WISCONSIN PROJECT
ON NUCLEAR ARMS CONTROL

# Red Flags in Real Cases

## Enforcement and Evasion of Russia Sanctions

PAUL ESAU

October 2023

## Introduction

Since February 2022, the United States has sanctioned thousands of individuals and companies and imposed export controls on most strategic goods as punishment for Russia's all-out invasion of Ukraine. Enforcing those sanctions and trade controls has required regulators to identify an evolving series of tactics being used to move financial assets and supply controlled goods to Russia or Belarus. To do so, the Departments of Commerce, Treasury, and Justice have publicized "red flags," or potential indicators that a party in a transaction is trying to evade government scrutiny. Red flags are warning signals that indicate an increased risk of fraudulent or illicit activity, like a connection to a sanctioned individual or abrupt changes in buying or shipping patterns.

The Bureau of Industry and Security (BIS) within the Department of Commerce maintains a list of general red flags on its website,[1] as well as a compendium of enforcement investigations titled "Don't Let This Happen to You!"[2] Since early 2022, BIS has also released periodic guidance on new red flags as export evasion practices have evolved.[3] Treasury's Financial Crimes

[1] "Red Flag Indicators," Bureau of Industry and Security World Wide Website, available at https://www.bis.doc.gov/index.php?option=com_content&view=article&id=51&catid=18.

[2] "Don't Let This Happen to You: Actual Investigations of Export Control and Antiboycott Violations," October 2022, U.S. Department of Commerce, available at https://www.bis.doc.gov/index.php/documents/enforcement/1005-don-t-let-this-happen-to-you-1/file.

[3] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Invasion Attempts," FIN-2022-Alert003, June 28, 2022, available at https://www.fincen.gov/sites/default/files/2022-06/FinCENandBisJointAlertFINAL.pdf; "Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls," March 2, 2023, available at https://www.bis.doc.gov/index.php/documents/enforcement/3240-tri-seal-compliance-note/file; "Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts," FIN-2023-Alert004, May 19, 2023, available at https://www.fincen.gov/sites/default/files/shared/FinCENandBISJointAlert_FINAL_508C.pdf; "Guidance to Industry on Iran's UAV-Related Activities," June 9, 2023, available at https://ofac.treasury.gov/media/931876/download?inline; "Exporting Commercial Goods: Guidance for Industry and Academia," BIS, September 26, 2023, available at https://www.bis.doc.gov/index.php/documents/enforcement/3336-2023-09-26-export-enforcement-five-guidance-for-industry-and-academia-priority-hs-codes/file.

Enforcement Network (FinCEN) has released similar lists of red flags specifically targeting financial transfers.[4] The red flags listed in this report are compiled from the above sources.[5]

Red flags aren't just guidelines – they also have legal implications. Exporters or financial institutions who encounter red flags are obligated to investigate and verify the transaction by "Know Your Customer" requirements within the U.S. Export Administration Regulations (EAR) or "Suspicious Activity Reporting" (SAR) requirements under by the Bank Secrecy Act.[6] Ignoring red flags, or worse, "self-blinding" by discouraging customers from sharing information about the ultimate end use or destination of the transaction, does not protect the exporter against liability.[7] In fact, doing so may increase the consequences of any enforcement action by the U.S. government.[8]

Red flags can arise in connection with many aspects of an export transaction, including (1) the product to be exported, (2) the customer buying the product, (3) the network or corporate

---

[4] "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts," FIN-2022-Alert001, March 7, 2022, available at https://www.fincen.gov/sites/default/files/2022-03/FinCENAlertRussianSanctionsEvasionFINAL508.pdf; "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and Their Family Members," FIN-2022-Alert002, March 16, 2022, available at https://www.fincen.gov/sites/default/files/2022-03/FinCENAlertRussianElitesHighValueAssets_508FINAL.pdf; "FinCEN Alert on Potential U.S. Commercial Real Estate Investments by Sanctioned Russian Elites, Oligarchs, and Their Proxies," FIN-2023-Alert002, January 25, 2023, available at https://www.fincen.gov/sites/default/files/shared/FinCENAlertRealEstateFINAL508_1-25-23FINALFINAL.pdf.

[5] The red flags listed in these sources vary widely in target and scope. This report has synthesized red flags repeated across multiple sources, and omitted some for which clear examples could not be found. Some red flags have evolved as the U.S. sanctions regime has become stricter, changing patterns of evasion.

[6] "Supplement No. 3 to Part 732," Title 15, Code of Federal Regulations, available at https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-732/appendix-Supplement%20No.%203%20to%20Part%20732; "Suspicious Activities Report (SAR)," Office of the Comptroller of the Currency World Wide Website, available at https://www.occ.treas.gov/topics/supervision-and-examination/bank-operations/financial-crime/suspicious-activity-reports/index-suspicious-activity-reports.html.

[7] "Know Your Customer Guidance," Bureau of Industry and Security World Wide Website, available at https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/47-know-your-customer-guidance.

[8] "Guidance on Charging and Penalty Determinations in Settlement of Administrative Enforcement Cases," Federal Register, Vol. 81, No. 120, June 22, 2016, p. 40508, available at https://www.govinfo.gov/content/pkg/FR-2016-06-22/pdf/2016-14770.pdf.

structure of the customer, (4) the export destination, (5) the logistics of the transaction, and (6) the alleged end use.

This report reviews the evolution of U.S. sanctions and trade restrictions since Russia's 2014 invasion of Ukraine and annexation of Crimea. It then illustrates common red flags using examples from ten recent U.S. enforcement cases (Appendix I) involving illicit exports or financial transfers to Russian entities, as well as several other investigations. What emerges is both a picture of the growing complexity of sanctions evasion and the corresponding importance of export compliance by exporters and financial institutions.

## The Evolution of Sanctions since 2014

The United States began imposing sanctions on Russian individuals, as well as the Russian financial, energy, and defense sectors, after the 2014 invasion of Crimea.[9] Additional rounds of sanctions were imposed in response to the chemical weapons attacks on Sergei Skripal in 2018 and Alexei Navalny in 2020, as well as Russian cyber intrusions, human rights abuses and weapons proliferation.[10] The sanctions include a U.S. arms embargo on transfers of military equipment, military financing, or military services to Russia, as well as a general "presumption of denial" on the export of most dual-use goods designated with an Export Control Classification Number (ECCN) and covered by the BIS Commerce Control List (CCL).[11]

On February 24, 2022, an unprecedented series of sanctions and export controls were imposed on Russia by the United States and its allies in response to Russia's full-scale invasion of Ukraine.[12] Nearly 1,700 entities were added to Treasury's Specially Designated Nationals (SDN)

---

[9] "U.S. Sanctions on Russia: An Overview," Congressional Research Service, August 29, 2019, available at https://crsreports.congress.gov/product/pdf/IF/IF10779/7.

