and regularly update lists of sanctions, politically exposed persons (PEPs), government watchlists, and negative media coverage. In addition, the 14th sanctions package against Russia included a ban on re-exports of Russian liquefied natural gas (LNG) within the EU, blocking financing for Russia's Arctic and Baltic LNG terminals to combat Russia's shadow fleet and limit its energy revenues.

Luxury Metals

Russia is actively boosting its gold reserves to diversify away from the USD, reaching $151.9 billion in November 2023.[23] As a major global supplier, Russia leads in both rough and cut diamonds markets. There are concerns that Russia might use gold and diamonds to bypass sanctions through laundering. In response, the EU has imposed sanctions on gold, diamonds, and jewelry from Russia.

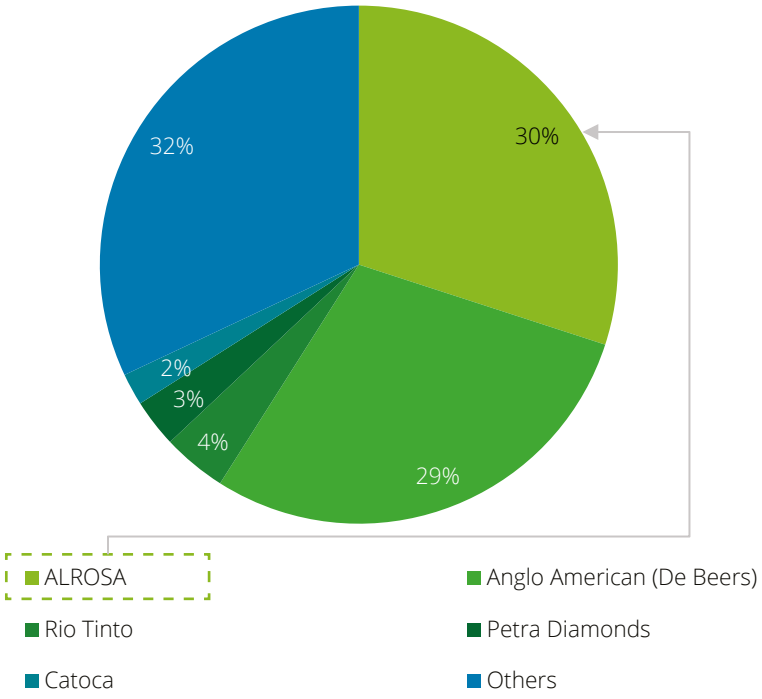
Diamond export statistics from Russia show a value of approximately $431 million in November 2023.[24] Research indicates that rough diamonds from Alrosa Group, a Russian government-owned entity, were imported into the US through third-country dealers by mid-March 2022. Alrosa, part of the 12th sanctions package, dominates Russian diamond exports, holding a global monopoly with about 90% market share.[25]

To address this through global collaboration, an internationally coordinated diamond ban among G7 members is proposed, emphasizing the tracing of diamonds from the mine to the final product. The system includes mandatory registration, "digital twins" of rough diamonds, and the issuance of certificates of origin, all recorded in a blockchain-based ledger for transparency.[26]

The system is operational as of March 1, 2024, in a pilot phase in Belgium, with around 20 economic operators participating, including LVMH, Kering, and Richemont. During this period, participants can choose to use either the traceability-based certification mechanism or other evidence proving the non-Russian origin. As of September 1, 2024, the use of the traceability-based certification mechanism will be mandatory.[27]

Key Vendors Market Share of Global Diamond Market by 2022

As of 2022, the Russian diamond mining conglomerate ALROSA had the largest market share of any diamond mining company in the world, 30%. In a close second, De Beers (owned by Anglo American) accounted for 29% of the global diamond production market share.[28]



