# Working Group Paper #16

# Challenges of Export Controls Enforcement

## How Russia Continues to Import Components for Its Military Production

By Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova,
Nataliia Shapoval, Anna Vlasyuk, and Vladyslav Vlasiuk[1]

The International Working Group on Russian Sanctions

January 11, 2024

https://fsi.stanford.edu/working-group-sanctions

[1] Data analysis was performed and policy recommendations were developed by Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, Anna Vlasyuk, and Vladyslav Vlasiuk. The KSE Institute Sanctions Team also includes Borys Dodonov, Oleksiy Gribanovskiy, Vira Ivanchuk, Antatoliy Kravtsev, Yuliia Pavytska, and Dmitro Pokryshka. We thank Thomas Andrukonis, Emily Kilcrease, Michael McFaul, Tymofiy Mylovanov, Jacob Nell, Steven Wilcox, as well as all members of the Yermak-McFaul International Working Group on Russian Sanctions for their contributions and comments.

The International Working Group on Russian Sanctions aims to provide expertise and experience to governments and companies around the world by assisting with the formulation of sanctions proposals that will increase the cost to Russia of invading Ukraine and that will support democratic Ukraine in the defense of its territorial integrity and national sovereignty. Our working group is comprised of independent experts from many countries. We coordinate and consult with the Government of Ukraine and those governments imposing sanctions. This consultation process helps to inform our views, but our members express independently held opinions and do not take direction from or act at the behest of the government of Ukraine or any other government, person or entity. All members of this working group participate in their individual capacity.

## Key Findings and Policy Recommendations

**Our key findings from the analysis are as follows:**

- **Continued Russian access to military inputs.** The analysis shows that, while export controls have had some effect on trade flows, Russia continues to be able to import large amounts of goods needed for military production. Since the imposition of restrictions, supply chains have adapted and most of the items in question now reach Russia via intermediaries in third countries, including China. Almost half of the imports in the first ten months of 2023 consisted of goods that were produced on behalf of companies from coalition countries, indicating major enforcement challenges.
- **Export controls remain a powerful instrument.** Russia has not been able to find substitutes for many products from coalition countries, in particular advanced electronics, as the continued involvement of these producers shows. This means that, fundamentally, the potential of export controls to significantly curtail Russia's ability to wage its war of aggression on Ukraine remains intact. However, major changes to the current enforcement approach are needed to improve their effectiveness.

**Our key policy recommendations are as follows:**

- **Bolstering corporate responsibility.** Improved export controls enforcement will ultimately not be possible without buy-in from the private sector, especially coalition-based producers of goods needed for Russia's military industry. Any effective control of the supply chain has to begin with the initial sale of an item to a distributor as it becomes increasingly complicated to trace its physical whereabouts and impede any illicit activities post-sale. To create incentives for corporates to set up compliance procedures, enforcement agencies must demonstrate a willingness and ability to investigate the trade with controlled goods and impose meaningful fines in the case of export controls violations.
- **Closing export controls policy gaps.** Significant inconsistencies continue to exist within the Russia export controls regime, which hinder effective enforcement and allow for circumvention. Restrictions need to be harmonized across coalition jurisdictions—along with derogations and licensing procedures, criminalization of sanctions violations, and negligence provisions that outline procedures that companies are expected to follow. As many of the goods in question are produced on behalf of coalition-based companies in third countries, it is also important to ensure that export controls in all jurisdictions apply extraterritorially the way U.S. ones do under the Foreign Direct Product Rule.
- **Targeting third-country circumvention.** Coalition authorities need to address the role of third-country intermediaries in export controls circumvention schemes, including those in China, Turkey, and the UAE. They can do so by imposing sanctions on entities that have been found to facilitate export controls violations involving any companies or individuals from coalition countries. Should this turn out to be insufficient to inhibit illicit trades, authorities should consider broader steps such as quotas or bans with regard to specific goods and specific countries. Any coercive measures should be accompanied by outreach to public and private sectors in key third countries.
- **Strengthening institutions and cooperation.** Enforcement agencies in sanctions coalition countries are not adequately equipped to implement and enforce comprehensive export controls such as those imposed on Russia. This includes the United States, where such measures have a longer track record. The European Union is lacking unified enforcement structures altogether, as member states remain responsible for the implementation of restrictive measures, including those imposed on the EU level. Considering that export controls will be an important part of the economic statecraft toolbox for the foreseeable future, these weaknesses need to be addressed. Better multilateral cooperation is also key.

## EXECUTIVE SUMMARY

In the aftermath of Russia's full-scale invasion of Ukraine, a coalition of countries – including European Union member states, the United States, United Kingdom, Japan, South Korea, and others—imposed **unprecedented export controls** on the Russian Federation, including with regard to dual-use goods.[2] The objective is to deprive the aggressor of critical inputs such as high-tech electronics for its war effort and military industry. This is the first real test case of 21st century export controls—or, more broadly, technology sanctions—and as such holds a place of critical importance beyond the specific case of Russia's unjust war against Ukraine. Such measures are rightfully seen as a new frontier in economic statecraft, and key lessons can and must be learned for future applications.

Export controls, however, present **major enforcement challenges** due to the complexity of global supply chains, the fact that large economies such as China are not part of the sanctions coalition, and because of a lack of experience and institutional resources on the part of the coalition countries. Therefore, it is not surprising that Russia continues to be able to acquire large amounts of the inputs that it needs for its military production. In the first ten months of 2023, imports of what the U.S., EU, UK, and other partners of Ukraine have identified as priority battlefield goods reached $8.77 billion—only a 10% decline compared to the pre-sanctions period. For all items that we consider to be critical for Russia's military industry, they were even higher—$22.23 billion. In this report, we outline well-known issues, including third-country circumvention schemes, but focus in particular on the role of producers from export controls coalition countries whose products are manufactured abroad and make their way to Russia due to insufficient compliance efforts by the private sector. Almost half of all of Russia's imports of the goods in question in 2023 ultimately stem from producers from the coalition.

Fundamentally, our analysis shows that the issues identified in previous research continue to plague export controls implementation and enforcement.[3] In addition, many of the producers from coalition countries whose products are repeatedly found in Russian weapons on the battlefield continue to trade with Russia via third-country intermediaries. **Improvements are urgently needed**—including through better cooperation between authorities and the private sector—not only to ensure the effectiveness of the current sanctions regime but also to preserve its credibility in the medium and long term.[4] Dual-use goods export controls are a complex undertaking. But having embarked on this course of action, it is critical to make these measures work and send a clear message to others that may want to challenge a rules-based international order. Ukraine is now facing a second winter with concerted Russian missile and drone strikes on civilian infrastructure. And foreign components continue to be found in the weapons that hit Kyiv and other cities on a daily basis.[5]

We **urge policy makers to take action** to ensure that export controls stay ahead of Russian efforts to circumvent them. Measures need to consider distinct challenges that exist on various stages of the supply chain and require specific solutions. They should aim to (i) close policy gaps in the existing exports controls regime; (ii) strengthen government institutions tasked with its implementation and enforcement; (iii) incentivize and empower the private sector to step-up compliance; (iv) target circumvention schemes that allow Russia to import goods via third countries; and (v) improve multilateral cooperation in the field of export controls.