[10] "Russia: The Navalny Poisoning, Chemical Weapons Use, and U.S. Sanctions," Congressional Research Service, August 26, 2021, available at https://crsreports.congress.gov/product/pdf/IF/IF11872; "U.S. Sanctions on Russia: An Overview," August 29, 2019.

[11] "U.S. Sanctions on Russia," Congressional Research Service, January 18, 2022, pp. 21-22, available at https://sgp.fas.org/crs/row/R45415.pdf; "How to Determine an Export Control Classification Number (ECCN)," Department of Commerce, available at https://www.bis.doc.gov/index.php/documents/regulations-docs/143-bis-eccn-pdf/.

[12] "Fact Sheet: Joined by Allies and Partners, the United States Imposes Devastating Costs on Russia," The White House, February 24, 2022, available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/fact-sheet-joined-by-allies-and-partners-the-united-states-imposes-devastating-costs-on-russia.

list and more than 370 to Commerce's Entity List; in addition, both the Russian financial and energy sectors were heavily restricted.[13] A wide swathe of dual-use and luxury goods were targeted immediately, and two new U.S. Foreign Direct Product (FDP) rules were created to control multi-step manufacturing and expand the reach of U.S. export restrictions.[14] The United States imposed a similar regime against Belarus on March 2, 2022.[15] In the words of National Security Advisor Jake Sullivan, the United States and its allies targeted Russia with "the most stringent technological restrictions ever imposed on a major economy"[16]

The primary intent of this coordinated sanctions campaign was to deprive Russia of electronics, materials, and sub-components needed by the Russian defense, aerospace, and maritime sectors and essential to its war machine. However, they also targeted the assets and lifestyles of the Russian elite supporting and profiting from war. Treasury's Financial Crimes Enforcement Network (FinCEN) issued two alerts in March 2022 highlighting red flags in financial transactions and potential transfers of real estate, luxury and high-value goods, and artwork, reflecting a focus on the assets of Russian oligarchs, elites, and their proxies.[17] The opacity of the real estate and art markets in particular were identified as key mechanisms for sanctions evasion with red flags specific to each market.[18] In the spring of 2022, a multilateral task force

---

[13] "Sanctions by the Numbers: 2022 Year in Review," Center for a New American Security, August 3, 2023, available at https://www.cnas.org/publications/reports/sanctions-by-the-numbers-2022-year-in-review.

[14] "Implementation of Sanctions Against Russia Under the Export Administration Regulation (EAR)," Federal Register, Vol. 87, No. 42, March 3, 2022, available at https://www.govinfo.gov/content/pkg/FR-2022-03-03/pdf/2022-04300.pdf.

[15] "U.S. Department of Commerce & Bureau of Industry and Security Russia and Belarus Fact Sheet," Department of Commerce World Wide Website, February 24, 2022, available at https://www.commerce.gov/news/fact-sheets/2022/02/us-department-commerce-bureau-industry-and-security-russia-and-belarus.

[16] "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit," The White House, September 16, 2022, available at https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit.

[17] "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and Their Family Members," March 16, 2022.

[18] "National Money Laundering Risk Assessment," Department of the Treasury, February 2022, p. 1., available at https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf; "The Art Industry and U.S. Policies That Undermine Sanctions," Staff Report, United States Senate Permanent Subcommittee on Investigations, July 27, 2020, p. 1, available at https://www.govinfo.gov/content/pkg/GOVPUB-

*(footnote continued)*

codenamed "REPO" blocked or froze more than $30 billion in assets owned by sanctioned Russian oligarchs, including luxury properties and several yachts.[19]

After Ukraine repulsed the initial onslaught, saving Kyiv, U.S. attention shifted to restricting supply networks for Russian military industry. Electronics, semiconductors, and precision instruments have been a particular focus of regulatory attention because of their utility in military systems and easy transportation/diversion. At several points, BIS, FinCEN, and Treasury's Office of Foreign Assets Control (OFAC) have issued joint alerts flagging lists of dual-use electronics at a particularly high risk of diversion to Russian military end users.[20] On May 19, 2023, BIS imposed licensing requirements on three full chapters of HTS codes covering electronics, instruments, and advanced fibers – a total of more than 1,200 new items. In early June, Commerce, Justice, State, and Treasury released another alert listing key electronics, engines, and components used by Iran to manufacture unmanned aerial vehicles (UAVs) being deployed by Russia in Ukraine.[21] The ubiquity of semiconductors and electronic components in both military and civilian systems has made them an important battleground in the economic war against Putin's regime.

The new rules disrupted conventional supply chains and attempted to exploit a key Russian vulnerability: its critical reliance on high technology imports.[22] However, they also created a lucrative market for those willing to continue supplying controlled goods despite the export

---

Y4_G74_9-PURL-gpo142344/pdf/GOVPUB-Y4_G74_9-PURL-gpo142344.pdf; "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and Their Family Members," March 16, 2022.

[19] "Russian Elites, Proxies, and Oligarchs Task Force Joint Statement," Department of the Treasury World Wide Website, June 29, 2022, available at https://home.treasury.gov/news/press-releases/jy0839.

[20] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Invasion Attempts," p. 3; "Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts," May 19, 2023, p.7.

[21] "Guidance to Industry on Iran's UAV-Related Activities," June 9, 2023, p. 5.

[22] Albeit at higher cost and requiring extraordinary effort from the Russian state. Max Bergmann, Maria Snegovaya, Tina Dolbaia, Nick Fention, *Out of Stock? Assessing the Impact of Sanctions on Russia's Defense Industry,* Center for Strategic & International Studies, April 2023, p. 13, available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230414_Bergmann_Out_Stock.pdf?VersionId=6jfHCP0c13bbmh9bw4Yy2wbpjNnfeJi8.

controls. Many sources have detailed how dual-use and high-technology goods have continued to flow into Russia, allegedly even approaching pre-war levels.[23]

## I. The Product

Although the spectrum of goods under U.S. export controls is vast, the alerts issued by U.S. authorities have highlighted certain categories as especially important. The direct export of military articles and services is obviously prohibited because of their utility on the Ukrainian battlefield. High-value luxury goods, such as real estate, aircraft, yachts, artwork, and precious metals, stones, and jewelry (PMSJ) have also been targeted as means of imposing pain on Russian elites. Finally, computer chip and microelectronic controls have been identified as crucially important to slowing Russian military industry, especially production of missiles and UAVs.

### RED FLAGS:

1. Is the product at high risk of diversion because of its potential end use by a Russian military producer or in another sanctioned sector?

    a. In June 2022, BIS and FinCEN published a list of ECCNs considered "Commodities of Concern," including aircraft parts, GPS systems, and oil field equipment.[24]

    b. Seven of the ten cases used in this report involve the illicit transfer of items classified under ECCNs on this list (Cases 1, 2, 3, 4, 5, 6, 7). Certain items, such as aircraft parts/equipment, antennas, integrated circuits, and spectrum analyzers, appear in multiple cases.

