Institute for
Financial Integrity

EXPERT INSIGHT

Russia 2024: The Two-Year Anniversary of the Invasion

Table of Contents

Russia 2024: The Two-Year Anniversary of the Invasion

Two years after Russia's invasion of Ukraine, Russia is the world's most sanctioned nation, with more than 17,000 designations imposed against it by world powers since Moscow began its invasion on February 24, 2022, according to data firm Castellum.AI. The United States, Australia, Canada, the EU, France, Switzerland, and the UK together imposed nearly 5,000 designations against Russian individuals and entities during the 2023 calendar year.

However, Russia, despite a marked decrease in its ability to access necessary military materiel, microchips, automobiles, aircraft, and other equipment during the past two years, remains defiant, with Russian president Vladimir Putin proclaiming that Moscow "would not give up what is ours" during his late-December end-of-year meeting with Russia's military leaders. Media reports indicate that Russia will not only procure ballistic missiles from North Korea and Iran to help rebuild its military arsenal, but significantly increase its military spending, suggesting that the Kremlin plans to continue its attacks on Ukraine despite an increase in sanctions pressure and a decrease in its ability to wage war.

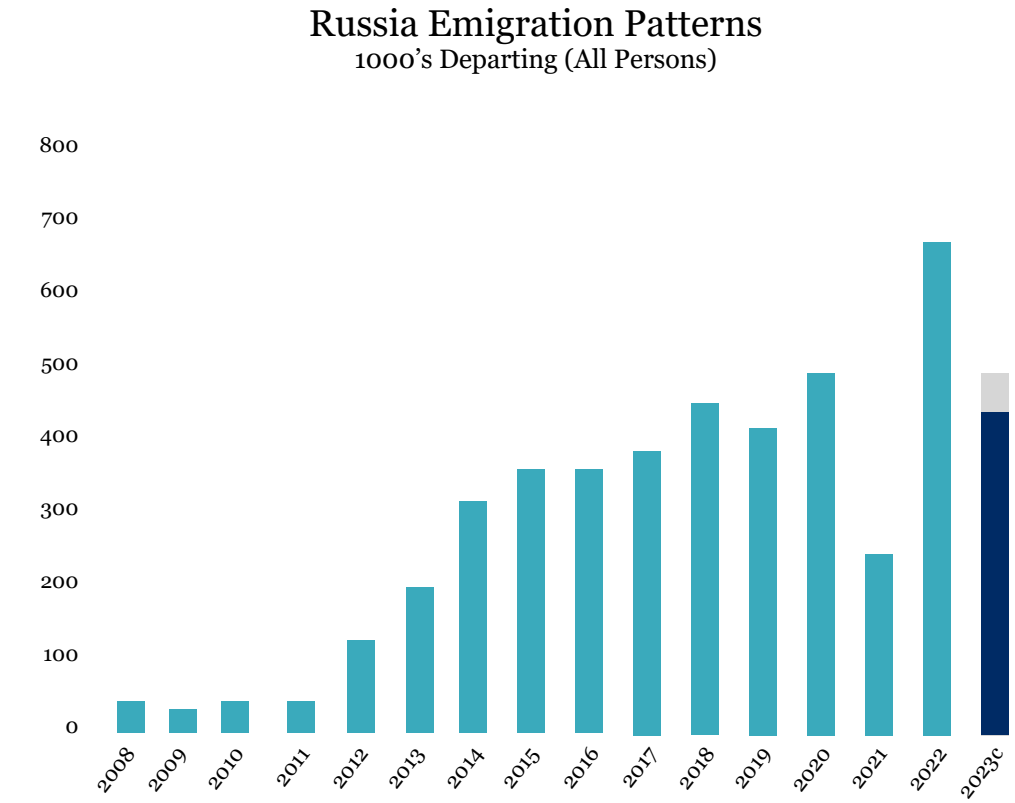
- US Treasury Chief Sanctions Economist Rachel Lyngaas in mid-December wrote in a blog that sanctions and export controls are damaging Russia's economy and limiting its access to the financing and material goods it needs to wage its war against Ukraine. In addition, Lyngaas writes, the war has exacerbated an increase in emigration from Russia that predated the Ukraine invasion, as hundreds of thousands of young and educated people left the country to avoid being forced to fight in the Kremlin's war and for opportunities abroad.

- Russia's proposed 2024 military budget is equivalent to 6 percent of the country's gross domestic product, according to the Carnegie Endowment for International Peace, and military spending this year will exceed social spending. Production of military equipment will consume most of Russia's defense spending.

    - Much like in previous years, Russia's 2024 defense spending will be hindered by the military-industrial sector's longstanding inefficiency, corruption, and unprofitability. For example, despite rising defense spending, Russia's state-owned military conglomerate Rostec made less income from the sale of weapons and military equipment in 2022 than it did in 2020. Roscosmos, the Russian space agency, ended 2022 with losses of 50 billion rubles (more than $550 million in current dollars), compared with losses of 31 billion rubles ($342 million) the year before. And the state-owned United Shipbuilding Corporation saw a loss of 20 billion rubles ($220 million) in 2022, compared with a loss of several billion rubles in 2021 and a net profit in 2019.