[2] The following jurisdictions have imposed export controls on Russia and are part of what we define as the "export controls coalition" for the purpose of this analysis: Australia, Canada, European Union, Japan, New Zealand, Norway, South Korea, Switzerland, Singapore, Taiwan, United Kingdom, and United States. For details on existing export controls, see Appendix 1.

[3] See "Russia's Military Capacity and the Role of Imported Components," International Working Group on Russian Sanctions & KSE Institute, and "Foreign Components in Russian Military Drones," International Working Group on Russian Sanctions & KSE Institute.

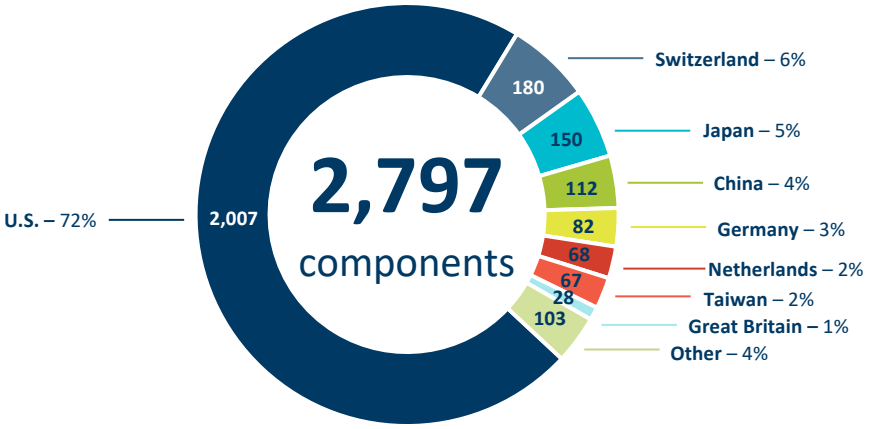
[4] See "Economic sanctions risk losing their bite as a US policy weapon," Elina Ribakova, Financial Times.

[5] See the NACP's (National Agency on Corruption Prevention, Ukraine) database on foreign components in Russia weapons here.

## I. Introduction: Why Export Controls Need to Be Improved

With Russia's brutal full-scale invasion now approaching its second anniversary, Ukrainians—civilians and soldiers alike—continue to endure the daily horrors of the war and occupation. Unprecedented export controls imposed on Russia were intended to substantially curtail the country's access to foreign components and its ability to produce advanced weapons systems. However, we are witnessing not only persistent offensive operations by the Russian military but also a second winter of concerted missile and drone strikes on civilian infrastructure, a reality which not be possible without the critical foreign components in those weapons. Ukraine's National Agency for Corruption Prevention (NACP) has documented close to 2,800 individual parts that have been found in Russian weapons on the battlefield so far—including in missiles, drones, armored vehicles, and other systems—with detailed information on the companies behind their production (see Figure 1).[6]

**Figure 1: Foreign components in Russian weapons by country of producer**



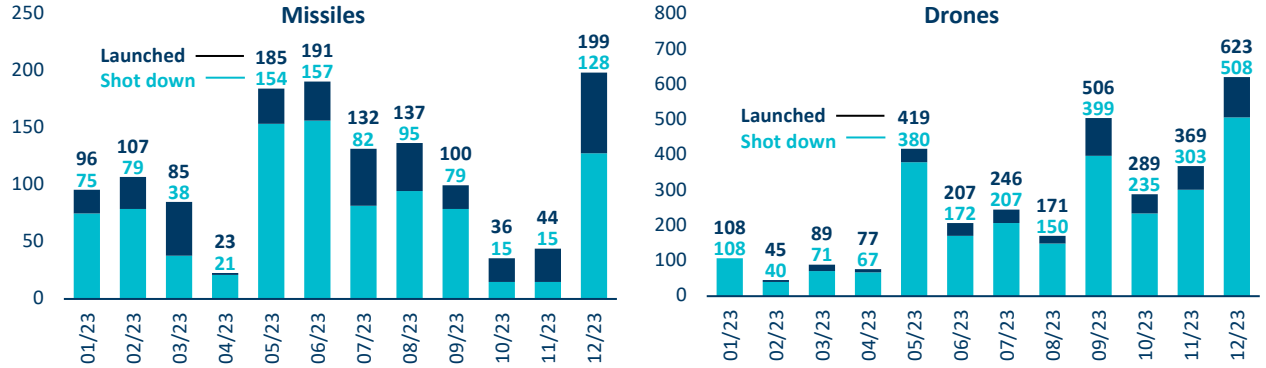

*Source: NACP, UA War Infographics, KSE Institute*

Russia continues to rely to a significant extent on foreign components for its military production. In fact, 95% of all parts found in Russian weapons on the battlefield were sourced from producers in coalition countries, with 72% accounted for by U.S.-based companies alone. These findings underscore the ongoing challenge to find viable substitutes from the Russian domestic market or its allies; components from China only make up 4% of the ~2,800 items identified in total. Thus, export controls remain a powerful tool to constrain the Russian war effort. However, their enforcement appears to be insufficient and steps need to be taken to enhance their effectiveness.

If anything, Russia's capacity to manufacture missiles and drones appears to have increased in 2023. Data from the Ukrainian military demonstrate how much drone attacks have increased throughout last year (see Figure 2) as Russia was able to localize the production of Iranian Shahed drones. According to estimates from the Ukrainian government, missile production capacities have also been expanded from ~50 units per month in 2022 to ~100 in mid-2023 and ~115 by the end of 2023. The dramatic increase in missile strikes in December is also a result of Russia's well-known strategy to build up stocks for attacks on civilian infrastructure during the winter. While Ukraine has been very successful in intercepting drones and missiles—83.8% and 70.3% were shot down, respectively—this puts a major strain on the country's air defenses. It also creates a Kafka-esq scenario in which Ukraine's allies have to provide more military assistance to Ukraine in order to defend it against weapons that Russia can only build because of its continued access to imported components that originate from Ukraine's allies.

[6] See the NACP's (National Agency on Corruption Prevention, Ukraine) database on foreign components in Russia weapons here.

**Figure 2: Russian missile and drone strikes on Ukraine in 2023**

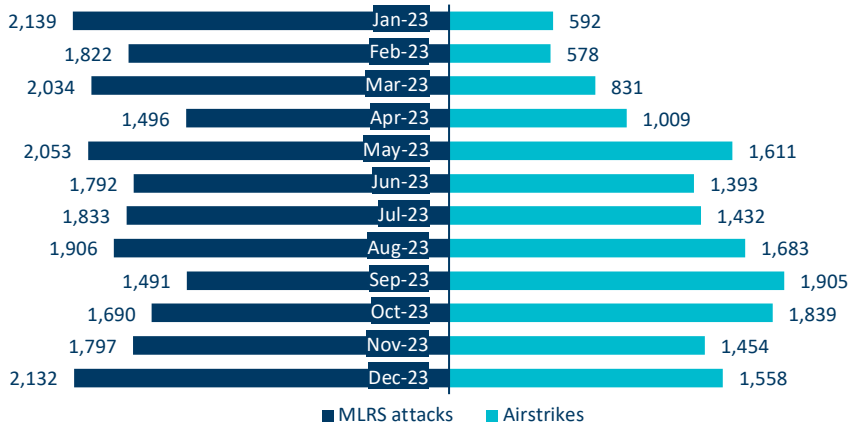



*Source: Air Force of Ukraine, KSE Institute*

Despite the expectation that sanctions on dual-use goods—introduced in response to the annexation of Crimea in 2014 and tightened considerably after the beginning of the full-scale invasion—would diminish the sophistication of Russia's military equipment, Ukrainian experts engaged in the dismantling of weapons from the battlefield suggest otherwise. Specifically, there is no clear evidence of meaningful substitution of advanced components from coalition countries with Russian or Chinese parts, which are presumably less advanced. These experts' observations indicate that changes primarily revolve around modernization efforts and incorporation of new features, rather than a fundamental shift in suppliers. This means that export controls have the potential to significantly curtail Russia's military production and ability to wage war on Ukraine.