2. Is the product at high risk of diversion because of its previous use in Russian munitions or military systems?

    a. In May 2023, BIS and FinCEN published a list of HS Codes considered "High Priority Items," including integrated circuits, capacitors, and wireless

[23] *Out of Stock? Assessing the Impact of Sanctions on Russia's Defense Industry,* April 2023, p. 19; Daniel Bush, "Russian Military Uses China in Sourcing Banned Tech from 59 U.S. Firms," Newsweek, June 21, 2023, available at https://www.newsweek.com/exclusive-russias-vast-sanctions-evasion-secures-us-european-tech-weapons-1807939.

[24] For the complete list, see p. 3. "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Invasion Attempts."

transceivers.[25] Items were included because of their similarity to components in Russian systems recovered from the battlefield.

b. On September 14, 2023, BIS published a tiered list of 45 "common high-priority items" by HS Code that consolidated and expanded on previous notices.[26] Two weeks later, the United States, Australia, Canada, New Zealand, and the United Kingdom (collectively the "Export Enforcement Five" or "E5") released a joint guidance notice prioritizing the new tiered list for export enforcement in all five countries.[27]

c. U.S. government releases have routinely emphasized the connection between export evasion and battlefield use. For example, advanced semiconductors and microprocessors smuggled by Yury Orekhov's network via front company NDA GmbH (Case 1) have been found in recovered Russian systems.[28]

3. Is the product identified as a key component in the production of Iranian UAVs being used by the Russian military?

a. In February 2023, in response to the sale of Iranian drones to the Russian military, BIS imposed additional licensing requirements on certain low-technology aircraft components, navigation equipment, and electronics destined to Iran, Russia, or Belarus.[29] The new regulations also created a new Foreign Direct Product (FDP) rule for Iran, and revised the existing Russia/Belarus FDP rule to include the new items. In May, U.S. authorities published an alert

---

[25] "Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts," May 19, 2023, pp. 6-7.

[26] "Russian Export Controls – List of Common High-Priority Items," BIS, September 14, 2023, available at https://www.bis.doc.gov/index.php/2011-09-14-14-10-06/russia-export-controls.

[27] "Exporting Commercial Goods: Guidance for Industry and Academia," BIS, September 26, 2023.

[28] "Justice Department Announces Charges and Arrests in Two Cases Involving Export Violation Schemes to Aid Russian Military," Department of Justice, October 19, 2022, available at https://www.justice.gov/opa/pr/justice-department-announces-charges-and-arrests-two-cases-involving-export-violation-schemes.

[29] "Export Control Measures Under the Export Administration Regulations (EAR) To Address Iranian Unmanned Aerial Vehicles (UAVs) and Their Use by the Russian Federation Against Ukraine," Federal Register, Vol. 88, No. 38, February 27, 2023, available at https://www.govinfo.gov/content/pkg/FR-2023-02-27/pdf/2023-03930.pdf.

explaining how new controls on certain aircraft components, navigation equipment, and electronics increased the likelihood of illegal attempts to divert these goods to Iran's highly export-dependent UAV manufacturers.[30]

b. In April 2023, OFAC designated a sanctions evasion network run by Mehdi Khoshghadam, head of Iran's Pardazan System Namad Arman (PASNA).[31] The network leveraged front companies in Iran, Malaysia, Hong Kong and China to supply electronic components to the Iranian government, military industry, and UAV program.

## II. The Customer

Since February 24, 2022, escalating sanctions have forced Russian and Belarusian entities to both create new illicit supply chains and adapt existing chains to illicit purposes. Increasingly, new entities have been incorporated or adapted to maintain the flow of military or dual-use products to sanctioned entities and to facilitate payment to suppliers. In response, BIS has recommended that export deals involving controlled items to entities created after February 24, 2022 should be flagged as potentially suspicious. However, especially early in the war, pre-existing supply chains were often leveraged to conduct newly illicit transactions. Entities with a history of exports to Russia/Belarus, or that developed a sudden interest in controlled items (or request a significant increase in exports of controlled items) after February 2022 were also identified for flagging.

### RED FLAGS:

1. Is the entity found on a sanctions list?

    a. Although most would-be smugglers seek to conceal their identity, particularly if they have been specifically designated, they do occasionally make mistakes. In June 2015, Andrey Shevlyakov (Case 2) used his own name in transactions with an American electronics distributor. After the distributor responded with an image of Shevlyakov's entry on the BIS Entity List, he cancelled the order.

---

[30] "Guidance to Industry on Iran's UAV-Related Activities," June 9, 2023.

[31] "Treasury Sanctions Procurement Network Supporting Iran's UAV and Military Programs," Iran Watch, April 19, 2023, available at https://www.iranwatch.org/library/governments/united-states/executive-branch/department-treasury/treasury-sanctions-procurement-network-supporting-irans-uav-military-programs.

2. Does the entity have a history of shipping to Russia or Belarus, even if the exported item is allegedly going to a non-sanctioned destination?

    a. Cyril Buyanovsky and Douglas Robertson (Case 4) had been exporting avionics equipment to Russia for years before new controls made their transfers illegal. Their company, which was based in Kansas, was literally named KanRus Trading.

3. Does the entity have any connection with the Russian Federal Security Services (FSB), the Russian military, or to an entity owned by the Russian state?

    a. Russian or Belarusian entities occasionally display FSB certificates on the Russian language version of their websites to indicate that they are authorized to work on classified projects. The phrase "special purpose projects" may also be used as a designation for military use.[32] For example, the website of Russia-based aviation company Aviazapchast displays five digital certificates, including one from the FSB.[33]

    b. State-linked companies often have the following designations within their business name: RAO, FGUP/FSUE, GK, SPRE/NIPP, and NPO/GNPO.[34]

4. Has the entity recently changed its name or reincorporated?

    a. In 2016, JSC Radioexport (Case 1), a trading company in Moscow, was added to the Entity List for supplying Russian military industry. Shortly afterward, Radioexport changed its name to JSC Network Technologies and began operating as a new company in an attempt to evade U.S. sanctions.

    b. After Andrey Shevlyakov (Case 2) and his company, Yaxart OU, were added to the Entity List in 2012, he removed himself and his wife from the management board and changed the company name to Metsandus OU. Metsandus continued

[32] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," June 28, 2022, p. 6

[33] As of September 2023. "Licenses and Certifications," Aviazapchast World Wide Web site, available at aviazapchast.com/about/license.

[34] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," June 28, 2022, p. 7.

to engage in illicit procurement activities under a new name and owner, and with a different address.

5. Has the entity recently purchased shipping vessels for no obvious business purpose? Is the entity situated on a shipping corridor with access to sanctioned countries?

    a. According to the Wall Street Journal, since 2021, the Turkish firm Beks Ship Management has purchased 37 vessels, including many old tankers, which operate as part of a "ghost fleet" trafficking in Russian oil.[35] Beks which began as a side venture for a Turkish socks and underwear magnate, has expanded the value of its fleet ten-fold in the last three years. Ships owned by the company load oil at Russian ports in the Pacific before sailing to China, India, and other buyers.