    - Russia in 2023 doubled its defense spending target to more than $100 billion (a third of all public expenditures) while canceling public salary increases scheduled for this year, according to Carnegie. As spending has grown, energy revenues have declined by almost 40 percent from January through October 2023.

Russia's significant defense spending increases, and the increased military cooperation with North Korea and Iran during the past year suggest that Moscow is committed to a long war in Ukraine. NATO Secretary General Jens Stoltenberg in November said that Russia is in Ukraine for the long haul, and that NATO allies must be prepared for continued fighting.



Sources: Russia Federal State Statistics Service, Treasury Staff Estimates, Courtesy of the U.S. Treasury Department

Russia's strategy: Disinformation Results In Attrition

The New York Times reported in October that Russia's strategy in Ukraine was to outlast the West's willingness to support Kyiv. US officials are convinced that Putin will work to undermine US and European support for Ukraine by using advanced technologies to further Russian narratives and stoke conspiracy theories in an effort to increase support for political candidates who oppose assistance to Ukraine. For example, Russia last year used newly created, verified accounts on X (formerly Twitter) to spread propaganda and disinformation about how much money the United States was spending on the war in Ukraine, suggesting that the funds should be spent on disaster relief in Maui after last summer's wildfires.

Russia will almost certainly increase its efforts to meddle in the 2024 US presidential elections. The Kremlin will likely support former President Trump's election bid this year, given Trump's stated desire to withdraw the United States from the NATO alliance.

- National Security Agency Director Gen. Paul Nakasone and FBI Director Chris Wray in January told an audience at a New York conference that Russian intelligence continues to look for ways to impact the US government's support for Kyiv by influencing US elections in Russia's favor.

- The former director of the US Cybersecurity and Infrastructure Security Agency (CISA), Chris Krebs, said last year that he expects both Russia and China to interfere in this year's presidential elections, with threat actors using similar playbooks to influence the elections as they did in 2020.

- Research organization Insikt Group in December examined an ongoing operation by the Russia-linked influence network called Doppelgänger that targets audiences in the United States, Germany, and Ukraine through Coordinated Inauthentic Behavior (CIB), including fraudulent "news" sites and social media accounts. In the United States, the campaign works to foment anti-LGBTQ+ sentiment, criticize the US military, and amplify political divisions around US support for Ukraine. The EU's DisinfoLab in 2022 exposed Doppelgänger as a Russia-based influence operation network.

    - Meta in 2022 attributed Doppelgänger to 2 Russian companies: Structura National Technologies and Social Design Agency. The latter's client list includes several Russian government agencies, local government entities, state-owned enterprises, and private companies. Neither entity is sanctioned by OFAC, but the EU in July 2023 designated both for engaging in disinformation efforts.


SANCTIONS
SANCTIONS
SANCTIONS
SANCTIONS
SANCTIONS
SANCTIONS

Focus on Enforcement

Global powers have continued to ratchet up sanctions pressure on Russia, imposing unprecedented restrictions to limit Moscow's access to needed resources, materiel, and technologies, hindering Russia's ability to conduct the war in Ukraine. Billions of dollars in Russian assets have been frozen, additional restrictions have been imposed, targeting economic sectors that supports Russian aggression, and US secondary sanctions on foreign financial institutions have been authorized.

- President Biden in late December 2023 signed Executive Order (EO) 14114 authorizing OFAC to impose secondary sanctions on foreign financial institutions that help Russia's military sector and facilitate transactions that support Russia's war in Ukraine.

- In its 2022-2023 annual review, the UK's Office of Financial Sanctions Implementation (OFSI) declared that as of October 2023, £22.7 billion of Russian assets were reported frozen since Russia's invasion of Ukraine began. OFSI director Giles Thomson noted in the foreword to the report that OFSI is increasing its focus on enforcement of sanctions, and the review states that "OFSI is undertaking a large number of complex investigations into Russia related breaches, which it anticipates will lead to public enforcement action."

    - The agency issued seven warning letters, two financial penalties, and closed 51 cases with no further action out of a recorded 473 suspected sanctions violations during the course of the UK fiscal year, which runs from 01 April to 31 March.

- The EU in 2023 implemented its 11th and 12th sanctions packages against Russia, that included a ban on direct or indirect import, purchase, or transfer of diamonds from Russia and implemented an anti-circumvention tool in the 11th package allowing the EU to restrict the sale, supply, transfer or export of specified sanctioned goods and technologies. The bloc noted that the ban on Russian diamonds in the 12th package of sanctions was part of a coordinated G7 effort to deprive Russia of revenues from its diamond sector.