Furthermore, investigations reveal that Russia is actively developing new capabilities in preparation for an extended conflict. Satellite imagery has shown the construction of new facilities dedicated to aircraft repair, missile production, drone assembly, and other military purposes.[7] For instance, aircraft plants in Kazan and Irkutsk have been expanded in recent months, which focus on Su-30 fighter jets—a pivotal aircraft type within the Russian air force. In addition, the Dubna machine building plant has seen construction, as has a facility in Kronstad, which plays a key role for missile production on behalf of the state-owned Tactical Missile Arms Cooperation. Notably, a significant portion of these construction projects commenced between 2018 and 2021, but there has been a noticeable acceleration in building activities after the February 2022 invasion.

**Figure 3: Russian airstrikes and MLRS attacks on Ukraine in 2023**




*Source: NACP, UA War Infographics, KSE Institute*

[7] See here.

This surge in construction suggests a strategic commitment to reinforcing military infrastructure, indicating a long-term perspective on the ongoing conflict. It has also contributed to an increasingly challenging situation on the battlefield, where Russia possesses the capacity to conduct large-scale operations and can effectively stop any counteroffensive by Ukraine (see Figure 3). At the same time, a global artillery shell deficit is forcing both sides to adapt their strategies. A noteworthy development is the rising use of First Person View (FPV) drones as an alternative to conventional weapons. Both Ukraine and Russia need to establish new production capacities as the nature of warfare constantly evolves—and Russia will likely need more foreign components going forward.

Amidst these concerning developments, it is important to acknowledge positive trends that have surfaced. First, recent issues plaguing Russia's civil aviation have shed light on supply chain challenge as far as spare parts are concerned, and similar constraints are potentially to be expected within the realm of military aviation.[8] Second, Russia is experiencing unparalleled losses across all categories of its military equipment. Even under the hypothetical scenario of an immediate cessation of military activities, it would take the country more than one year to restore missile capabilities, and considerably longer to replace destroyed armored vehicles. These developments underscore the magnitude of the setbacks that Russia has encountered and substantial time and resources that will be required for the rebuilding of its military in the aftermath of the war.

Moreover, Ukrainian intelligence services have indicated that they observe a discernible deceleration of the Russian military industry, echoing President Zelensky's remarks in his December 21, 2023, address.[9] While specific details regarding these developments are unavailable, especially with regard to individual weapons systems, this aligns with our findings regarding growing supply chain disruptions as far as foreign inputs are concerned. The future course of the war may be decided in 2024.[10] While Ukraine will require continued financial and military support from its allies in order to defeat Russian aggression, it is also critical that coalition countries finally make export controls more impactful. The trade with export-controlled goods clearly continues despite considerable media attention devoted to specific cases of foreign companies' components discovered in Russian weapons and the circumvention schemes that allow Russia to acquire critical inputs for its military industry.[11]

On the line is not only the freedom and security of the Ukrainian people, but the credibility of the sanctions regime. Export controls are rightfully seen as the new frontier in economic statecraft but, in the absence of robust enforcement, they risk losing their bite.[12] Ukraine's allies can ensure that the country possesses the technological superiority to win the war, but only if they get serious about constraining Russia.

[8] The number of civilian planes in the air has dropped by roughly two-thirds; see here.

[9] See here.

[10] See "Adaptation at the Front and the Big Picture in Ukraine," Michael Kofman and Ryan Evans, War on the Rocks.

[11] See "The shadowy network smuggling European microchips into Russia" Chris Cook and Max Seddon, FT; "Elektroniklieferungen deutscher Firmen landen offenbar bei russischen Rüstungskonzernen," Benjamin Bidder et al., Spiegel; "Wie ein deutscher Computerchip in russische Raketen gelangt," Konrad Schuller, FAZ; and "How U.S.-made chips are flowing into Russia," Nikkei.

[12] See "Economic sanctions risk losing their bite as a US policy weapon," Elina Ribakova, Financial Times.

## II. How Russia Continues to Import Components for Its Military Production

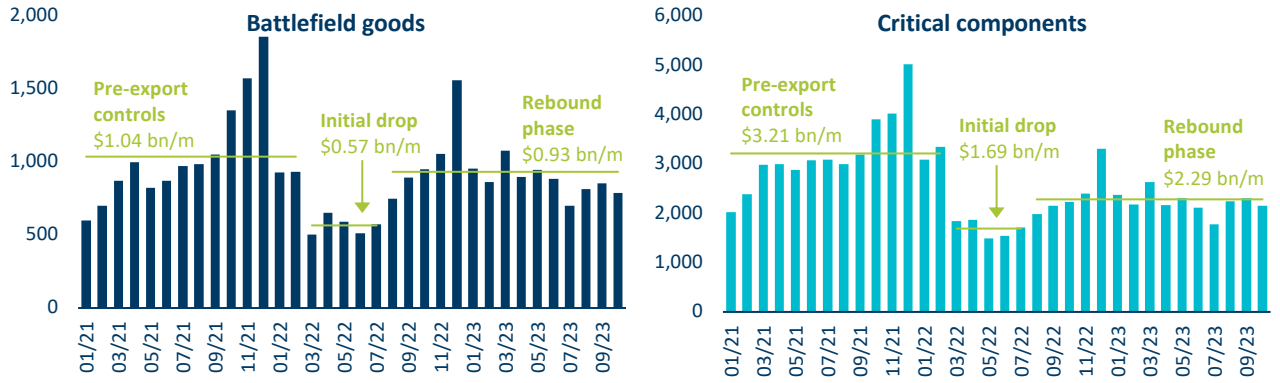
### *II.1. "Battlefield Goods" vs. "Critical Components"*

In our analysis, we look at two separate sets of goods that are important for Russia's military industry and war effort: (1) The European Union, United States, United Kingdom, and other coalition countries have identified a list of 45 (6-digit) Harmonized System (HS) codes that they consider of particular importance for export controls enforcement – the so-called **"common high-priority items" (a.k.a. "battlefield goods")**.[13] (2) We rely on our own definition of **"critical components"** – excluding some battlefield goods that are largely used for civilian purposes (e.g., smart phones), but going beyond in other areas where we think a wider focus is needed. This results in a list of 485 HS codes on the (more detailed) 10-digit level.[14] Our analysis of trade flows is based on a transaction-level dataset of Russian imports and aims to provide a comprehensive mapping of supply chains.[15]

### *II.2. Rebound in Imports of Foreign Components*

**Russian imports of battlefield goods have largely recovered from their sharp drop in the aftermath of the imposition of export controls, while those of critical components are lagging behind.** For both sets of goods, we observe a clear impact of export controls in mid-2022 (see Figure 4). However, when it comes to battlefield goods, Russia appears to have been able to rework supply chains, and monthly average imports of $932 million were only 10.0% lower in 2023 compared to the pre-sanctions period.[16] The situation is noticeably different for the broader set of critical components, where a monthly average of $2.29 billion in 2023 represents a 28.8% drop vs. before February 2022. Thus, export controls appear to show some results for certain goods.