## III. The Network

The most common method of sanction evasion is the use of front or shell companies, third-party intermediaries, and/or transshipment points to disguise the involvement of sanctioned entities or Russian end users.[36] The use of networks of intermediaries allows sanctioned individuals or corporations to disguise both the destination of the purchased goods as well as the origin of payment for those goods.

### RED FLAGS:

1. Does an entity involved in the transfer have a connection to a previously sanctioned person, company, or address?

    a. In March 2022, the State Department designated a Russian defense-related firm, Radioavtomatika, for supplying foreign equipment to Russian military end

[35] Jared Malsin, "The Ghost Fleet Helping Russia Evade Sanctions and Pursue Its War in Ukraine," The Wall Street Journal, August 18, 2023, available at https://www.wsj.com/business/energy-oil/the-ghost-fleet-helping-russia-evade-sanctions-and-pursue-its-war-in-ukraine-19e77a0c, accessed on August 31.

[36] "Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls," March 2, 2023, p. 1.

users.[37] Over the following months, several Radioavtomatika officials established a network of front companies and intermediaries in Armenia, China, and Uzbekistan to evade sanctions and continue importing critical technologies. Another Russian company, Novastream Limited, was set up at the same address as a former Radioavtomatika representative office under a director also linked to the sanctioned company.[38]

   b. Between 2018-2020, German company NDA GmbH (Case 1) was used to conduct multiple purchases of controlled electronics from U.S. companies, despite being co-owned by Yury Orekhov. Orekhov is heavily linked to Russian oligarch Oleg Deripaska and his aluminum company Rusal, which were sanctioned in 2018.

2. Do all entities involved in the transfer have a web presence? Does its alleged address correspond to a physical office?

   a. Yury Orekhov (Case 1) and his co-conspirators often claimed that Malaysian company NDA Aerospace was an intermediary or end user in transactions with U.S. companies. However, U.S. investigators later discovered that only one of the multiple Malaysian addresses listed for the company had visible signage – a single empty room in a strip mall. In reality, "NDA Aerospace" was a shell entity run by Orekhov and fellow defendant Svetlana Kuzurgasheva.

3. Is any entity involved in the transfer using a personal email address or home address?

   a. Boris Livshits (Case 3) created a front company called Strandway LLC to receive shipments of U.S.-origin dual-use goods before exporting them to Europe. He often used the New Hampshire residence of fellow defendant Alexey Brayman as the company's address of record. Brayman would receive shipments at his home before repackaging them for transfer to Europe.

---

[37] "Targeting Russian Elites and Defense Enterprises of Russian Federation," Department of State, March 3, 2022, available at https://www.state.gov/targeting-russian-elites-and-defense-enterprises-of-russian-federation.

[38] "Treasury Imposes Swift and Severe Costs on Russia for Putin's Purported Annexation of Regions of Ukraine," Department of the Treasury, September 30, 2022, available at https://home.treasury.gov/news/press-releases/jy0981; "Treasury-Commerce-State Alert: Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex," October 14, 2022, p. 4, available at https://ofac.treasury.gov/media/928856/download?inline.

b. Andrey Shevlyakov (Case 2) used eight Estonian shell companies to obscure his involvement in the procurement of U.S.-origin microelectronics. Several of the companies were owned by Shevlyakov's wife or had been previously registered to the couple's address in Tallinn.

c. Ilya Balakaev (Case 5) often smuggled spectrum analyzers and signal generators from the U.S. on his person after having ordered them online to the home of an accomplice in Virginia. Between April 2020 and March 2021, Balakaev caused 30 shipments of spectrum analyzers and associated parts to be shipped to the Virginia address.

4. Is the entity's order similar in content and value to a previously rejected order from a different party?

    a. After being recruited by the Serniya Network in 2017, Nikoloas Bogonikolos (Case 6) was instructed by Yevgeniy Grinin (Case 3) to acquire controlled items from a Minnesota-based company. Since the company had previously rejected an order from Grinin for export to Russia, Bogonikolos attempted to disguise the similarity by adding several new items to his request and stating that the end user was in the Netherlands.

5. Is there a common set of financial institutions, individuals, or addresses linking multiple transactions to a sanctioned individual?

    a. In 2018, Graham Bonham-Carter (Case 8) was instructed to set up a company in his name to manage Russian oligarch Oleg Deripaska's property in London following the imposition of sanctions on Deripaska. In 2021, this company was also used to facilitate payment from Deripaska to another company that managed the oligarch's properties in New York and Washington. Around the same time, Bonham-Carter used his personal credit card to pay the shipping cost for 18 pieces of art purchased by a third shell company, Turcos Limited, at a New York auction house. His connection to the properties, art, and Deripaska increased the risk of each individual transaction.

6. Does the transaction involve law firms in offshore financial locations, especially those with historical connections to Russian elites?

a. In February 2023, OFAC sanctioned Igor Vladimirovich Zimenkov, a Cyprus- and Russia-based arms dealer operating a sanctions evasion network supporting Russian military industry.[39] Several companies in the network, including GMI Global Manufacturing & Integration LTD, GBD Limited, Kliosa Limited, and Mateas Limited, shared a registered address associated with Assiotis Andreas & Partners LLC, a Cyprus-based law firm. According to the Assiotis Andreas & Partners website, the firm specializes in serving Russian clients with corporate registration services.[40]

## IV. The Destination

Since most strategic goods can no longer be shipped directly from the United States to Russia or Belarus, illicit transactions are often routed through transshipment points in other, less-scrutinized jurisdictions. According to BIS, common destinations for transshipment include Armenia, Brazil, China, Georgia, India, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, Singapore, South Africa, Taiwan, Tajikistan, Turkey, United Arab Emirates (UAE), and Uzbekistan.[41] Countries such as Armenia, Brazil, China, India, Nicaragua, Turkey, and Uzbekistan have been particularly reluctant to increase export monitoring and enforcement, making them favorable vectors for sanctions evasion.[42] Many countries proximate to Russia, including Armenia, Kazakhstan, and Turkey have experienced exponential growth in imports and exports of electronics and other sanctioned goods – indicating the increased importance of those countries to the Russian market.[43]

---

[39] "Treasury Targets Global Sanctions Evasion Network Supporting Russia's Military-Industrial Complex," Press Release, Department of the Treasury, February 1, 2023, available at https://home.treasury.gov/news/press-releases/jy1241, accessed on August 31, 2023.

[40] As of September 2023. "About Us," Assiotis Andreas & Partners LLC World Wide Web site, available at http://assiotislaw.com/about-us.

[41] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," June 28, 2022, p. 5.