On the second anniversary of Russia's invasion, the United States and its allies released hundreds of new designations targeting Russia's ability to continue to wage war and the facilitators that help Russia access the resources it needs to enhance its military capabilities and engage in aggression against its neighbors.

- OFAC and the US State Department together designated 553 individuals, vessels, and entities to mark the second anniversary of Russia's invasion of Ukraine and the death of Russian opposition leader Alexey Navalny last week in an Arctic prison colony. With the latest tranche of designation, OFAC has targeted Russia's financial infrastructure, including the Mir National Payment System and Russian banks, investment firms, and financial technology (fintech) companies. OFAC also designated 26 third-country entities and individuals in 11 countries, including China, Serbia, the UAE, and Liechtenstein. OFAC is also targeting Russia's access to unmanned aerial systems (UAS). The Commerce Department's Bureau of Industry and Security also added more than 90 companies to the Entity List.

- The UK on February 22 released a list of more than 50 new designations to mark the second anniversary of Russia's invasion of Ukraine. The new sanctions target munitions suppliers as well as key sources of Russian revenue, including in the metals, diamonds, and energy sectors. Entities from Türkiye, three companies based in China, and two in Belarus were included in this package of sanctions.

- The EU's new sanctions package against Russia will add nearly 200 entities to mark the second anniversary of Russia's invasion. The entities sanctioned by the bloc include companies that make dual-use electronic components, banks, government agencies, and other organizations that support Russia's war. The bloc is also targeting Russia's access to unmanned aerial vehicles (UAV).

Additional designations and restrictions are part of the bigger enforcement picture, as countries work together to hinder sanctions evasion. Allies are increasingly providing guidance to firms and financial institutions about how to best detect Russia's efforts to access restricted financial resources, goods, and technologies, and pressure countries to stop acting as transshipment points and facilitators for Russia's illicit activities.

- The UK's National Crime Agency (NCA) in November issued a Red Alert to financial institutions and other stakeholders warning that Russia is using gold to undermine the UK sanctions regime. The agency stressed that Russia since July 2022 has been increasingly shipping its gold to countries that have not imposed sanctions against the precious metal originating from Russia, where it is melted and refined, masking its origin, so it can be sold in other countries. The NCA in January also issued an Amber Alert, warning that sanctioned Russian actors are using specialized storage facilities to store artwork as investments to evade sanctions.

- The EU in September published a guidance note to help export companies and others conduct due diligence to detect increasingly elaborate Russian schemes to evade EU sanctions. The guidance includes a list of red flags that may indicate that trading partners are inclined to circumvent EU sanctions.

Enforcement of international sanctions also involves prosecution and designation of individuals and entities that violate sanctions or facilitate sanctions evasion. OFAC, in coordination with the UK, in April 2023 sanctioned a facilitation network that was helping designated Russian oligarch Alisher Usmanov gain access to the global financial system. The US Treasury throughout the year continued targeting sanctions evasion facilitators and disrupting Russia's international supply chains that helped it gain access to high-priority items

- The US Justice Department started 2024 with the arrest of Ilya Kahn, a citizen of the United States, Israel, and Russia, who is accused of involvement in a years-long scheme to secure and unlawfully export sensitive technology from the United States for the benefit of a US-designated Russian business. Joint Stock Company Research and Development Center Elvees was sanctioned by OFAC following Russia's invasion of Ukraine in February 2022. Elvees' clients include elements of the Russian military and the Federal Security Service (FSB).

- The Justice Department in December charged Belgian national Hans De Geetere with unlawfully exporting sensitive military-grade technology from the United States to Russia and China. De Geetere allegedly acquired and illicitly diverted US-origin electronic components to the two countries that can be used in missiles, drones, and military radar. Belgian authorities that month arrested and questioned De Geetere and five alleged co-conspirators. OFAC sanctioned De Geetere and his companies, and BIS included them on the Entity List.

- The Justice Department in October unsealed a criminal complaint, charging and arresting a New York resident and two Canadian nationals in connection with a global procurement scheme that used two entities registered in Brooklyn to purchase millions of dollars' worth of dual-use electronics on behalf of Russian end-users, including those connected with Russia's military. One of the defendants this month pleaded guilty to money laundering conspiracy for her role in a scheme to send UAS components and guided missile systems, as well as other weapons to Russia.

- A multinational investigation in Europe into an international smuggling network that helped Russia evade EU sanctions resulted in the arrest of three individuals in January. Two of the suspects administered a trading company registered in the Netherlands that exported "technological and laboratory equipment" with potential military uses to Russia, according to Eurojust. The third suspect is an employee of an external contractor, allegedly knew about the violations. The trading company is now run by an administrator in Russia, who is also the sole shareholder of the entity.

In addition to raids and prosecutions, G7 allies are exploring ways to force Russia to pay for the damages it has caused in Ukraine. The United States in December proposed that working groups from G7 countries explore ways to seize $300 billion in frozen Russian Central Bank assets. Backed by the UK, Japan, and Canada, the proposal suggests preparing options for G7 leaders to consider at a potential meeting around February 24th—the second anniversary of Russia's invasion. G7 leaders assert that Russia is obligated under international law to end its war and pay for the damage it has caused, which exceeds $400 billion dollars, according to the World Bank.