21. https://windward.ai/knowledge-base/illu minating-russias-shadow-fleet (as of July 2023).
22. https://windward.ai/knowledge-base/illuminating-russias-shadow-fleet/ (as of July 2023).
23. https://english.news.cn/20231215/cd8b7a903a1e452ea3c92090c1a6d911/c.html (as of December 15, 2023).
24. https://www.statista.com/statistics/983857/monthly-value-of-diamond-exports-from-russia/ (as of November 2023).
25. https://www.haaretz.com/israel-news/2022-04-13/ty-article-magazine/.premium/the-israeli-diamond-traders-funding-putins-war-machine/00000180-5b9d-dc66-a392-7fdfe98b0000?v=1705076327922 (as of November 2023).
26. https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_6642 (s of December 18, 2023).
27. https://www.reuters.com/markets/commodities/us-lukewarm-g7-russian-diamond-ban-after-industry-backlash-2024-05-17/ (as of June 19, 2024).
28. https://www.statista.com/statistics/585450/market-share-of-diamond-supply-worldwide-by-producer/ (as of December 19, 2023).

03. Ownership Structures

It is not uncommon for sanctioned countries to adopt complex ownership structures, such as front companies, shell and shelf companies, trusts, and foundations in high-risk jurisdictions. They often leverage expertise from lawyers and accountants to consolidate investments in offshore financial centers, aiming to circumvent sanctions.

Wagner Group

Focusing on typical schemes for the restrictive measures against Russia, the involvement of the Wagner Group should be highlighted. The Wagner Group, a Russia-based private military entity led by Dimitriy Utkin and formerly financed by the passed-away Yevgeniy Prigozhin, operates in Ukraine, Libya, the Central African Republic (CAR), Mali, and Sudan. The group actively engages in the Russian war against Ukraine, leading attacks on Soledar and Bakhmut.[29] The US State Department has stated in June 2023 that the Wagner Group is involved in weapon smuggling by using its operations in Mali, to bolster Russian forces in Ukraine.[30]

Recognizing the complexity of evasion tactics, the EU Council has expanded its restrictive measures by adding individuals and entities linked to the Wagner Group to the EU sanctions list. This decision, finalized on April 19, 2023, concludes the "Wagner Package" initiated on February 25, 2023.[31] Those listed, including Wagner Group commanders involved in the capture of Soledar and leaders in Mali and CAR, face asset freezes and travel bans. Additionally, EU citizens and companies are prohibited from providing funds to these sanctioned individuals and entities, with the relevant legal acts published in the Official Journal of the EU.[32]

Impact of sanctions

The EU can target individuals and entities for individual financial measures (asset freeze and prohibition to make funds or economic resources available) or for specific restrictions such as ban on all transactions (for example Article 5aa [sic] of Regulation (EU) No 833/2014). These measures can impact non-targeted entities as follows: (i) for the asset freeze measures, the assets of entities owned for more than 50% by the designated person/entity or controlled by them must be frozen; (ii) specific restrictions applied to targeted entities can impact entities whose proprietary rights are directly or indirectly owned for more than 50% by the targeted entities.[33]

Identified red flags

The EU Commission identifies red flags related to ownership structures, including:

- Complex offshore corporate arrangements in Russia-friendly jurisdictions lacking business justification
- Recent mergers with sanctioned entities
- Shared addresses suggesting shelf company use
- Corporate ownership reductions below 50%
- Changes in beneficial ownership during sanctions periods
- Frequent sanctioned-to-non-sanctioned share transfers with shared addresses
- Potential control by designated persons despite ownership thresholds; and CEOs or managers inaccessible directly, with communications handled by Power of Attorney-(PoA-)holding representatives[34]