[42] David Albright, Sarah Burkhard, and Spencer Faragasso, "A Strategic Challenge: A Peddling Peril Index Analysis of Countries' Restricted Russia Trade," Institute for Science and International Security, July 10, 2023, available at https://isis-online.org/isis-reports/detail/a-strategic-challenge-a-PPI-analysis-of-countries-restricted-Russia-trade.

[43] Agathe Demarais, "No, Russia is Not Massive Skirting Sanctions," Foreign Policy, May 25, 2023, available at https://foreignpolicy.com/2023/05/25/russia-sanctions-evasion-west-ukraine-war-oil-gas-semiconductors-china; Jeffrey A. Sonnenfeld and Michal Wyrebkowski, "The Dangerous Loophole in Western Sanctions on Russia,"
*(footnote continued)*

## RED FLAGS:

1. Is the exported item being shipped or delivered to a common transshipment point or by an abnormal route?

    a. Between 2020 and 2022, Cyril Buyanovsky and Douglas Robertson (Case 4) were directed by their Russian customers to ship avionics equipment to locations in Armenia, Germany, Laos, and the UAE for eventual reexport to Russia.

    b. In 2022, Oleg Patsulya and Vasilii Besedin (Case 7) attempted to ship aircraft brake assemblies to the Maldives and Turkey for eventual reexport to Russia.

    c. In October 2022, Vadim Konoshchenok (Case 3) was detained at the Russian-Estonian border. Hidden in his truck were 35 different types of U.S.-origin semiconductors and electronic components, as well as thousands of rounds of sniper ammunition sold for alleged end use in Finland, Germany, Latvia, and Luxembourg. The physical proximity of various European countries to Russia made them ideal conduits for transshipment.

2. Is a bank, financial institution, or freight forwarding firm listed as the item's final destination?

    a. Freight forwarders, banks, and financial institutions do not typically consume items, which means they are rarely the final destinations for export shipments. Transactions allegedly intended for freight forwarders in traditional transshipment hubs should be scrutinized carefully.[44]

    b. In 2022, Oleg Patsulya and Vasilii Besedin (Case 7) attempted to use their company, MIC, to procure aircraft brake assemblies in the U.S. for end use by several Russian airlines. In one instance, parties assured their U.S. supplier that the assemblies would be used in Turkey, although they had already arranged for a Turkish freight forwarder to ship the parts to Russia. In another, they listed a freight forwarder in the Maldives (Intermodal Maldives) as the Ultimate

---

Foreign Policy, September 7, 2023, available at https://foreignpolicy.com/2023/09/07/western-sanctions-russia-ukraine-war.

[44] "FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts," June 28, 2022, p. 6.

Consignee for two brake assemblies, despite having once again arranged for the parts to be reexported to Russia.[45]

## V. The Transaction

The cat-and-mouse game between sanctions evasion and sanctions enforcement is constantly evolving, and often requires nefarious actors to abruptly change shipping routes or payment methods. These changes may seem confusing or needlessly complicated to suppliers, or lead to false statements on shipping documentation.

### RED FLAGS:

1. Does the entity prefer to pay cash for an item that would usually be financed?

    a. Yury Orekhov and co-conspirator Juan Fernando Serrano Ponce (Case 1) used couriers to deliver bulk cash payments to companies in Venezuela and Russia. The cash, exchanged for Venezuelan oil, helped the network evade sanctions against both countries.

2. Does the entity attempt last-minute changes to shipping instructions that seem to contradict customer history or previous practice?

    a. In December 2022, Vasilii Besedin (Case 7) attempted to purchase two aircraft brake assemblies from a company in Florida and have them shipped to the Maldives. After discovering that shipments to the Maldives were receiving special scrutiny from U.S. Customs, he asked the supplier to ship the assemblies to Turkey instead. The shipment was interdicted by BIS.

3. Has the invoice or other business document been altered to obscure the ultimate customer?

    a. In 2018, Richard Masters (Case 9) told the Spain-based company managing Russian Oligarch Viktor Vekselberg's yacht, the *Tango*, to begin referring to it as the *Fanta* on official documentation. Employees from the company created a digital invoice bearing the new name for subsequent contracts with U.S. companies.

---

[45] Indictment, p. 22; "Oleg Sergeyevich Patsulya…" BIS, Federal Register, Vol. 88, No. 97, May 19, 2023, available at https://www.govinfo.gov/content/pkg/FR-2023-05-19/pdf/2023-10750.pdf.

4. Has the buyer declined routine maintenance for the purchased commodity?

    a. In 2015, Texas-based Vorago Technologies shipped a radiation and temperature-hardened 16Mb SRAM wafer valued at $125,000 to a Bulgarian-based client, MTIG. A few months later, Vorago's Vice President of International Sales offered to travel to Bulgaria to oversee assembly. MTIG did not agree to the visit, and subsequently shipped the goods to Russia.[46]

5. Is payment coming from a third-party country or business?

    a. Because of U.S. sanctions, Cyril Buyanovsky (Case 4) often received payment to KanRus Trading Company from one country for goods being shipped to another. For example, in 2020, Buyanovsky received payment from a company in UAE for repairing avionics equipment he later shipped to Germany. One piece of the equipment had arrived bearing an FSB sticker and was obviously Russian in origin.

    b. Between 2018 and 2021, Richard Masters (Case 9) routinely directed employees of a Spain-based yacht company to charge purchases to their personal debit or credit cards to avoid U.S. scrutiny. In one case, Masters asked a U.S. company to invoice a third party rather than the *Tango* to avoid a U.S. wire transfer.

6. Is the entity purchasing small numbers of dual-use products from multiple, similar suppliers?

    a. Boris Livshits (Case 3), acting as an intermediary between the Serniya Network and U.S. suppliers, favored breaking up large orders to avoid attention from U.S. law enforcement. For example, in 2019 the Physics Institute of the Russian Academy of Sciences (FIAN) requested a "chip set" of 45 advanced semiconductors, which Livshits argued should only be purchased 5-10 items at a time.

7. Does the entity undervalue, or ask to undervalue, the purchase on shipping documentation?

---

[46] "Order Relating to Silicon Space Technology Corporation d/b/a Vorago Technologies, Inc.," BIS, September 28, 2021, available at https://efoia.bis.doc.gov/index.php/documents/export-violations/export-violations-2021/1333-e2686/file.

a. Most U.S.-origin exports require filing an electronic notice within the U.S. Automated Export System (AES).[47] However, shipments valued at under $2,500 are generally exempt from this requirement.[48] Additionally, U.S. entities and banks who receive or process a transaction exceeding $10,000 are required to report it to the IRS.[49] Entities engaging in export evasion may seek to exploit these thresholds.

b. In January 2021, Douglas Robertson (Case 4) emailed an invoice for a $28,769 equipment repair to an intermediary for a Russian aerial services company. The intermediary responded by proposing the goods be undervalued at $3,645, to which Robertson replied "can I change value to less than $2,500? Less paperwork for me." The final shipping label and invoice claimed the value of the equipment was $2,275.

c. In December 2020, Boris Livshits (Case 3) made a $9,900 payment from a front company for an oscilloscope which would typically cost far more than $10,000. Livshits seemed to have been undervaluing the equipment to avoid IRS reporting requirements.

