KSE | Institute

Sanctions Circumvention: Export Control Effectiveness through Private Sector Compliance

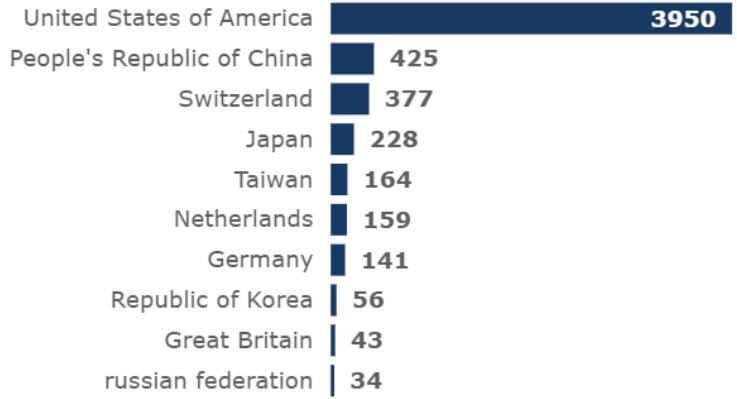
Pavlo Shkurenko
Sanctions and Compliance Advisor

June 9, 2026

Foreign Components in Russian Weapons

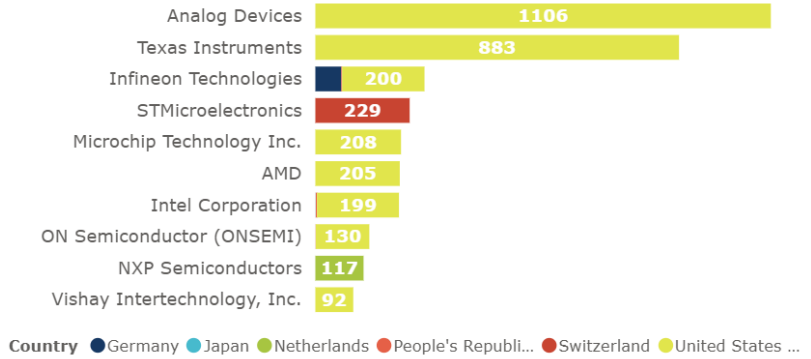
- Components from sanctions coalition companies are **routinely found in Russian weapons**.
- **US-based companies** account for ~68%, led by **Analog Devices** and **Texas Instruments**.
- **Switzerland, the Netherlands, and Germany** rank highest among European countries.
- Sweden: 7 components (Axis video encoders, RIFA film capacitors, others)

Components by country (out of ~5,800)



Source: Ukrainian defense intelligence service (GUR), KSE Institute

Components by company (out of ~5,800)

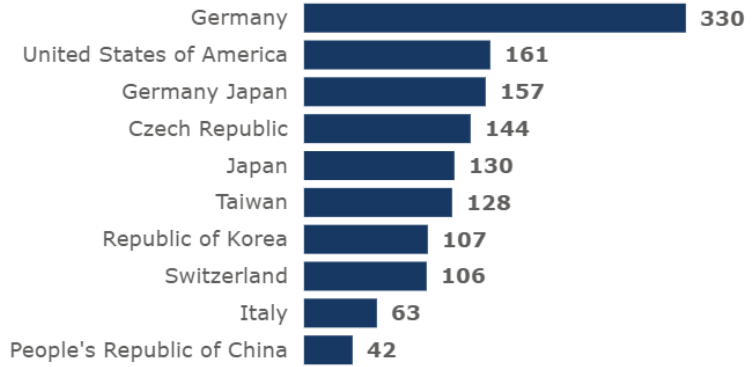


Source: Ukrainian defense intelligence service (GUR), KSE Institute

Foreign Machinery in Russian Military Production

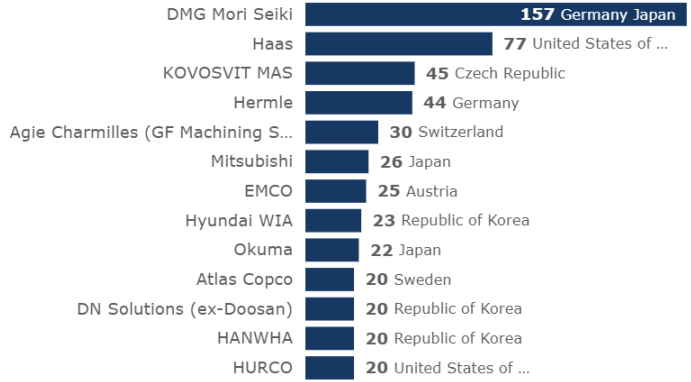
- CNC tools from sanctions coalition-based companies **plays a critical for the Russian military industry**.
- **Germany, Japan, US, and Czech Republic** top the list, followed by Switzerland, Taiwan, and South Korea.
- Japan's **DMG Mori Seiki accounts for more than 10%** of all identified equipment alone (157 machines).
- **Sweden**: 43 pieces of equipment from 9 manufacturers
- **Atlas Copco**'s screw compressors are used at Smolensk aviation plant in production of Kh-59 missiles and UAVs
- **Hexagon AB** coordinate measuring machines are used in production of engines for cruise missiles, Su aircrafts, universal gliding and correction modules for aircraft bombs (UMPK)