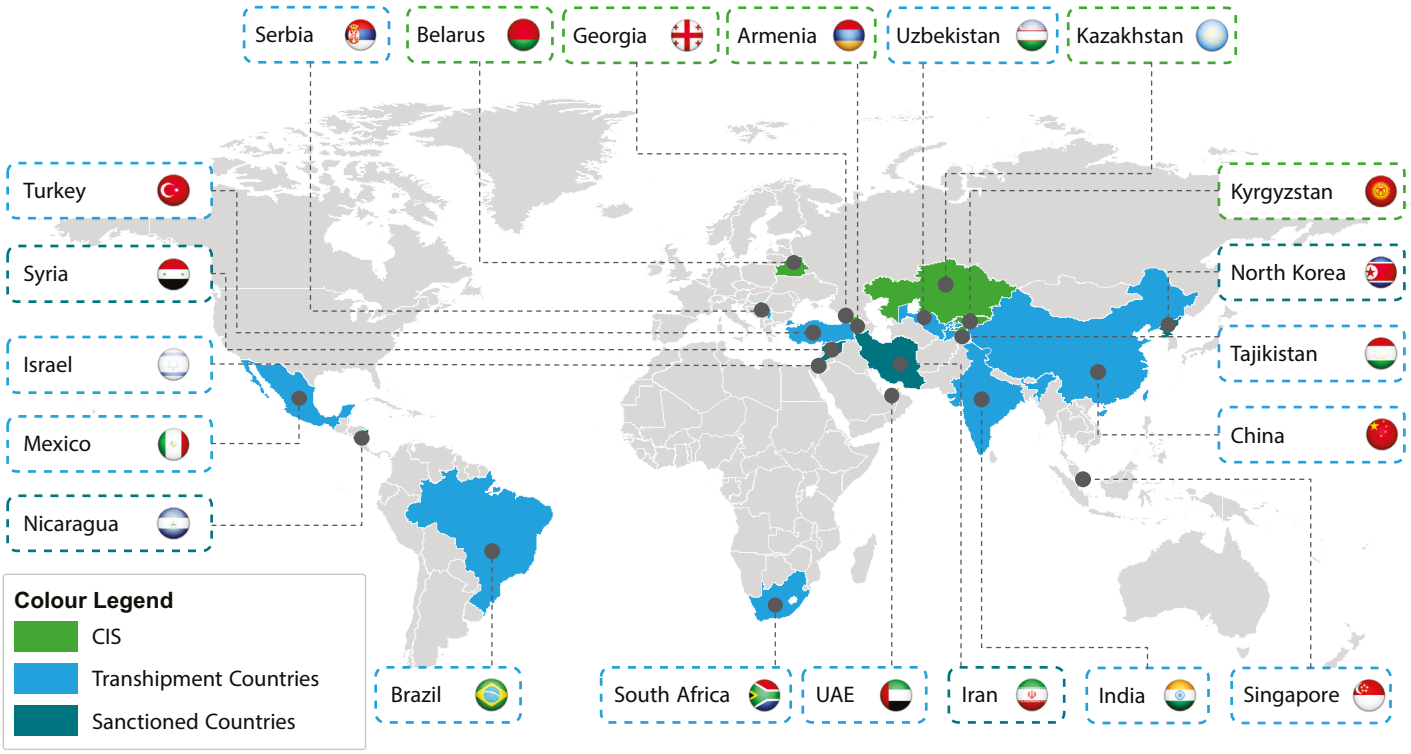
These flags signal heightened risks demanding increased scrutiny and diligence from financial institutions.