## VI. The End Use

Exporters of U.S. controlled goods are generally required to follow due diligence obligations in researching potential customers and how they will use the goods. In many cases, the ultimate consignee is required to sign an "End User Statement" as well as a "Destination Control Statement" explaining the final purpose of the good and promising to notify the supplier before any re-export. End User Statements are an essential source of red flags for exporters.

---

[47] "Filing Your Export Shipments Through AES," International Trade Administration World Wide Website, available at https://www.trade.gov/filing-your-export-shipments-through-automated-export-system-aes.

[48] "Subpart D-Exemptions From the Requirements for the Filing of Electronic Export Information," Title 15, Code of Federal Regulations, August 22, 2023, available at https://www.ecfr.gov/current/title-15/subtitle-B/chapter-I/part-30/subpart-D.

[49] "Introduction to the Bank Secrecy Act," Bank Secrecy Act, Anti-Money Laundering, and Office of Foreign Assets Control, Sec. 8.1, Federal Deposit Insurance Corporation, p. 1, available at https://www.fdic.gov/regulations/safety/manual/section8-1.pdf; "Understand How to Report Large Cash Transactions," IRS World Wide Website, February 2021, available at https://www.irs.gov/newsroom/understand-how-to-report-large-cash-transactions.

## RED FLAGS:

1. Does the alleged end use match historical patterns of evasion?

    a. Since 2014, the United States has imposed multiple rounds of sanctions on Russia's space sector, while providing limited exceptions for goods supporting government space cooperation.[50] Claiming that an export would be used by a Russian state space corporation to further such cooperation was therefore a common method of sanction evasion early in the war. For example, in 2018 Yuri Orekhov (Case 1) obtained advanced semiconductors and microprocessors from U.S. producers by claiming that the end use was related to the International Space Station (ISS), or that the end user was ROSCOSMOS, the Russian equivalent of NASA.

2. Is the customer or purchasing agent reluctant to answer questions about the end use of the item?

    a. In several cases, inquiries about end use foiled attempts to procure dual-use goods for Russian entities. For example, in Case 1, part of a fraudulent order intended for the Moscow-based Research Institute of Precision Instruments was detained by the supplier because of unanswered questions about the end use. In Case 7, an automated disclaimer about end use from a U.S. supplier deterred Oleg Patsulya from pursuing an order. Instead, he forwarded the email onward to another conspirator, noting "Do not write to these freaks."

3. Is the item incompatible with the stated end use?

    a. In at least one transaction involving sensitive military-grade technology, Yury Orekhev (Case 1) informed his U.S. suppliers that an item would be used for applications in space, even though its specifications were only suitable for use in military aircraft or missile systems.

    b. After importing a U.S.-origin jig grinder for Latvian company CNC Weld, Eriks Mamonovs (Case 10) claimed the grinder was too large to fit inside the CNC Weld plant. Mamonovs used this alleged incompatibility with the agreed end use

[50] Jeremy Grunert, "Sanctions and Satellites: The Space Industry After the Russo-Ukrainian War," War on the Rocks, June 10, 2022, available at https://warontherocks.com/2022/06/sanctions-and-satellites-the-space-industry-after-the-russo-ukrainian-war.

to justify his decision to transfer the grinder to another company, Sapphire Universal, LLP. In fact, this transfer had been planned from the beginning of the conspiracy.

4. Is the item more sophisticated (advanced) than needed for the stated end use?

    a. During negotiations between Vorago Technologies and Ilias Sabirov, Sabirov claimed an evolving series of potential end uses for Vorago's 16Mb SRAM wafers in Bulgaria. These included robotics applications, device assembly and testing, motion control for heavy industry machines, and automotive engine and exhaust systems.[51] Radiation and temperature-hardened wafters (like those sold by Vorago) are generally too expensive for use in civilian automotives but are critical components of missiles and military satellites.

## Conclusion

The red flags listed by U.S. government agencies and tangible examples of those flags in recent U.S. enforcement actions provides insight into the variety of networks, routes, and tactics used by sanctions evaders. Some of the cases in this report document sophisticated procurement networks with direct ties to the Russian state (Cases 3, 5, 6), while others involve opportunistic amateurs seeking to profit financially in a turbulent market (Cases 2, 4, 7).[52] The commodities involved are also diverse. Some cases primarily involve financial sanctions evasion (Cases 8, 9) or dual-use items regulated by the EAR (Cases 4, 7, 10), while others center on military-grade goods or technologies (Cases 3 & 6).

As Russia's war of aggression against Ukraine enters its 20th month, the focus of U.S. sanctions and related enforcement has increasingly identified military export evasion and illicit high-technology transfer as critical to the Russian war machine. Russia's effort to rearm and sustain its military campaign also appears focused on supply from states that have historically been

[51] David Gauthier-Villars, Steve Stecklow, John Shiffman, "Special Report – How Military Technology Reaches Russia in Breach of U.S. Export Controls," Reuters, April 29, 2022, available at https://www.reuters.com/article/us-ukraine-crisis-russia-sanctions-idAFKCN2ML19M, accessed on August 30, 2023; "Order Relating to Silicon Space Technology Corporation d/b/a Vorago Technologies, Inc.," September 28, 2021

[52] Patsulya and Besedin used the wealth accrued from their illicit activity to purchase a luxury BMW 740i sedan and a Sea Ray Sundancer cruiser. (p. 2)

recipients of Russian technology – Iran and North Korea – and from suppliers in China.[53] These trends will likely yield additional guidance and new red flags as methods of evasion become more sophisticated, and as export enforcement cases continue to be battles in an ongoing campaign to make Russian procurement in support of its war effort slower, more complicated, and costlier.

The United States is not the only country using the concept of "red flags" as a resource for exporters and to publicize its effort to counter Russian aggression more generally. A number of countries have published their own lists of risk indicators of Russia-related sanctions evasion, including "frontier states" Estonia, Latvia, Lithuania, Finland, and Poland, as well as Australia, Canada, the United Kingdom, and the European Union.[54] New cooperative export control and enforcement mechanisms have also emerged to counter this threat, including the 39-member Global Export Control Coalition (GECC) and the expansion of the Five Eyes partnership to encompass export control coordination.[55]

---

[53] "Kim Jong-un and Putin Plan to Meet in Russia to Discuss Weapons," The New York Times, September 4, 2023, available at https://www.nytimes.com/2023/09/04/us/politics/putin-kim-meeting-russia-north-korea-weapons.html.