Strategic Trade Controls

As K2 Integrity's Chip Poncy and Amir Fadavi wrote on the first anniversary of Russia's invasion, *"it has become increasingly clear that strategic trade controls are playing a substantial role in degrading Russia's military capabilities and weakening Russia's economy."*

Two years after Russia's invasion, the Commerce Department's Bureau of Industry and Security (BIS) has strengthened its enforcement policies, increased its cooperation with the interagency, academia, industry, and foreign governments, and included more than 465 individuals and entities from Russia, China, Iran, and elsewhere on the Entity List.

However, the work is far from done, according to the Yermak-McFaul International Working Group on Russian Sanctions, which is led by the Head of the Office of the President of Ukraine Andrii Yermak and former US Ambassador to Russia Michael McFaul, and which publishes recommendations for sanctions and other policy actions against Russia and Belarus and evaluates their effectiveness. In a recent Working Group Paper "Challenges of Export Controls Enforcement," the group highlighted that despite increased sanctions and export control pressure, Russia continues to access goods it needs for military production. The report makes several recommendations to tighten enforcement:

- Bolstering corporate responsibility by creating incentives for firms to create compliance procedures;
- Closing policy gaps and ensuring that export controls in all jurisdictions apply extraterritorially;
- Targeting third-party circumvention by imposing sanctions on entities that have been found to facilitate transactions that violate export controls; and
- Strengthening institutions and cooperation to empower enforcement agencies to better implement comprehensive trade controls against Russia.

Although sanctions implemented at the end of 2023 will limit the ability of Russian subsidiaries of western companies to access business software and other technologies, the Yermak-McFaul Working Group in mid-January also assessed that despite the Kremlin's efforts to reduce Russia's reliance on western software for critical systems, software developers and related parties still maintain connections with companies in countries that have imposed sanctions against Russia—mainly through licensing or business ties.

- The group's assessment recommends practical steps to mitigate the risk of Russia continuing to access software that helps its war in Ukraine and highlights Russia's main areas of dependence on software capabilities, specifically focusing on the military-industrial complex, the energy and extractive sectors, and other critical sectors of the Russian economy that could be vulnerable to disruption by software restrictions.

The Working Group's recommendations are critical because Russia continues to use western software to manufacture the munitions and key military systems necessary to conduct its continued aggression in Ukraine. Russia also uses western software to extract oil and gas more efficiently to increase the revenues it can use to enhance its military capabilities. Moscow also uses western databases, analytics, and financial software to run its wartime economy and suppress the free flow of information, run information operations, and interfere in the governance of other countries around the world. The Working Group recommends imposing sanctions on Russian software developers, ensuring western companies stop providing updates and support for existing users, holding IT companies and intermediaries accountable if they continue providing licenses, technical support, or updates to Russia, monitoring compliance, and other policy actions to limit Russia's access to critical software.

Russia is heavily dependent on countries such as China and former Soviet republics for access to needed machinery and technologies. Deceptive tactics, such as the use of third-party intermediaries or transshipment points, help Russia disguise the involvement of parties on the Entity List or SDN List and obscure the true identities of Russian end users. Complicit European companies also help Moscow gain access to needed weapons and technologies, and China has emerged as a major lifeline, helping Russia purchase machine tools and other equipment for the country's military sector.

- Ukraine's National Resistance Center highlighted that on 26 December 2023, during a meeting of CIS leaders, Russian President Vladimir Putin claimed that Russia reached preliminary agreements with Uzbekistan on the creation of shell companies, which will be funded by the Russian government. These companies will export products and components to several Russian defense enterprises, such as Elektropribor plant in Kazan city, Elekon plant, Stella-K, and others. Touted as "Cooperation in the transport industry," the strategy is intended to help Russia evade western sanctions and export controls.

- Several Finland-based logistics companies are managed or owned by Russians and have supplied Russia with technologies and other products needed by Moscow in its war with Ukraine. The clients of these companies are linked to the Russian military sector or intelligence agencies, according to Finnish media. Media outlet Yle has found that more than 20 Finnish companies have exported vital military products to Russia. Ukraine says that between January and October of last year, western companies supplied Russia with $2.9 billion worth of components that can be used for military production despite sanctions and strategic trade controls.

- OFAC in November sanctioned 130 individuals and entities facilitating Russia's access to much-needed technology and equipment from third countries, designating producers, exporters, and importers of nearly all of the high-priority items identified by the international coalition imposing sanctions and export controls on Russia. Entities based in China, Türkiye, and the UAE were sanctioned for sending high-priority dual-use goods to Russia.