**Figure 4: Russian imports of battlefield goods and critical components, in $ million**




*Source: KSE Institute*

- In the period before the full-scale invasion (January 2021-February 2022), Russia imported an average of $1.04 billion in battlefield goods per month and $3.21 billion in critical components. Numbers were particularly high in the fourth quarter of 2021—$1.59 billion and $4.31 billion per month, respectively—as Russia prepared for the war in anticipation of export controls being imposed.

[13] For the list of "Common High Priority Items" (as of September 2023), see here and Appendix 2.

[14] For the HS codes included in our list of "critical components," see Appendix 2.

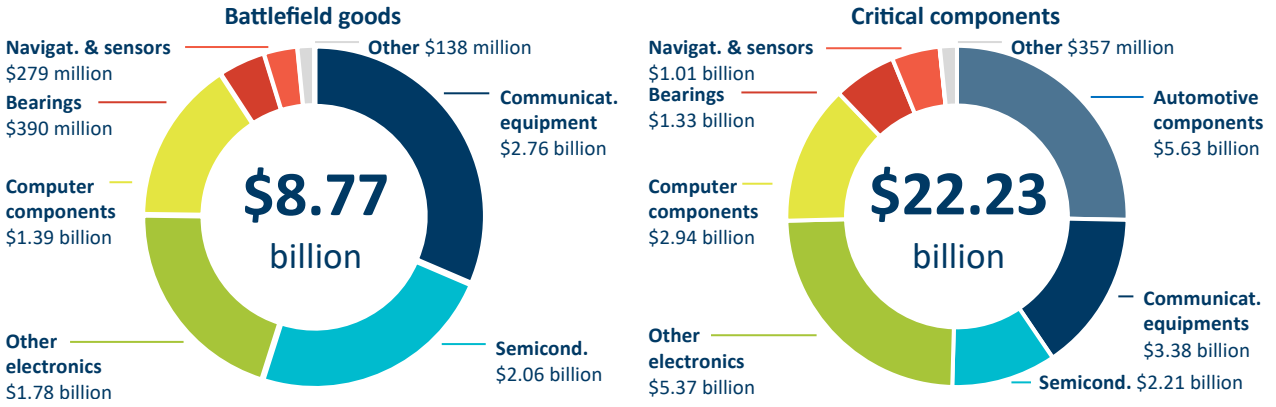
[15] We recognize that legitimate concerns exist with regard to Russian trade data. We undertake extensive efforts to validate the data used in our analysis by comparing numbers on different aggregation levels with other sources, including mirror trade data. Despite the existence of some discrepancies, we believe that the data can be relied upon. We will continue to conduct such efforts but urge readers to evaluate our findings in the context of these considerations. We also emphasize that our findings of trade of coalition-based entities with Russia does not necessarily represent export controls violations, since many exemptions and derogations from the regime exist. Finally, our findings likely understate the role of Central Asian countries in circumvention schemes as the data does not include all trade between Russia and members of the Eurasian Economic Union.

[16] For an analysis of volume and price effects, see "Decision to leave: Economic sanctions and intermediated trade," Maxim Chupilkin, Beata Javorcik, Aleksandra Peeva, and Alexander Plekhanov, EBRD (forthcoming).

- After the imposition of sanctions, Russian imports for both sets of goods dropped sharply—to a monthly average of $565 million for battlefield goods and $1.69 billion for critical components in March-July 2022. This represents declines of 45.5% and 47.4%, respectively, vs. the pre-sanctions period.
- In the second half of 2022, however, trade in these goods recovered as Russia was able to adapt supply chains. In August-December 2022, they came to $1.04 billion per month for battlefield goods (84.1% higher than during March-July) and $2.41 billion for critical components (42.8% higher).
- In January-October 2023, imports of battlefield goods came close to their pre-sanctions levels at $932 million per month—a decline of only 10.0%. For critical components, we observe noticeably different dynamics. Here, monthly average imports of $2.29 billion in 2023 represent a 28.8% decline.

**Russia imported battlefield goods worth $8.77 billion in January-October 2023, while imports of critical components reached $22.23 billion.** Specific findings with regard to the extent of the recovery aside, it is clear that Russia continues to be able to acquire large amounts of goods that we consider to be of particular importance for its military industry. This indicates that export controls enforcement is facing major challenges. It is also instructive to take a closer look at the composition of these imports (see Figure 5).[17]

**Figure 5: Composition of Russian imports in January-October 2023**




*Source: KSE Institute*

- With regard to battlefield goods, four categories of goods dominate: communications equipment ($2.76 billion in January-October 2023 or 31.4% of the total), semiconductors ($2.06 billion, 23.5%), other electronics ($1.78 billion, 20.3%), and computer parts ($1.37 billion, 15.6%).
- With regard to critical components, seven categories deserve particular attention: automotive parts ($5.63 billion or 25.3% of the total), other electronics ($5.37 billion, 24.2%), communications equipment ($3.38 billion, 15.2%), computer parts ($2.94 billion, 13.2%), semiconductors ($2.21 billion, 9.9%), bearings and transmission shafts ($1.33 billion, 6.0%), and navigation equipment ($1.01 billion, 4.6%).

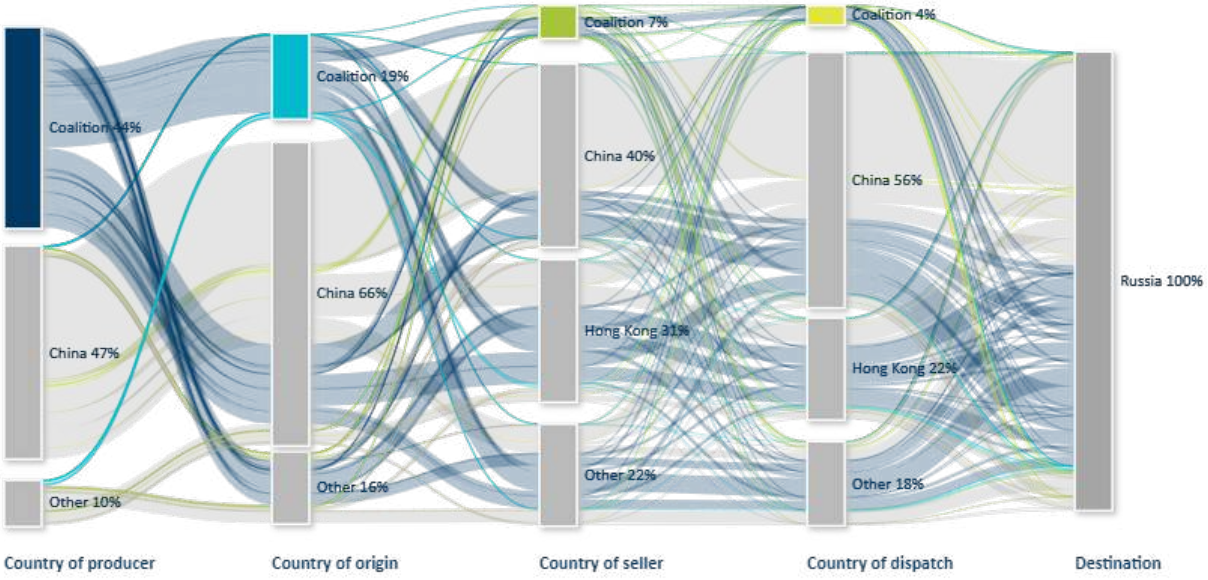
### *II.3. Fundamental Changes to Supply Chains*