[54] "Practical Guidance for Economic Operators to Detect and Prevent Circumvention of Sanctions Has Been Published," Ministry of Foreign Affairs of the Republic of Lithuania World Wide Website, July 17, 2023, available at https://urm.lt/default/en/news/practical-guidance-for-economic-operators-to-detect-and-prevent-circumvention-of-sanctions-has-been-published; "European Commission Guidance for EU Operators: Implementing Enhanced Due Diligence to Shield Against Russia Sanctions Circumvention," European Union, 2023, available at https://finance.ec.europa.eu/system/files/2023-09/230905-guidance-eu-operators-russia-sanctions-circumvention_en.pdf; "Red Alert - Financial Sanctions Evasion Typologies: Russian Elites and Enablers," Office of Financial Sanctions Implementation, HM Treasury, July 2022, available at https://database.riskreport.org/sites/default/files/2022-07/uk-red-alert-financial-sanctions-evasions-russia-typologies-07122022.pdf; "Special Bulletin on Russia-Linked Money Laundering Activities," Financial Transactions and Reports Analysis Centre of Canada, May 2023, available at https://fintrac-canafe.canada.ca/intel/bulletins/rlml-eng.pdf; "Advisory to the Australian Exports Sector on Russian Evasion – Third Country Transhipment Hubs, Shell Companies and End Users," Department of Foreign Affairs and Trade, available at https://www.dfat.gov.au/sites/default/files/advisory-australian-export-sector-russian-sanctions-evasionithird-country-transhipment-hubs-shell-companies-end-users.pdf.

[55] "Five Eyes Partners Agree to Formalize Cooperation on Export Control Enforcement," BIS, June 28, 2023, available at https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3294-2023-06-28-bis-press-release-five-eyes-export-enforcement-coordination/file; "Exporting Commercial Goods: Guidance for Industry and Academia," BIS, September 26, 2023.

A more robust framework for allied export control cooperation is needed, particularly to respond to strategic competition with Russia and China.[56] The United States has increasingly focused on preventing high-technology transfers to those countries and on rallying its allies and trading partners to do the same. The current emphasis on red flags previews what lies ahead by signaling both the critical importance of export controls for this next phase of great-power competition and a renewed focus on enforcement and compliance in both the public and private sectors.

[56] Ian Stewart, "Export Controls in an Era of Strategic Competition: Implications for the Existing Landscape and the Need for a New Multilateral Trade Review Regime," Strategic Trade Review, Vol. 9, Issue 10, Winter/Spring 2023, available at https://strategictraderesearch.org/wp-content/uploads/2023/02/Ian-Stewart-Export-Controls.pdf; Christopher A. Casey, "Export Controls—International Coordination: Issues for Congress," Congressional Research Service, September 8, 2023, available at https://crsreports.congress.gov/product/pdf/R/R47684.

## Appendix of U.S. Export Enforcement Cases

**Case 1**: In October 2022, Yury Orekhov and four other Russian nationals were indicted for exporting advanced semiconductors and microprocessors to Russia using falsified documentation and a German front company called Nord-Deutsche Industrieanlagenbau GmbH (NDA GmbH).[57] End use statements filed by the conspirators often claimed that the exports were for use in Malaysia, or by ROSCOSMOS or other Russian space program entities. Two Spanish oil brokers were also indicted for a related scheme which used NDA GmbH to smuggle Venezuelan oil to Russia and China. Payments for the illicit transactions were facilitated using cryptocurrency, bulk cash drops, and banks in less-regulated jurisdictions.

**Case 2**: In October 2022, Estonian national Andrey Shevlyakov was indicted for illicitly procuring U.S.-origin microelectronics and high-tech products on behalf of the Russian government and military via a series of Estonian shell companies.[58] Shevlyakov also attempted to acquire computer hacking software (Metalsploit Pro) for a Russian client, and organized frequent smuggling trips across the Estonian-Russian border to deliver goods.

**Case 3**: In December 2022, Russian nationals Yevgeniy Grinin, Aleksey Ippolitov, Boris Livshits, Svetlana Skovortsova, and Vadim Konoshchenok, and U.S. nationals Alexey Brayman and Vadim Yermolenko, were indicted for illicitly procuring military-grade and dual-use technologies, and sniper ammunition from the United States to Russia's defense sector.[59] They were operators in a larger proliferation operation described by the U.S. Treasury Department's Office of Foreign

---

[57] "Justice Department Announces Charges and Arrests in Two Cases Involving Export Violation Schemes to Aid Russian Military," Press Release, U.S. Department of Justice, October 19, 2023, available at https://www.justice.gov/opa/pr/justice-department-announces-charges-and-arrests-two-cases-involving-export-violation-schemes; "United States of America against Yury Orekhov…" Indictment, 22-cr-00434, September 26, 2022, available at https://www.justice.gov/usao-edny/press-release/file/1545431/download.

[58] "Estonian National Charged with Helping Russian Military Acquire U.S. Electronics, Including Radar Components; Sought-Computer Hacking Software," Press Release U.S. Department of Justice, April 5, 2023, available at https://www.justice.gov/usao-edny/pr/estonian-national-charged-helping-russian-military-acquire-us-electronics-including; "United States of America against Andrey Shevlyakov," Indictment, 22-cr-00490, October 27, 2022, available at https://www.justice.gov/d9/2023-04/indictment_22cr490.pdf.

[59] "Russian Military and Intelligence Agencies Procurement Network Indicted in Brooklyn Federal Court," Press Release, U.S. Department of Justice, December 13, 2022, available at https://www.justice.gov/opa/pr/russian-military-and-intelligence-agencies-procurement-network-indicted-brooklyn-federal; "United States of America against Yevgeniy Grinin…" Superseding Indictment, 22-cr-409, December 5, 2023, available at https://www.justice.gov/usao-edny/press-release/file/1557531/download.

Assets Control (OFAC) as the "Serniya Network."[60] Ippolitov received requests from Russian end users and relayed them to Grinin and Skvortsova, who directed Livshits to procure the items from U.S. companies via a series of shell companies in New York. Konoshchenok would physically smuggle items across the Estonia-Russia border.

**Case 4**: In March 2023, American nationals Cyril Gregory Buyanovsky and Douglas Robertson were indicted for exporting avionics equipment to Russian buyers through Buyanovsky's company, Kanrus Trading Inc.[61] Both men concealed the transactions by falsifying the true end users, value, and destinations of the goods, and by transshipping them through other countries.

**Case 5**: In February 2023, Russian national Ilya Balakaev was indicted for conspiring with the Russian Federal Security Service (FSB) to export surveillance equipment from the United States to Russia on behalf of Russia.[62] The equipment in question, spectrum analyzer and signal generators, are used to detect hidden surveillance devices and transmit secret communications. Balakaev also conspired with a North Korean official to procure hazardous gas detectors and corresponding software for North Korea.

**Case 6**: In May 2023, Greek national Nikoloas Bogonikolos was indicted for smuggling U.S. military and dual-use technologies to Russian intelligence operatives while operating as a defense contractor for NATO.[63] Bogonikolos operated the Aratos Group, a network of military

---

[60] Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," March 31, 2022.