- China is now Russia's main source of CNC machine tools. Russian customs data show that Chinese producers shipped $68 million worth of CNC tools to Russia in July 2023, according to the Financial Times, which also examined export records that showed numerous companies that help Russia gain access to critical machinery have strong links with China's People's Liberation Army.

Guidance Helps Recognize Evasion

US regulators and partners have published various guidance during the past year to help firms and financial institutions recognize signs of Russian sanctions and trade controls evasion.

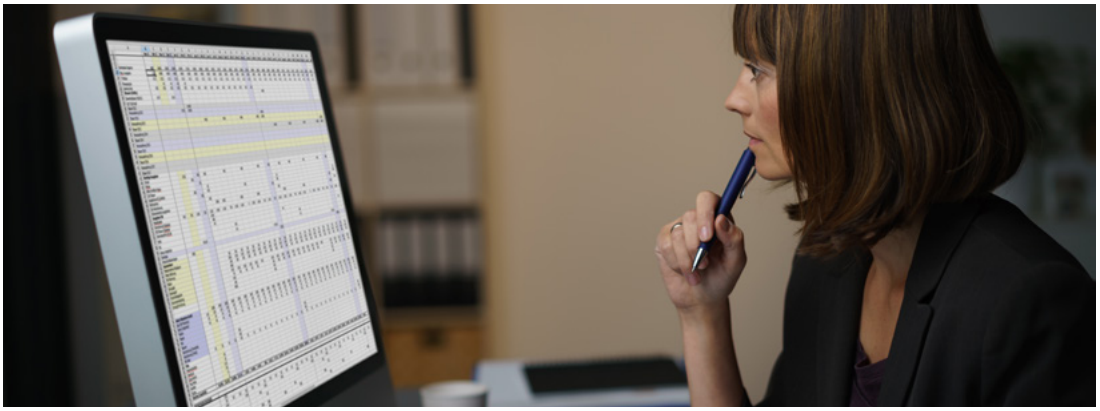
- On May 19, 2023, the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the US Department of Commerce's Bureau of Industry and Security (BIS)1 issued a new joint alert providing additional information regarding new BIS export control restrictions related to Russia, as well as reinforcing ongoing U.S. Government engagements and initiatives designed to further constrain and prevent Russia from accessing needed technology and goods to supply and replenish its military and defense industrial base. As a supplement to this alert, BIS is issuing this guidance for exporters and reexporters that provides further details on evasion typologies, highlights nine high priority Harmonized System (HS) codes to inform their customer due diligence, and identifies additional transactional and behavioral red flags to help identify suspicious transactions relating to possible export control evasion.

- Departments of Justice, Commerce, Homeland Security, State and Treasury in December jointly advised maritime and transportation industry on know-your-cargo policy.

- The UK's NCA in early December issued an alert to financial institutions and other members of the UK regulated sector warning that Russia is trying to procure UK sanctioned goods through intermediary countries. In January, the agency also issued an alert on the use of specialized art storage sectors by sanctioned individuals.

- The multilateral Russian Elites, Proxies, and Oligarchs (REPO) Task Force in March 2023 issued a global advisory on Russian sanctions evasion. Methodologies included the use of real estate assets to hold value, the use of family members and close associates to ensure continued access and control, the use of complex ownership structures to avoid identification, the use of third-party jurisdictions and false trade information to facilitate the shipment of sensitive goods and technologies to Russia, and the use of enablers in key professions to open bank accounts, send and receive money, and create corporate structures. BIS, OFAC, and the Justice Department that month also issued a joint compliance note on the use of third-party intermediaries or transshipment points to evade Russian- and Belarussian-related sanctions and export controls.

Enhanced Due Diligence for entities located in high-risk jurisdictions such as Russia or its neighboring countries is critical to recognizing evasion attempts. Research may include an analysis of the beneficial ownership of firms involved in shipments of goods to Russia and company leaders' connections to possibly sanctioned entities and individuals, Russian intelligence or military services, and supply chains.