**Supply chains for battlefield goods and critical components have changed substantially.** Export controls have contributed to fundamental realignments in global supply chains with regard to important inputs for Russia's military industry. Intermediaries in third countries—in particular China, Turkey, and the UAE—are now responsible for the overwhelming share of sales and shipments to Russia. However, a large portion of battlefield goods and critical components imported by Russia continues to be produced on behalf of companies headquartered in countries that have, in fact, imposed comprehensive export controls. This means that Russia has not been able to find alternative suppliers for these goods and that sanctions remain a potentially powerful tool. But it also demonstrates that export controls face substantial enforcement challenges.

[17] In Box 2, we take a closer look at a specific category of goods that plays a key role for Russia's military capacity: CNC machines.

**Dominant share of battlefield goods and critical components now reaches Russia via third countries.** The key finding of our analysis is that direct sales and shipments from export controls coalition countries have largely been replaced by transactions that involve third-country intermediaries. This is the case for the trade with battlefield goods as well as with critical components. While not surprising given the fact that many countries playing an important role in these goods' production have imposed export controls, this dynamic represents a significant challenge for the enforcement of the sanctions regime as the monitoring of transactions becomes much more difficult for the enforcement agencies of coalition countries, including customs services.

**Figure 6: Mapping of Russian imports of battlefield goods in January-October 2023**[18]




Percentages in this chart differ from the ones reported in the remainder of this chapter, as well as in Appendix 3, since only transactions with data for all stages of the supply chain are included here.

*Source: KSE Institute*

**Mapping out trade in battlefield goods and critical components is key to enforcement.** For producers and entities participating in the trade with them, it is critical to understand how Russia continues to be able to import significant quantities of items that are critical for its war in Ukraine. Mapping out trade flows and identifying patterns—including jurisdictions through which physical shipments are routed and where involved intermediaries are located—will support private sector compliance efforts. At the same time, it will help enforcement agencies to monitor developments, prosecute violations, and improve the export controls regime.

**Untangling complex supply chains along several key dimensions.** For the purpose of a comprehensive understanding of Russia's capacity to import battlefield goods and critical components, we investigate transactions along several dimensions, including: i) the ultimately-responsible producer of a good and location of its headquarter (*"country of producer"*); ii) the jurisdiction in which the item was manufactured (*"country of origin"*); iii) the entity that conducted the final sale to Russia and its location (*"country of seller"*); iv) the jurisdiction from which the item was finally shipped to Russia (*"country of dispatch"*); and v) the ultimate buyer of the good in Russia. Figure 6 visualizes how battlefield goods reached Russia in January-October 2023.

**Companies from export controls coalition countries continue to play a key role in supply chains.** For instance, we find that countries that have imposed export controls on Russia were still involved in 48.5% of all imports of battlefield goods in January-October 2023 as the location of the producer's headquarter, production facility, final seller to Russia, or dispatcher. This illustrates two key facts: (1) sanctions violations are likely widespread

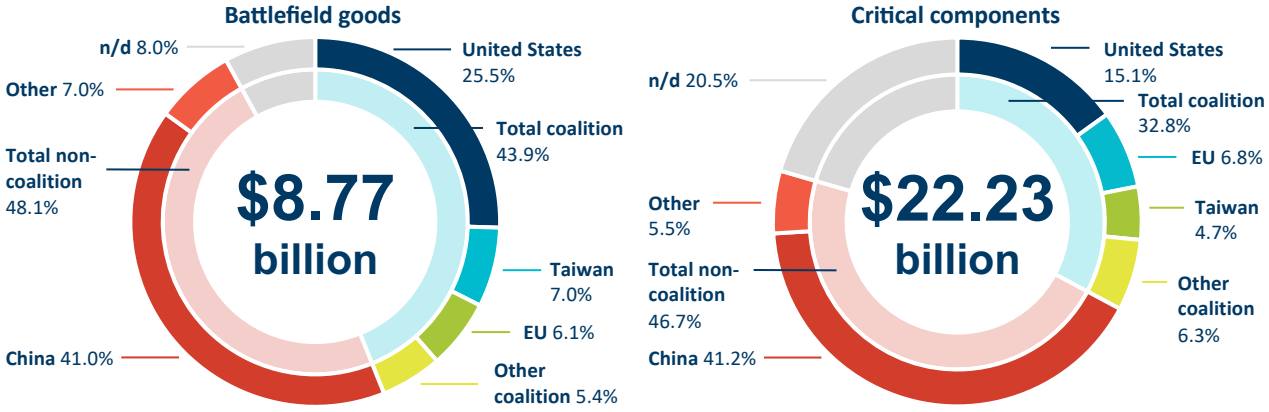
[18] For the purposes of the analysis, we distinguish between mainland China ("China" in the text, figures, and tables) and the special administrative regions of Hong Kong ("Hong Kong") and Macao ("Macao") as dynamics are distinctly different.

and systemic; and (2) export controls remain an exceptionally powerful tool to reign in Russia's capacity to wage its brutal war on Ukraine. The different stages of the supply chain are discussed in more detail below and additional information on the most important countries on each stage can be found in Appendix 3.

***Stage 1: Where Producers Are Headquartered***

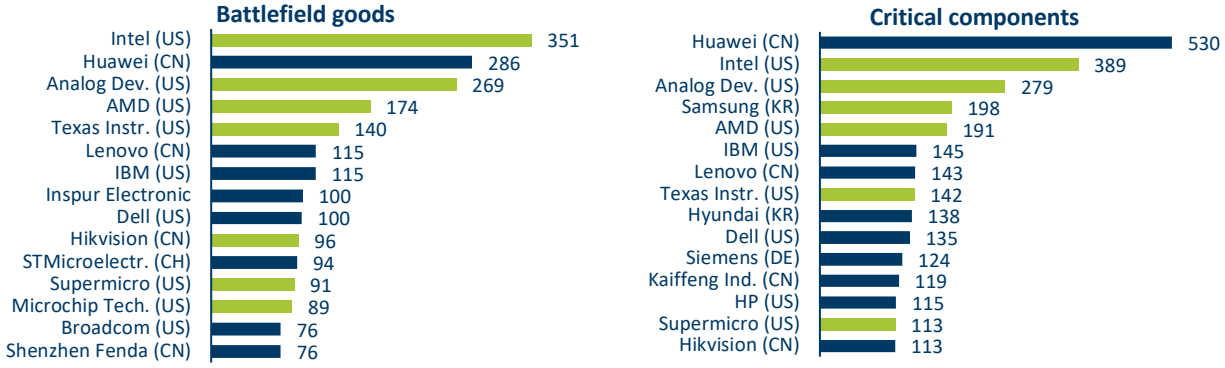
**Producers headquartered in coalition countries were responsible for at least 43.9% of battlefield goods and 32.8% of critical components in January-October 2023.** Within supply chains, coalition countries play the biggest role, by far, when it comes to the ultimately-responsible producers. Entities headquartered in the United States alone accounted for 25.5% of battlefield goods and 15.1% of critical components in the first ten months of the year, followed by those from the European Union and Taiwan (see Figure 7).[19] In terms of specific companies, we find that most major international technology companies headquartered in the export controls coalition continue to trade with Russia through third-country intermediaries (see Figure 8), including, most notably, Intel (U.S.), Analog Devices (U.S.), AMD (U.S.), Texas Instruments (U.S.), and IBM (U.S.).[20] Due to the broader critical components sample, the top-list for these goods includes additional companies such as Samsung and Hyundai (both South Korea). Outside of the coalition, it is largely producers from China that play a role for Russia's continued access to both sets of goods, including Huawei and Lenovo.