Equipment by country (out of ~1,500)



Source: Ukrainian defense intelligence service (GUR), KSE Institute

Equipment by company (out of ~1,500)

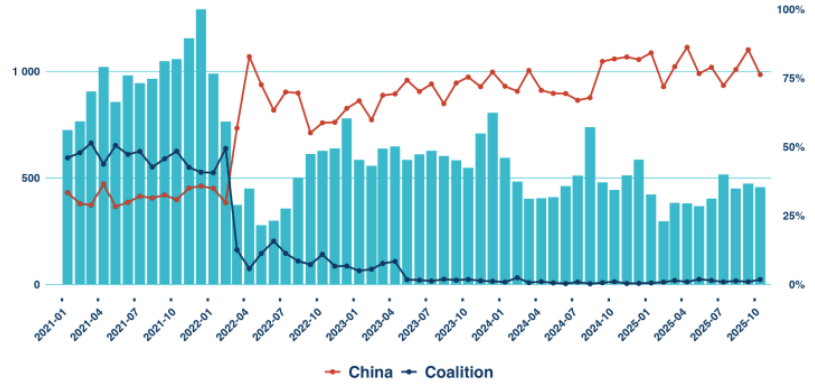


Source: Ukrainian defense intelligence service (GUR), KSE Institute

Russian Access to Export-Controlled Technology

- Russia continues to be able to **import significant quantities of export-controlled goods** that are critical for its military production.
- **China has become the most important supplier** (~75%) of such goods to Russia following the imposition of export controls.
- Publicly-available trade data do **not allow to distinguish** between goods made in China by Chinese companies and goods from Western producers transshipped via China.
- Data point to **significant mark-ups paid by Russia** due to the cost of establishing and maintaining circumvention networks and Chinese exploitation of Russia's situation.
- **<u>Sanctions work but could be more effective.</u>**

Reported Exports of CHP to Russia, $ million



Source: UN Comtrade, national authorities, KSE Institute

Export Controls: Circumvention Channels

Substitution

Russia acquires war-critical goods from **producers located outside** of the countries that imposed export controls.

~67%

of total Russian CHP imports (2023: 55%)

Transshipment

Russia acquires war-critical goods manufactured in sanctions coalition countries **via third-country intermediaries**.

~16%

of total Russian CHP imports (2023: 21%)