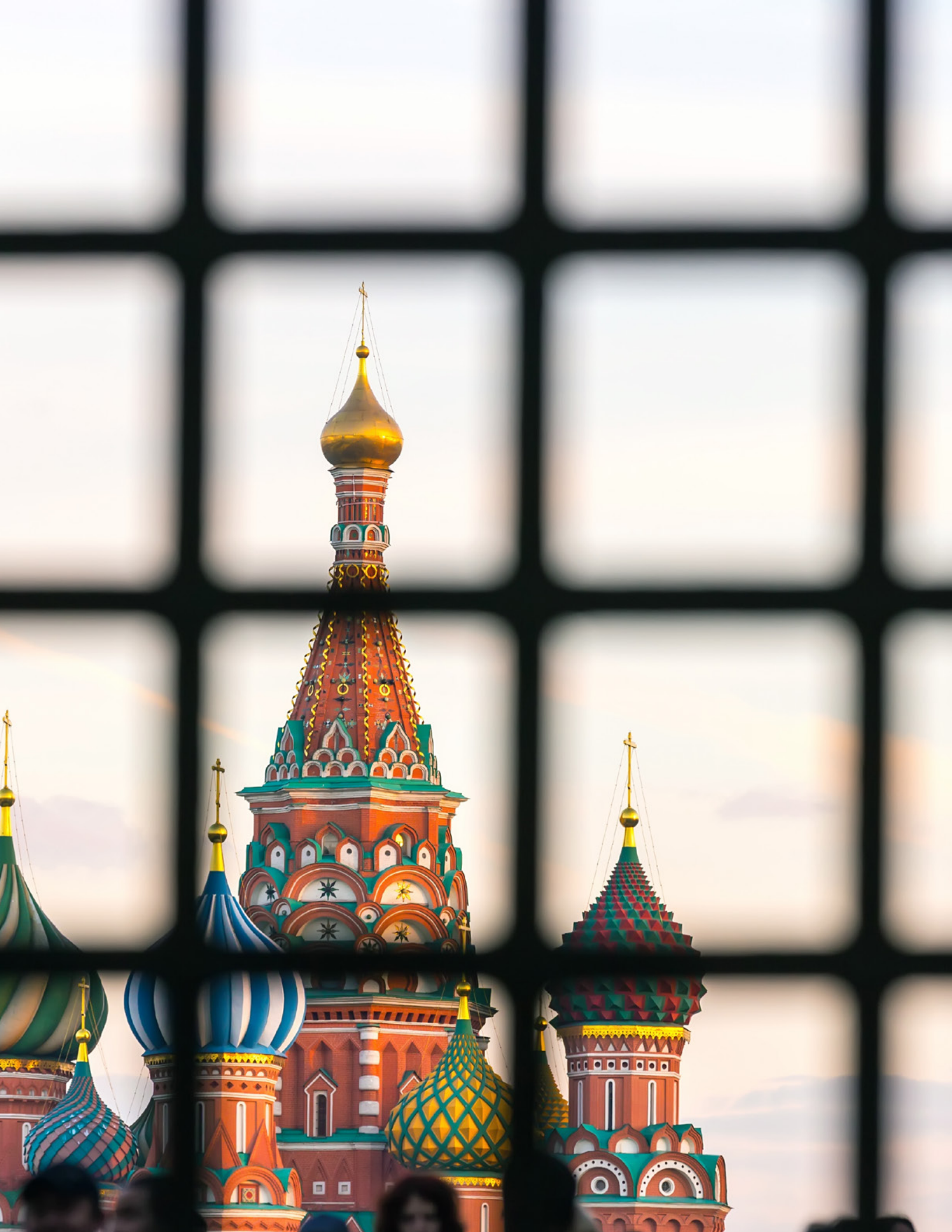


Case Study: Viktor Labin, Groupe d'Investissement Financier, and OOO Sonatek

A recent report by Russian investigative media outlet, the Insider, shone a spotlight on a Russian military intelligence (GRU) officer, Viktor Labin, whose company, Belgium-based Groupe d'Investissement Financier, has been routing European technologies that Russia needs to conduct its war in Ukraine through a shell company in Turkey to Moscow-based OOO Sonatek.

Russia has not been able to create an import-substitution mechanism for coordinate-measuring machines, so its military-industrial complex relies largely on imported products sourced through Sonatek, whose owner and CEO, Ruslan Labin, is Viktor Labin's son. The Insider obtained classified Russian data indicating that in 2022, Sonatek provided supply and maintenance services to at least 18 Russian defense companies. Ruslan confirmed to The Insider that the defense companies mentioned in its report were, indeed, Sonatek's customers, providing corroboration for the information in the outlet's documents.

Viktor Labin, when contacted by The Insider for corroboration to the information about his company's activities, claimed that his Belgian company stopped delivering equipment to Sonatek after sanctions were imposed on Russia in the aftermath of its invasion. However, The Insider obtained records that show Labin's Groupe d'Investissement Financier only stopped delivering machines to Sonatek in April 2023, and that subsequently, the Belgian entity began processing its deliveries to Sonatek through a Turkish shell company with a similar name: Groupe d'Investissement Financier Osborne.



Secondary Sanctions

Secondary sanctions are strictly a US concept that allow the United States to target foreign persons engaged in transactions with specific Russian actors or sectors, even if no US nexus exists. OFAC kin September 2022 issued a determination US Treasury Undersecretary for Terrorism and Financial Intelligence Brian Nelson in February 2023 met with Turkish and UAE government officials and banking sector representatives and threatened to enact secondary sanctions on companies that still trade with Russia in an effort to undermine Russia's ability to procure military materiel to conduct the war in Ukraine.

President Biden in December 2023, signed Executive Order 14114, authorizing secondary sanctions to be imposed on foreign financial institutions found to be involved in significant transactions that help Russia's military industrial sector. Foreign financial institutions that are designated by OFAC for helping Russia's military will face either full blocking sanctions, cutting them off from the US and global financial systems, or face significant restrictions on their US correspondent accounts.