29. https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Gueterlisten/gueterlisten_node.html (as of December 19, 2023).
30. https://www.state.gov/sanctioning-entities-and-individual-connected-to-wagner-group-in-africa/ (as of June 19, 2024).
31. https://www.consilium.europa.eu/en/press/press-releases/2023/04/13/russia-s-war-of-aggression-against-ukraine-wagner-group-and-ria-fan-added-to-the-eu-s-sanctions-list/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Russia%27s%20war%20of%20aggression%20against%20Ukraine%3A%20Wagner%20Group%20and%20RIA%20FAN%20added%20to%20the%20EU%27s%20sanctions%20list (as of June 19, 2024).
32. https://www.consilium.europa.eu/en/press/press-releases/2023/04/13/russia-s-war-of-aggression-against-ukraine-wagner-group-and-ria-fan-added-to-the-eu-s-sanctions-list/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Russia%27s%20war%20of%20aggression%20against%20Ukraine%3A%20Wagner%20Group%20and%20RIA%20FAN%20added%20to%20the%20EU%27s%20sanctions%20list (as of June 19, 2024).
33. https://finance.ec.europa.eu/system/files/2023-12/guidance-eu-operators-russia-sanctions-circumvention_en.pdf (as of June 19, 2024).
34. https://finance.ec.europa.eu/system/files/2023-12/guidance-eu-operators-russia-sanctions-circumvention_en.pdf (as of June 19, 2024).

Snapshot of Currently Involved Circumvention Countries

The circumvention of sanctions has always been an issue but has reached greater dimensions since the Russia/Ukraine sanctions came into force with certain countries being more in the focus of investigators. According to a publication of the US Bureau of Industry and Security countries currently involved in the circumvention of Russia/Ukraine sanctions can be divided into different types. This section below highlights three of them: Transhipment Countries[35], the Commonwealth of Independent States (CIS)[36], and Sanctioned Countries[37]. The transhipment countries have been identified by the Bank of International Settlement through analysis of historical and current trends, export and re-export data, as well as changes identified through compliance efforts in the field. The involvement of these countries in international trade transactions complicates the enforcement of international sanctions, necessitating coordinated efforts to prevent violations.

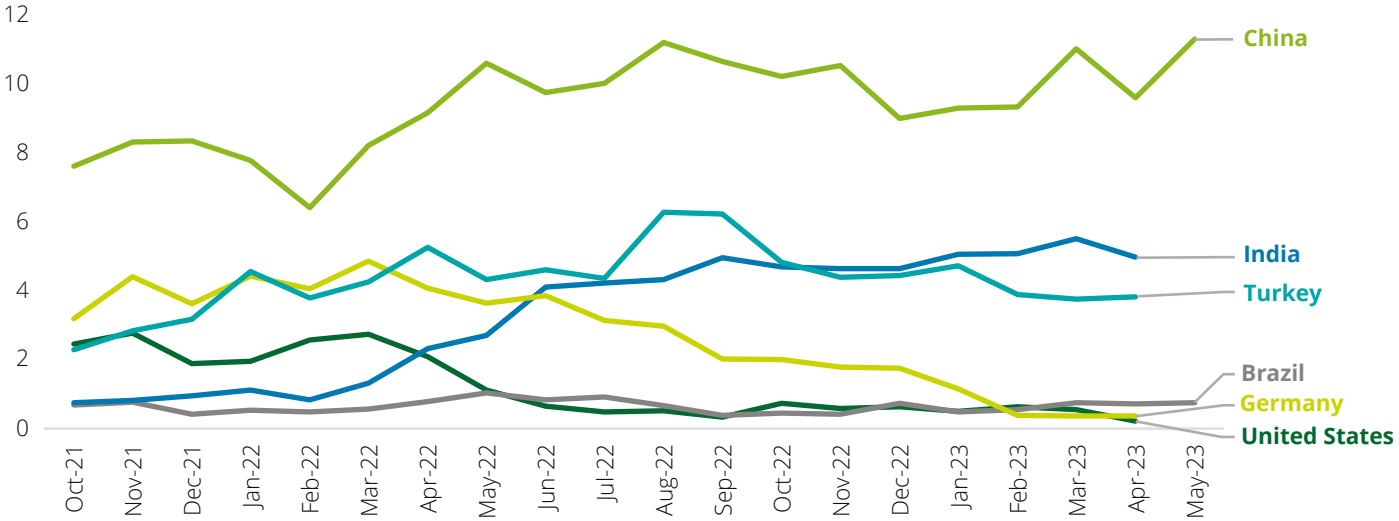
World Map: Detected Circumvention Involved Countries