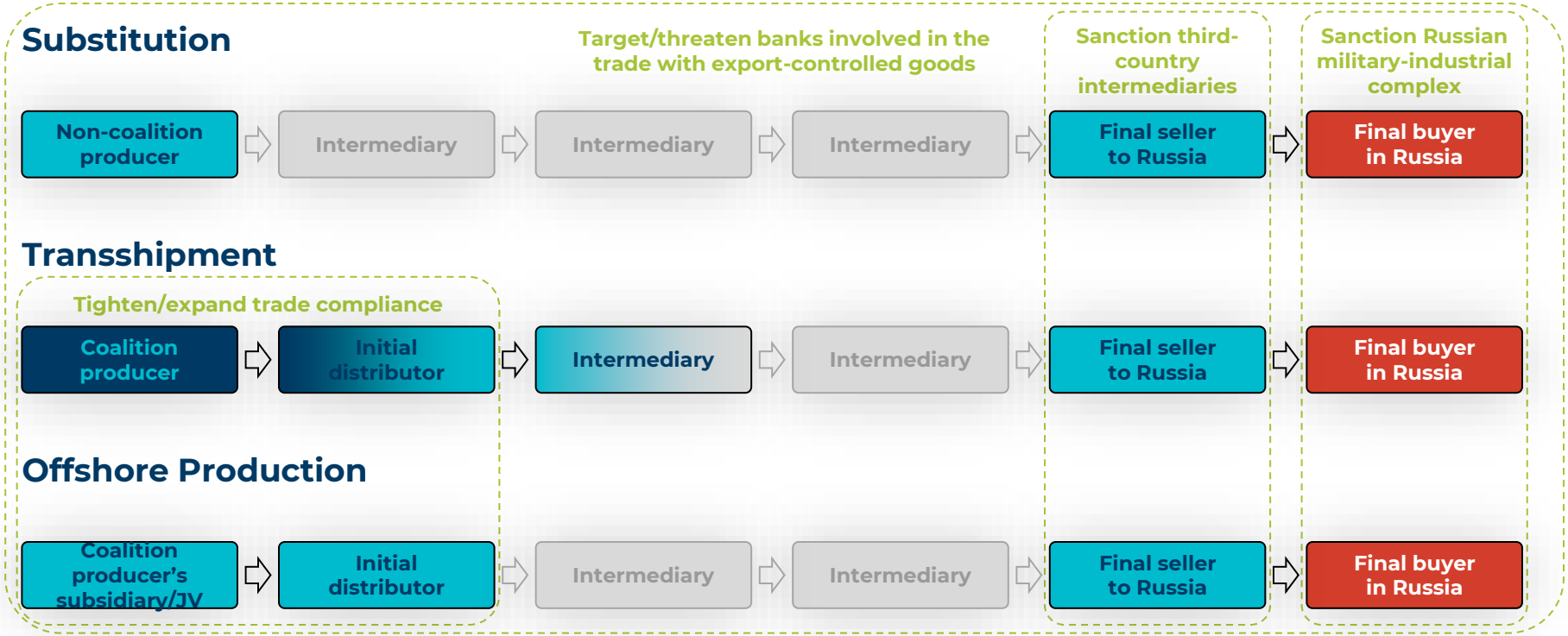
Offshore Production

Russia acquires war-critical goods from sanctions coalition-based companies that are **manufactured offshore**.

~13%

of total Russian CHP imports (2023: 18%)

Export Controls: Legal Loopholes and Next Steps



Role of Businesses

The Global Context: Sanctions and export regulations are now permanent fixtures in international business due to escalating geopolitical risks.

Vital Interest: Compliance is not just a legal requirement but essential for mitigating legal, reputational, and ethical risks.

Tone at the Top: Leadership commitment is the cornerstone of a robust compliance strategy

Best Practices in Due Diligence

- Understand the requirements
  - a **dedicated person** to monitor legal updates and brief management regularly.
  - Depending on a sanctions program, the restrictions may apply to *transactions, business partners, products, trades and holdings of securities, including derivatives, and other more complex criteria*, such as relationship with governments or a percentage of revenue that an entity received from Russia.
- Set your policies
  - At minimum equal to regulation
  - Tiered approach depending on country of sale
  - Introduce 1) preventive, 2) transactional, and 3) post-fact controls
- Classify your products
  - Identify potential exposure by categorizing materials and technologies, often defined by CN codes.
  - Implement a systematic process in your ERP to flag dual-use or regulated items. Pay special attention to automotive components, communications, navigation, sensors, semiconductors, and electronic equipment, **even if the products don't have an explicit dual-use designation**.

Best Practices in Due Diligence

- Screen your partners
  - Mitigate risks from customers and distributors reselling to Russia by including **re-export, end-use, and end-user** clauses in agreements.
  - Emphasize a zero-tolerance policy for sanctions evasion.
  - Use screening solutions that integrate with your ERP for real-time checks against sanction lists, ensuring a hard stop (as opposed to system warning) for any matches.
  - Features such as approximate search, search by address, as well as translation/transliteration of company names.
  - If screening manually, ensure robust audit trail, and flag companies with shared addresses or partial ownership with entities of concern.
- Address conflict of interest
  - **Separate the sales and due diligence roles** to prevent conflicts of interest.
  - If not possible, implement a four-eyes principle for reviewing the due diligence and screening documentation.
  - The **legal officer** should oversee trade compliance in regional branches. Pay special attention to hubs for sanction circumvention, such as China, Hong Kong, Turkey, UAE, and Taiwan.

Best Practices in Due Diligence

- Train your team
  - Educate your team on critical components and battlefield goods, common red flags, and sanction evasion practices.
  - Stress the leadership's complete dedication to sanctions compliance.
  - A weak management tone could undermine the entire compliance structure, leading employees to prioritize paperwork over protecting the business.
  - Deliberately avoiding information, failure to resolve a red flag or an escalated concern within the company may be seen as **aggravating circumstances** by the export controls investigators.

Building Up the Compliance Program

1. **Contractual Language**: Incorporate export controls compliance clauses into contracts and secure written certifications of end-use and end-user. Audit and follow-up, ensure **clear and predictable outcomes** to counterparties.
2. **Internal Training**: Conduct **regular and simple** training sessions on red flags to foster a culture of vigilance and encourage reporting of concerns.
3. **Partner Screening**: Use automated solutions or manual searches for business partner screening. Avoid conflicts of interest and maintain a clear audit trail.
4. **Building Relationships**: Meet with counterparties in person and develop market knowledge. Report legitimate compliance concerns **about competitors** to level the playing field.