- Banks in Turkey have increased scrutiny of transactions linked to Russia to avoid the risk of secondary sanctions. The move has led to longer processing times for money transfers and instances of funds being returned or delayed. At least two state-owned banks in China are also tightening curbs on their relationships with Russian clients and plan on severing ties with clients on the SDN list and stopping the provision of financial services to the Russian military industry.

- A Chinese bank used by Russian importers this month ceased all settlements with Russia and Belarus. Chouzhou Commercial Bank made the business decision in response to EO 14114, according to Russian media.

WINCH
ONLY

Oil Price Cap

In late 2022, the G7, EU, and Australia, collectively known as the Price Cap Coalition, implemented a $60 per barrel price cap on Russian-origin crude oil in an effort to limit Russia's energy profits. In response, Moscow almost immediately began exploring ways to evade the price cap, using methodologies it has developed since Russia illegally annexed Crimea in 2014 and tactics it learned from Iran and North Korea's known evasion tactics.

Russia uses everything from fraudulent documents to third-country supply chain intermediaries and complex corporate structures to hide the origins of the oil it ships. Russia also determined that failure to itemize costs such as shipping, freight, customs, and insurance can allow it to charge more for its oil and claim that the increased price is simply ancillary costs bundled into the package. In addition, Russia uses a "shadow" fleet of vessels with questionable ownership, multiple changes in flags and registration, and which engage in "dark" activities such as ID and location tampering to transport its oil.

In response to Russia's multiple strategies to ship its oil above the price cap, the United States and its partners have issued multiple guidance, advisories, and alerts to inform and warn stakeholders about indicators of possible Russian evasion activities. In addition, sanctions have been imposed on individuals, entities, and vessels transporting Russian-origin crude oil above the price cap.

- The Price Cap Coalition this month published additional guidance on compliance with the $60 per-barrel cap on Russian oil introduced in 2022. The alert includes an overview of evasion methods and recommendations for detecting and mitigating these techniques, advising stakeholders to look for fraudulent documentation, opaque shipping and ancillary costs, third-country supply chain intermediaries and complex and irregular corporate structures, and other irregularities.

- In its second price cap enforcement action of 2024, OFAC this month designated four entities and identified one vessel, the NS Leader, as blocked property for violating the price cap and transporting Russian Urals crude oil late last year priced at more than $80 per barrel, using the services provided by a covered US entity during the voyage.

- OFAC in late December in coordination with Price Cap Coalition partners, updated its Guidance on Implementation of the Price Cap Policy for Crude Oil and Petroleum Products of Russian Federation Origin, to strengthen the attestation and recordkeeping processes for certain covered service providers and reduce opportunities for bad actors to disguise Russian oil purchased above the cap.

The Yermak McFaul International Working Group this month also published its 18th Working Group Paper highlighting that Russia remains dependent on its energy exports for budget revenues and assessing that the revenues are vulnerable to disruption and reduction. The Working Group recommends stepping up enforcement actions against violators, making illicitly shipping Russian oil too risky, thereby increasing its costs. In addition, the Working Group assesses that targeting oil and gas-related services that Russia relies on for production and exports, such as tech-driven efficiencies, would deprive Russia's energy sector of western tech advancements, forcing it to rely on less advanced technology and limited expertise, as technological experts continue to emigrate outside the country.

Magnitsky Act:

The Magnitsky Act was passed in 2012 by the US Congress and signed by then-President Obama to punish Russian officials responsible for the death of Russian tax attorney Sergei Magnitsky in a Moscow prison in 2009. Magnitsky was imprisoned after investigating a $230 million fraud involving Russian tax officials, and the Magnitsky Act, named for the lawyer, was passed to punish Russian individuals involved in corruption and human rights violations.

After the bill's passage, multiple Russian judges, tax officials, and others were sanctioned pursuant to the Magnitsky Act. Since then, multiple western countries passed their own versions of Magnitsky-style legislation to target corruption and human rights violations, and the Global Magnitsky Act of 2016 authorizes the US government to sanction foreign government officials worldwide who are engaged in corruption and human rights violations, freeze their assets, and ban them from entering the country.

- Canada late last year sanctioned officials in Russia, Iran, and Burma for taking part in human rights violations, including Russians who participated in a violent anti-gay crackdown in Chechnya by overseeing kidnapping and torture against LGBT individuals.

- Czechia last year approved its own version of the Magnitsky Act and sanctioned the head of the Russian Orthodox Church, Patriarch Kirill (aka Vladimir Gundyayev), under the authority for supporting Russia's war in Ukraine.

- The UK last year imposed targeted sanctions on six Russian nationals involved in the arbitrary detention of Russian activist and opposition leader Vladimir Kara-Murza, who was arrested in Russia in April 2022 for condemning Russia's invasion of Ukraine.