[61] "Two U.S. Citizens Arrested for Illegally Exporting Technology to Russia," Press Release, U.S. Department of Justice, March 2, 2023, available at https://www.justice.gov/opa/pr/two-us-citizens-arrested-illegally-exporting-technology-russia; "United States of America v. Cyril Gregory Buyanovsky and Douglas Edward Robertson," Indictment, 23-cr-20010, March 1, 2023, available at https://www.justice.gov/d9/press-releases/attachments/2023/03/02/kanrus_unsealed_indictment_3_0.pdf.

[62] "Task Force KleptoCapture Unseals Two Cases Charging Evasion of Russian Economic Countermeasures," Press Release, U.S. Department of Justice, February 24, 2023, available at https://www.justice.gov/opa/pr/task-force-kleptocapture-unseals-two-cases-charging-evasion-russian-economic-countermeasures; "United States of America against Ilya Balakaev," Indictment, 23-cr-00079, February 21, 2023, available at https://www.justice.gov/d9/press-releases/attachments/2023/02/24/us_v._balakaev_indictment_0.pdf.

[63] "Founder and President of European Defense Conglomerate Charged with Helping the Russian Military Evade U.S. Sanctions and Export Controls," Press Release, U.S. Department of Commerce, May 16, 2023, available at https://www.justice.gov/usao-edny/pr/founder-and-president-european-defense-conglomerate-charged-helping-russian-military; "United States of America against Nikolaos Bogonikolos," Complaint, 23-mj-412, May 2, 2023, available https://www.justice.gov/opa/press-release/file/1583866/download.

and technology companies in the Netherlands and Greece. The equipment he purchased included advanced electronics, tactical military antennas, quantum computing technology, and sophisticated lasers. His Russian contacts were part of the Serniya Network.

**Case 7**: In May 2023, Russian nationals Oleg Sergeyevich Patsulya and Vasilii Sergeyevich Besedin were indicted for exporting aircraft parts and components to Russian airlines using their Florida-based company MIC P&I, LLC.[64] The two operators took requests from Russian airlines, then attempted to procure parts from U.S. aircraft parts suppliers by lying about the identity of the customers and the destination of the goods.

**Case 8**: In September 2022, U.K. national Graham Bonham-Carter was indicted for violating sanctions imposed on Russian Oligarch Oleg Vladimirovich Deripaska in 2018.[65] Bonham-Carter committed wire fraud to fund Deripaska's U.S. properties and attempt to expatriate the oligarch's artwork from an auction house in New York City.

**Case 9**: In November 2022, Russian-Swiss national Vladislav Osipov and U.K. national Richard Masters were indicted for sanctions evasion and money laundering in the operation of sanctioned Russian Oligarch Viktor Vekselberg's yacht *Tango*.[66] Masters ran a yacht management company in Palma de Mallorca, Spain which was contracted to oversee *Tango* for

---

[64] "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force," Press Release, U.S. Department of Commerce, May 16, 2023, available at https://www.justice.gov/opa/pr/justice-department-announces-five-cases-part-recently-launched-disruptive-technology-strike; "United States of America v. Oleg Sergeyevich Patsulya and Vasilii Sergeyevich Besedin," Complaint, 23-mj-03233, May 12, 2023, available at https://www.justice.gov/opa/press-release/file/1583871/download.

[65] "U.K. Businessman Graham Bonham-Carter Indicted for Sanctions Evasion Benefitting Russian Oligarch Oleg Vladimirovich Deripaska," Press Release, U.S. Department of Justice, October 11, 2023, available at https://www.justice.gov/opa/pr/uk-businessman-graham-bonham-carter-indicted-sanctions-evasion-benefitting-russian-oligarch; "United States of America v. Graham Bonham-Carter," Indictment, 22-cr-00503, October 11, 2022, available at https://www.justice.gov/d9/press-releases/attachments/2022/10/11/u.s._v._bonham-carter_indictment.pdf.

[66] "Arrest and Criminal Charges Announced Against British and Russian Businessmen for Facilitating Sanctions Evasion of Russian Oligarch's $90 Million Yacht," Press Release, U.S. Department of Justice, January 20, 2023, available at https://www.justice.gov/opa/pr/arrest-and-criminal-charges-announced-against-british-and-russian-businessmen-facilitating; "United States of America v. Vladislav Osipov," Indictment, 22-cr-00369, November 15, 2022, available at https://www.justice.gov/opa/press-release/file/1563256/download; "United States of America v. Richard masters," Indictment, 22-cr-00368, November 15, 2022, available at https://www.justice.gov/opa/press-release/file/1563251/download.

Vekselberg. Osipov was a senior employee of Vekselberg and the attorney-in-fact for the British Virgin Islands-based company listed as *Tango*'s owner.

**Case 10**: In September 2022, Latvian nationals Eriks Mamonovs and Vadims Ananics, and Ukrainian national Stanislav Romanyuk, among others, were indicted for conspiring to smuggle a jig grinder from Connecticut to Russia via Latvia and Estonia.[67] A jig grinder, because of its potential application to nuclear and military programs, requires a license for export or re-export to Russia.

[67] "European Nationals and Entities Indicted on Charges of Violating U.S. Laws for Their Attempt to Export a Dual-Use High-Precision Jig Grinder to Russia," Press Release, U.S. Department of Justice, October 19, 2022, available at https://www.justice.gov/usao-ct/pr/european-nationals-and-entities-indicted-charges-violating-us-laws-their-attempt-export; "United States of America v. Marat Mustafaev…" Indictment, 22-cr-00110, July 7, 2022, available at https://www.wisconsinproject.org/wp-content/uploads/2023/10/Romanyuk-Indictment-322cr00110.pdf.

## About the Author

Paul Esau is a 2023 Herbert Scoville Jr. Peace Fellow at the Wisconsin Project. He contributes research to the Risk Report database with a focus on sanctions, export controls, and export enforcement cases. Before joining the organization, he earned a PhD in History from Wilfrid Laurier University in Ontario, Canada. His dissertation explored Canadian military export policy during the Cold War.

## About the Wisconsin Project

The Wisconsin Project on Nuclear Arms Control is a non-profit, non-partisan organization based in Washington D.C. that conducts research, advocacy, and public education designed to inhibit the spread of nuclear, chemical, and biological weapons and the missiles to deliver them. The organization was founded in 1986 by Gary Milhollin, in cooperation with the University of Wisconsin.

The Wisconsin Project's mission is to reduce the risk that exports will accelerate the proliferation of weapons of mass destruction. The Project helps governments comply with the export restrictions in international agreements and helps them ensure that their national controls on strategic goods are enforced. The Project also publicizes clandestine transactions in these goods and draws attention to weaknesses in trade agreements and national laws. Through its research, testimony, and publications, the Project has influenced the export policies of major supplier countries.