**Figure 7: Imports in January-October 2023 by country of producer**




*Source: KSE Institute*

**Figure 8: Imports in January-October 2023 by producer (top-15), in $ million***




*Source: KSE Institute *green = companies whose components have been found on the battlefield*

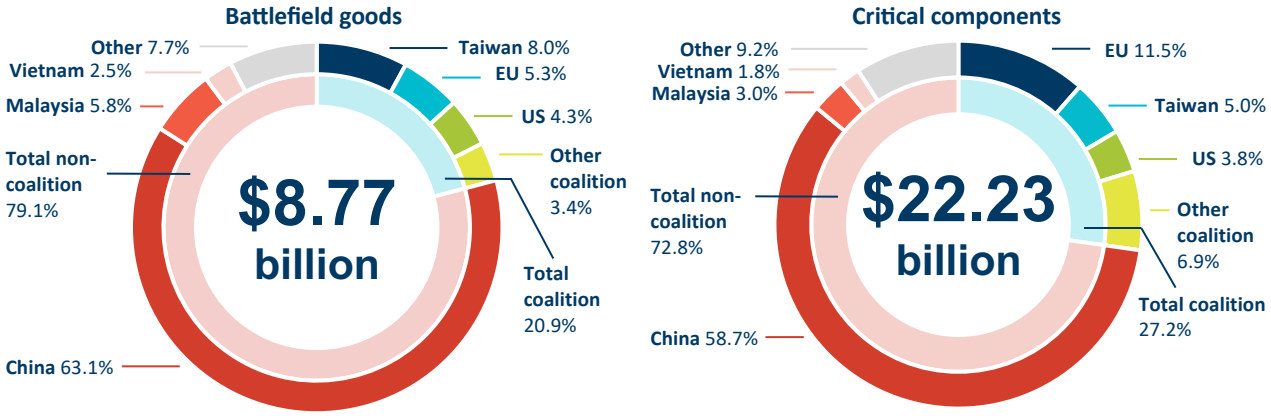
[19] These numbers likely understate the role of coalition producers somewhat as country assignments have not been made for all entities. We continue to work on reducing the share of transactions without identified producer countries.

[20] We take a closer look at two companies whose products are found in almost all types of Russian military equipment on the battlefield—Analog Devices and Texas Instruments—in Box 1.

***Stage 2: Where Goods Are Manufactured***

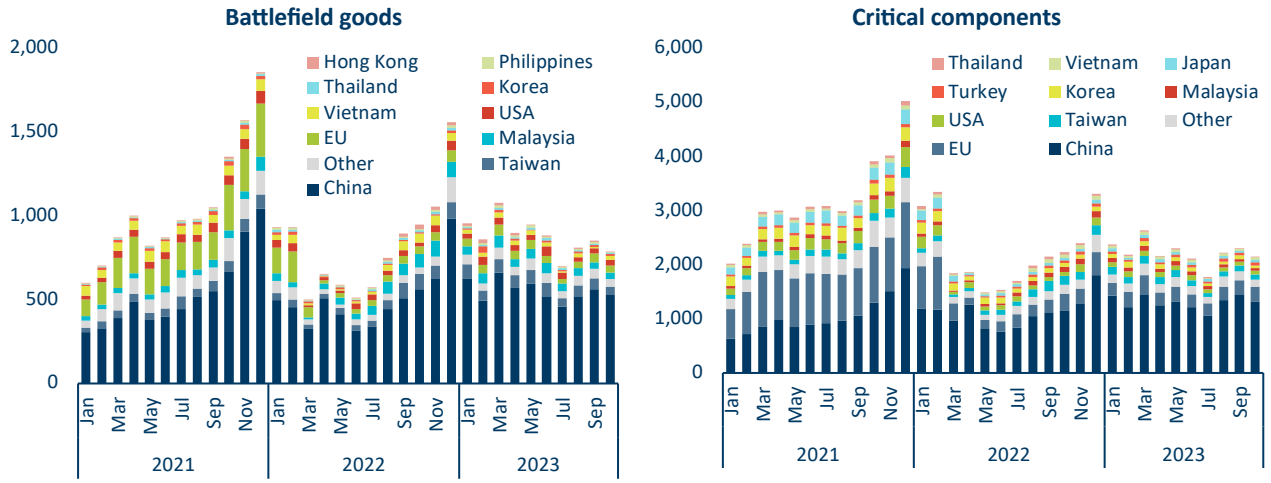
**20.9% of battlefield goods and 27.2% of critical components were manufactured in countries of the export controls coalition in January-October 2023.** While the role of coalition countries as countries of origin is much more limited than with regard to the location of the ultimately-responsible producers, their role remains surprisingly significant (see Figure 9). The European Union, Japan, South Korea, Taiwan, and the United States deserve particular attention. Their numbers pale, however, in comparison to those of China, which alone accounts for 63.1% of battlefield goods and 58.7% of critical components production. Importantly, a substantial share of Russian imports are produced in third countries on behalf of entities from sanctions coalition countries—26.8% ($2.02 billion) in the case of battlefield goods in January-October 2023. Roughly two-thirds of these products are manufactured in China. Changes with regard to manufacturing locations are not as significant as those for later stages of the supply chain. EU- and U.S.-based producers have long relied on production facilities abroad, not only since the start of Russia sanctions (see Figure 10).