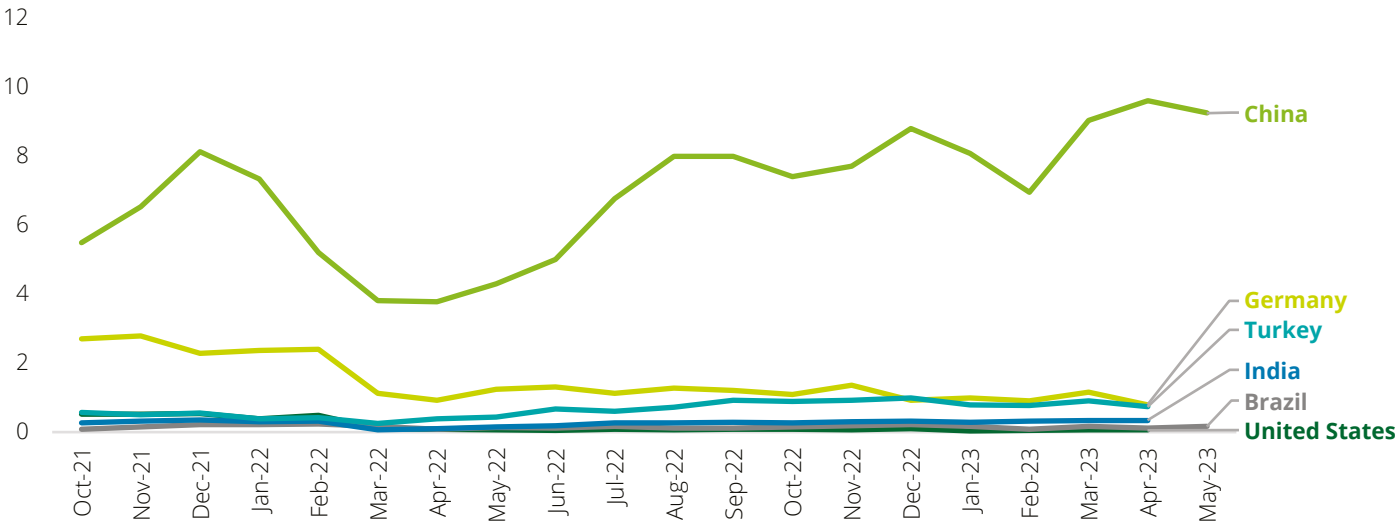
The EU's sanctions have significantly impacted Russia's exports to other countries. Russia's exports to China, India and Turkey have seen significant growth since 2022, as indicated by charts published by The Observatory of Economic Complexity (OEC). The sanctions imposed by the EU and US have a clear impact on Russia's trade pattern, leading to a significant decrease in shipments compared to pre-conflict levels. This change has motivated Russia to redirect its exports towards other major trading partners. Notably, since 2022, countries like China, India, and Turkey have become the top destinations for Russian exports, while Western nations such as the US and Germany have seen a notable decrease in their trade with Russia. This signifies a major shift in Russia's trade patterns.

35. https://www.bis.doc.gov/index.php/documents/policy-guidance/3120-best-practices-faq-draft-8-15-22-final/file (as of June 19, 2024).
36. https://www.linkedin.com/pulse/russia-sanctions-evasion-role-cis-sanctions-sos-74sge?trk=public_post_main-feed-card_feed-article-content (as of January 3, 2024)
37. https://www.iiss.org/publications/strategic-comments/2022/russia-and-sanctions-evasion/ (as of June 19, 2024).