Given Russia's documented kidnapping of Ukrainian children and the consequent International Criminal Court's issuance of arrest warrants against Putin and Russia's Commissioner for Children's Rights Maria Lvova-Belova, the documented torture of Ukrainian victims, the intentional targeting of civilian infrastructure in Ukraine, and the arbitrary arrests of western journalists and censorship efforts, the West will almost certainly continue to use Magnitsky authorities to impose additional sanctions on Russian individuals and entities.

The EU in January imposed restrictive measures against four persons and one entity under the EU's Global Human Rights Sanctions Regime. Three individuals were involved in the arbitrary detention of Vladimir Kara-Murza, and one individual and entity—Ekaterina Mizulina and the Safe Internet League she chairs—were designated for serious abuses of freedom of opinion and expression.

In addition to Kara-Murza, Russia has kept opposition leader Alexey Navalny in prison since his attempted poisoning in 2020 and reported that Navalny died on February 16. Western partners are imposing human-rights sanctions against those involved in Navalny's death.

- The UK on February 21 sanctioned six individuals it deems responsible for Navalny's death, including Vadim Konstantinovich Kalinin, who oversaw the prison camp where Navalny was kept in solitary confinement for up to two weeks at a time. Kalinin and the others (high-level officials at the Arctic penal colony where Navalny was kept) are designated under the UK's Global Human Rights Sanctions Regulations.

Moscow in March 2023 detained Wall Street Journal reporter Evan Gershkovich. The journalist was detained on espionage charges by Russia's Federal Security Service while on a reporting assignment in the country. Another journalist, Russian-American Radio Free Europe-Radio Liberty editor Alsu Kurmasheva was detained in Russia in October 2023. A US-Russian dual citizen in early January was arrested in Moscow on supposed drug charges. Robert Woodland Romanov was born in Russia and adopted by a US couple when he was a toddler. He returned to Russia in 2020 and connected with his biological mother.


POLAND
BELARUS
Kiev
SLOVAKIA
UKRAINE
HUNGARY
MOLDOVA
ROMANIA
SERBIA
KOSOVO
BULGARIA
Black Sea
MACEDONIA
GREECE
Ankara
TURKEY
GEORGIA
ARMENIA
Mediterranean Sea
CYPRUS
SYRIA
IRAQ

Conclusion and Key Takeaways

Based on Putin's remarks, Russia's continued adjustments to evade sanctions, and increases in defense spending, Moscow is committed to a long war in Ukraine, which will result in stronger sanctions pressure and enforcement. Firms and financial institutions must be on the lookout for not just evasion efforts, but also monitor supply chains, conduct enhanced due diligence, and update risk assessments, as regulators target Russia's military, government officials, oligarchs, and those who facilitate their access to restricted goods and technologies.

- Although future sanctions and additional restrictions are difficult to predict, adverse media monitoring is critical to ensuring robust compliance efforts. Media outlets can identify possible third-country facilitators, transshipment points and intermediaries, and entities through open-source research and their own sources.

- Expanded US authorities against foreign financial institutions that help Russia's military sector circumvent restrictions will allow secondary sanctions to be imposed. Monitoring clients' transactional activities, researching possible links to Russia's military-industrial base, and regularly updating client profiles can help banks avoid being designated under US secondary sanctions.

- An increased focus on sanctions enforcement means the United States, the EU, the UK, and other jurisdictions will increasingly take coordinated action and collaborate to hold sanctions violators accountable.

- Firms and financial institutions must monitor advisories, alerts, and other guidance issued by regulators, which may contain novel evasion methodologies or red flags indicating a client or counterparty may be evading sanctions. Alerts identifying high-risk goods and sectors, advisories helping stakeholders identify sanctions violations, and guidance highlighting common transactional risks and mitigation measures can help companies enhance their compliance efforts.

- Strategic trade controls will become ever more important as western countries and allies work to prevent Russia from accessing needed technologies, machinery, and other equipment to enhance its military capabilities. The Commerce Department this year already has expanded existing restrictions against Russia and Belarus, including by expanding the scope of the Export Administration Regulations (EAR) Russian and Belarusian Industry Sector Sanctions and making certain changes to the licensing requirements that apply to the occupied Crimea region of Ukraine.

To mark the two-year anniversary of Russia's invasion of Ukraine, the United States, UK, and EU are releasing a flurry designations and associated press releases, as well as new guidance to help stakeholders enhance their compliance efforts. Allies are coordinating their actions against not just Russian entities involved in the country's aggression against Ukraine, but also entities in jurisdictions that help Russia gain access to critical goods and technologies necessary for Moscow to conduct its war in Ukraine. Regulators are increasingly targeting entities in third countries that are reshipping restricted technologies to Russia. Research into customers, trade partners, and their clients' business activities—especially if located in a high-risk jurisdiction such as any of the countries that are known transshipment points for restricted technologies, such as Türkiye, Kazakhstan, Kyrgyzstan and other Central Asian countries, and several Caucasus nations—can be key to detecting and deterring Russian sanctions evasion.