**Figure 9: Imports in January-October 2023 by country of origin**




*Source: KSE Institute*

**Figure 10: Dynamics of imports by country of origin, in $ million**



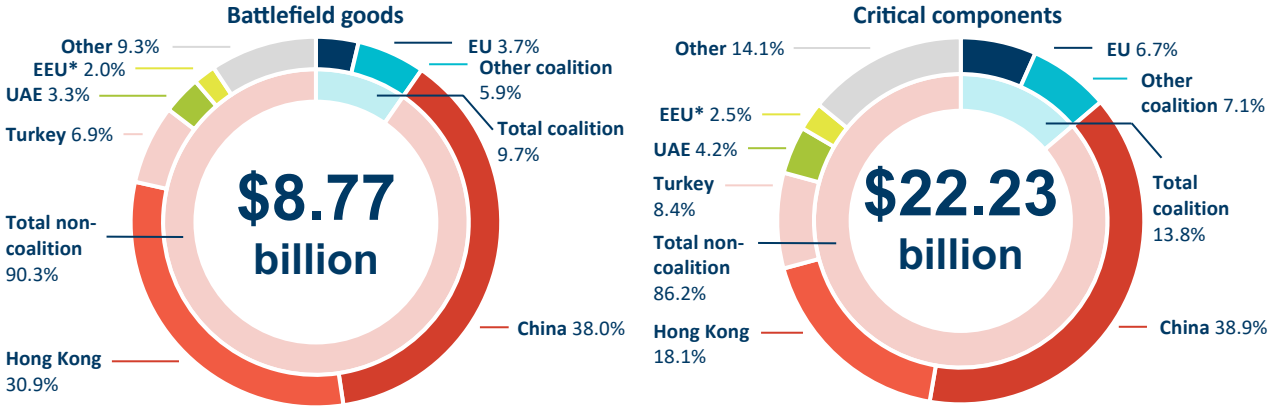

*Source: KSE Institute*

***Stage 3: Where Final Sellers to Russia Are Located***

**9.7% of battlefield goods and 11.8% of critical components were sold by entities in coalition countries in January-October 2023.** When it comes to the ultimate sale to Russia, coalition countries play a much more limited role as most Russian imports are now predominantly conducted via third-country entities, independent of where the products were manufactured or which companies are ultimately responsible for their production. Five jurisdictions deserve particular attention with regard to this part of the supply chain (see Figure 11): China

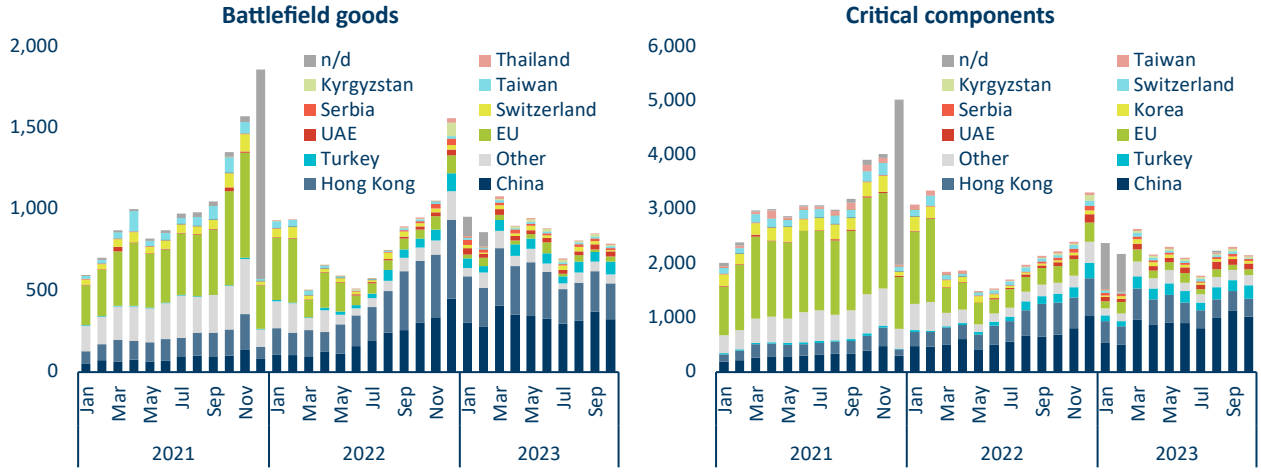
(38.0% for battlefield goods, 38.9% for critical components), Hong Kong (30.9%, 18.1%), Turkey (6.9%, 8.4%), the UAE (3.3%, 4.2%), and countries of the Eurasian Economic Union (2.0%, 2.5%).[21] The shift compared to the pre-sanctions period is significant as sales from the EU used to make up a large portion (see Figure 12).

**Figure 11: Imports in January-October 2023 by country of seller**



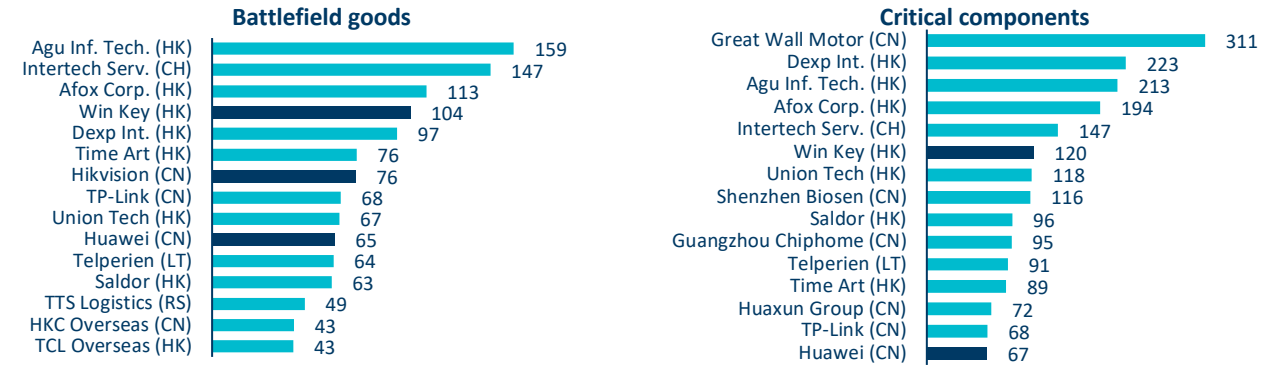

*Source: KSE Institute*

**Figure 12: Dynamics of imports by country of seller, in $ million**




*Source: KSE Institute*

**Figure 13: Imports in January-October 2023 by seller (top-15), in $ million***




*Source: KSE Institute *dark blue = sanctioned by the United States*

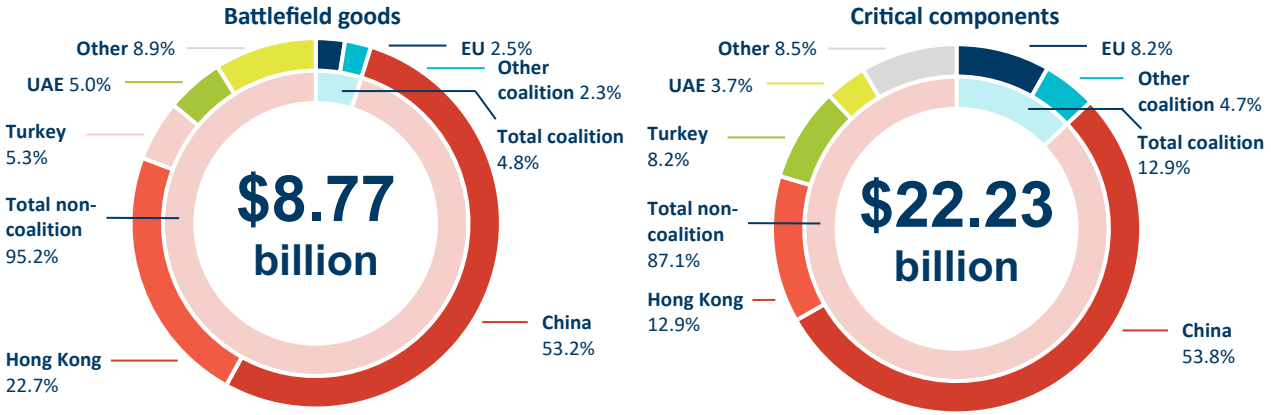
[21] Not at all trade between Russia and other members of the Eurasian Economic Union is captured by our datasets. Thus, numbers likely underestimate the role of these countries for Russia's ability to acquire battlefield goods/critical components.