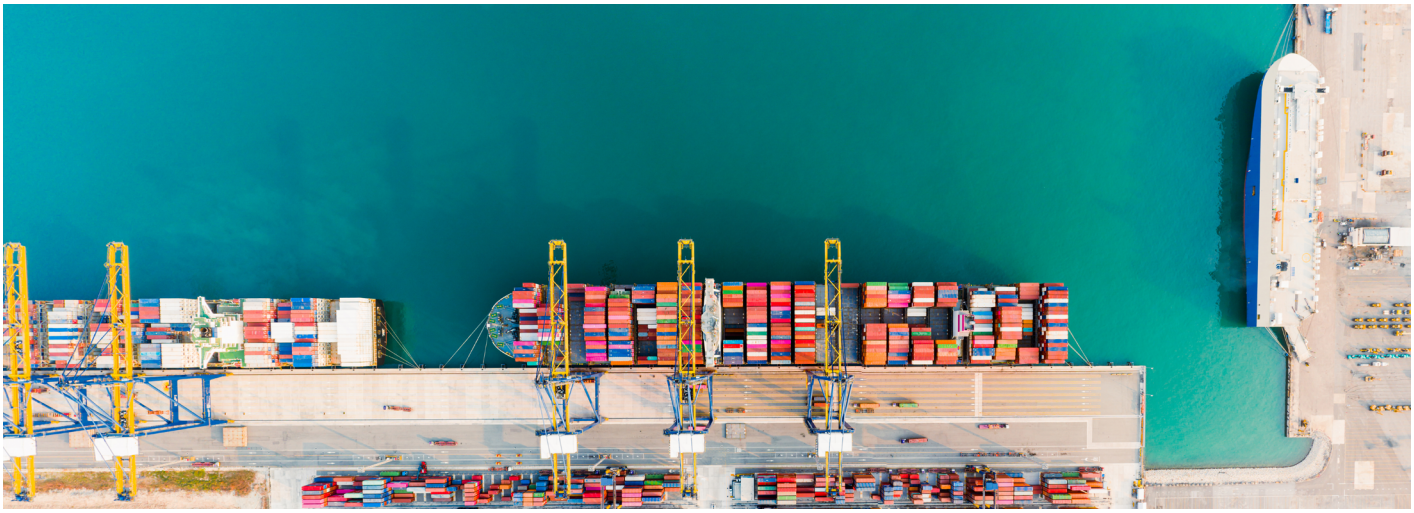
Russia's Exports since Oct 2021 to May 2023 (in $B)



Russia's Imports since Oct 2021 to May 2023 (in $B)



Source: https://oec.world/en/profile/country/rus?latestDataNonSubnationalMonthSelector=201901 (as of July 2023).



Conclusion

Sanctions are targeted measures imposed by governments to deter or punish undesirable behavior by a state or another actor. Enforcing sanctions effectively is crucial for their success. In the context of the international sanctions against Russia, the developments over more than two years highlight again the importance of international commitment and cooperation for a successful and efficient implementation of restrictive measures, including the ongoing monitoring of circumvention attempts and continuous adjustment of countermeasures. With view on the German market, the Sanctions Enforcement Act 2 (Sanktionsdurchsetzungsgesetz II) serves as a crucial guiding framework for financial institutions. It transfers asset investigation and freezing powers to the federal government, streamlining enforcement and establishing a register for sanctioned persons and assets. Automatic application of UN sanctions lists further enhances compliance and curbs sanction breach risks.

The dynamic nature of sanctions enforcement poses unprecedented challenges for European financial institutions. These challenges include embedded money laundering, fraud, and tax evasion, along with reputation laundering risks and asset flight complications.

Contacts

Dr. Andreas Burger
Partner

Financial Advisory | Financial Services
Anti-Financial Crime Advisory
Mobile: +49 151 5807 6486
anburger@deloitte.de

Agnes Checinski
Director

Financial Advisory | Financial Services
Anti-Financial Crime Advisory
Mobile: +49 151 5807 1085
achecinski@deloitte.de

Youxuan Gao
Senior Consultant

Financial Advisory | Financial Services
Anti-Financial Crime Advisory
Mobile: +49 151 1829 5902
yogao@deloitte.de

Deloitte.