While automation and data tools can improve **efficiency**, the educated judgment and case-by-case analysis by your **team** are essential to prevent major control failures.

Red Flags and Risk Mitigation

Documentation

- Sales supporting documents (invoices, letters of credit) do not list **the actual end-user**.
- A customer or re-seller **refuses to disclose** details to banks, shippers, or third parties.
- Customer is **evasive** and especially **unclear** about whether the purchased product is for domestic use, for export, or for reexport.
- **Bank account number** has a country code different from the customer's country.
- Payment details **change last-minute** to exclude the country or entity of concern.
- After being declined the sale, the customer or re-seller **comes back as another entity**.

Shipping

- A freight forwarding firm, or virtual company or secretary service provider, is listed as the product's final destination.
- Atypical or illogical shipping routes to reach a destination, e.g. shipping through Hong Kong or Dubai where a more direct route is available.
- Packaging is inconsistent with the stated method of shipment or destination.

Red Flags and Risk Mitigation

Business model

- Customer has little or **no business background**, or a recently registered company.
- **Ownership structure** is not transparent or atypical; minimal share capital.
- Product or software sold is **not in line with the customer's business**.
- Customer is **overpaying** for a product and/or pushes for urgent delivery.
- Customer is willing to **pay cash for a very expensive item** when the terms of sale would normally call for financing.
- If the product is being paid for or received by a **different party**, does their relationship make sense?
- Customer is **unfamiliar with the product's performance characteristics** but still wants the product.
- Product is not in line with the **technological level of the country** of the end-user, e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- Customer claims to be a manufacturer but has **no apparent production facilities** (e.g. it is extremely rare to have manufacturing in Hong Kong).
- Search result by alleged address of production facilities look like an office building.
- Routine installation, training, or maintenance **services are declined** by the customer.

Red Flags and Risk Mitigation

Communications and web presence

- Phone numbers' country codes don't match the destination country.
- Map search by address returns locations at or nearby **military facilities**.
- Entity has no web presence and/or **no corporate domain** for email accounts (using gmail, hotmail, qq, etc instead).
- English and Chinese language versions of the company website are vastly different in content.
- No company **website**, or a website only in Russian.
- Website of an alleged Chinese company does not have the MIIT ICP Recording Number on the page.

Enforcement Case Examples – Corporate Liability

- **Alfa Laval** (Denmark): Pleaded guilty to exporting centrifuge spare parts to its Russian sister company, resulting in a fine.
  - Implementation of automated ERP "hard stops" and a four-eyes principle would have flagged the sanctioned destination regardless of the "internal" nature of the transaction.

- **Dutch FIU Case:** A company that previously sold to Russia suddenly "switched" all business to intermediaries in circumvention countries
  - Market knowledge and relationship building would have required an investigation into why long-standing Russian clients were suddenly replaced by shell companies with Russian shareholders. Monitoring historical trade patterns is a core best practice.

Enforcement Case Examples – Corporate Liability

- **Alus Grupp OÜ** (Estonia): A freight forwarder convicted for aiding the transport of resonance testing machines to Russia via Kazakhstan and the UAE; the company was fined €100,000.
- **Marine Technics Baltia OÜ** (Estonia): Convicted of exporting gas generators and propulsion systems to military end-users like Kalashnikov Concern using false end-user certificates for Turkey.
  - Hub-Specific Vigilance: Applying extra scrutiny to known circumvention hubs.
  - Verification of End-Use Certificates: Marine Technics used false certificates for Turkey. Best practices mandate securing written certifications and verifying them through independent market knowledge.
  - Illogical Routes: Spotting "atypical or illogical shipping routes" (e.g., shipping through Dubai when a direct route is available) is a primary red flag.

Enforcement Case Examples – Individual Liability

- **Germany**: Arrests were made in 2026 involving 16,000 deliveries to 24 different Russian defense companies valued at €30 million.
- **Finland**: Two individuals received suspended jail sentences for exporting drones, processors, and electronic equipment valued at €140,000.
- **Belgium**: Prosecution of individuals for exporting machinery and materials (iron, alumina) for use by the Russian military

Fostering a Culture of Vigilance

Leadership's commitment: set the tone at the top, and reiterate frequently

Proactive compliance and a robust internal control framework

Education: red flags and evasion patterns

Final Goal: Protect the business legally and reputationally and contribute to the global peace and security.

Thank you!

Contacts:

Pavlo Shkurenko
Sanctions and Compliance Advisor,
Research Lead on Russian Military-Industrial Complex
pshkurenko@kse.org.ua