**Chinese and Hong Kong-based companies dominate final sales to Russia.** Not surprisingly, this segment of the supply chain is much more diversified/fragmented thus the largest individual entities account for a relatively small share of the total trade. However, there are still companies that play an outsized role and deserve particular attention (see Figure 13). While many of the top-sellers are located in China and Hong Kong, there are some which are headquartered in coalition countries, including Intertech Services (Switzerland), Telperien (Lithuania), MR Global (Switzerland), D-Link (Taiwan), and Mykines (United Kingdom).

***Stage 4: From Where Goods Are Shipped to Russia***

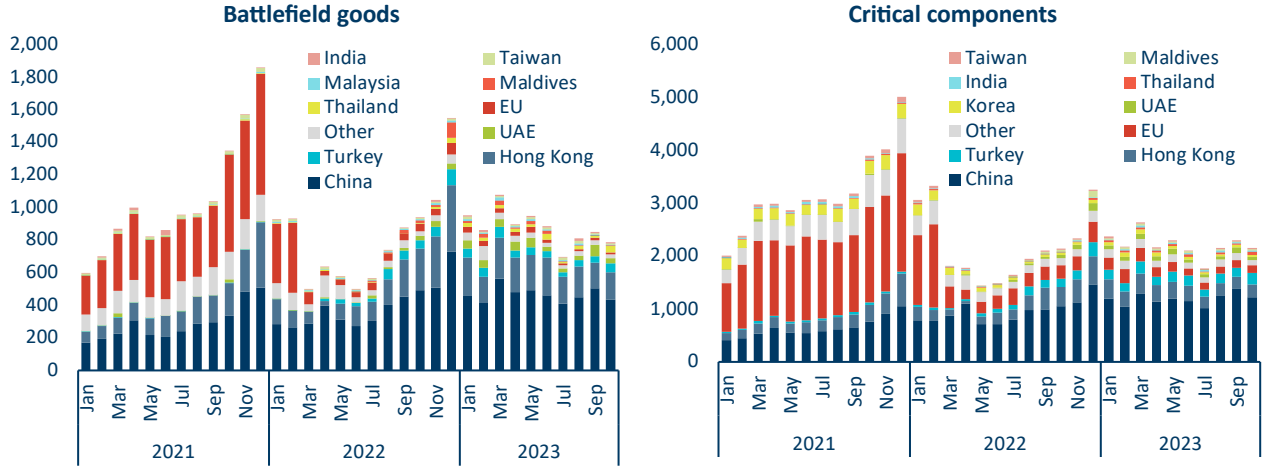
**Only 4.8% of battlefield goods and 12.9% of critical components shipped from coalition countries to Russia in January-October 2023.** Jurisdictions participating in the export controls regime play the least important role when it comes to the final shipment of the goods (see Figures 14 and 15). This is not surprising, as dispatching the items in question from the territory of coalition countries would allow authorities,—in particular customs services—to trace and interrupt trades. But the share is also far from zero, indicating that the problem goes beyond enforcement and includes loopholes and inconsistencies as far as sanctioned goods, derogations etc. are concerned. More than half of all goods, in value terms, are shipped to Russia from China (53.2% and 53.8%, respectively), followed by Hong Kong, Turkey, and the UAE. Together, these four jurisdictions account for 86.2% of total battlefield goods shipments and 78.6% of critical components shipments.

**Figure 14: Imports in January-October 2023 by country of dispatch**




*Source: KSE Institute*

**Figure 15: Dynamics of imports by country of dispatch, in $ million**

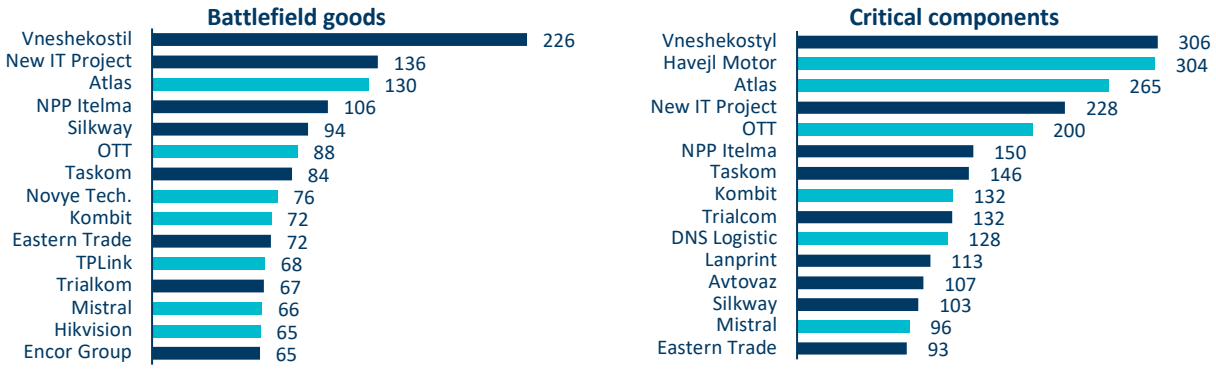



*Source: KSE Institute*

***Stage 5: Who Is Buying the Goods in Russia***

**Sanctions on Russian buyers of battlefield goods and critical components are not consistent.** Entities within the Russian military industry generally do not feature as buyers of battlefield goods and/or critical components. Nevertheless, Russian buyers are an important element of the supply chain and their analysis is important for coalition companies' due diligence. Similar to previously-mentioned areas of sales and shipments, the number of individual companies involved is big and, thus, their respective shares of total imports small (see Figure 16). Some of the most important buyers—including Vneshekostil, Novyi IT Project, and NPP Itelma—are sanctioned in the United States but not in other jurisdictions such as the European Union, United Kingdom etc.[22] This creates major challenges in terms of export controls enforcement. We also find that companies linked to the Russian military industry (e.g., EMC Expert, Favorit, NPP Itelma, IQ Components, Kvazar, SMT iLogic, Testkomplekt, and VMK) appear as final buyers of battlefield goods and critical components in the data—with a substantial share of the products in question stemming from producers located in coalition countries.

**Figure 16: Imports in January-October 2023 by buyer (top-15), in $ million***




*Source: KSE Institute *dark blue = sanctioned by the United States*

### *II.4. Key Foreign Companies Continue to Trade with Russia*

In this chapter, we look specifically at the trade with Russia of companies whose products have repeatedly been found in Russian weapons on the battlefield.[23] Appendix 4 lists the more than 250 companies included in the analysis. Several large multinational technology companies deserve particular attention in this context, including U.S.-based AMD, Analog Devices, Broadcom, Hewlett Packard, Honeywell International, Intel Corporation, Kingston Technology, Microchip Technology, and Texas Instruments. But other export controls coalition jurisdictions are also well-represented by Hitachi (Japan), Infineon Technologies (Germany), NXP Semiconductors (Netherlands), Samsung (South Korea), and STMicroelectronics (Switzerland).

While the discovery of their products in Russian weapons does not mean that sanctions violations took place—products may have been sold to Russia before the start of the full-scale invasion—, we find that the companies' goods continue to make their way to Russia in large quantities through third-country intermediaries. But there is some positive news as well: the value of this trade appears to be declining significantly throughout 2023. Below, we summarize key findings along several dimensions, including different stages of the supply chain.

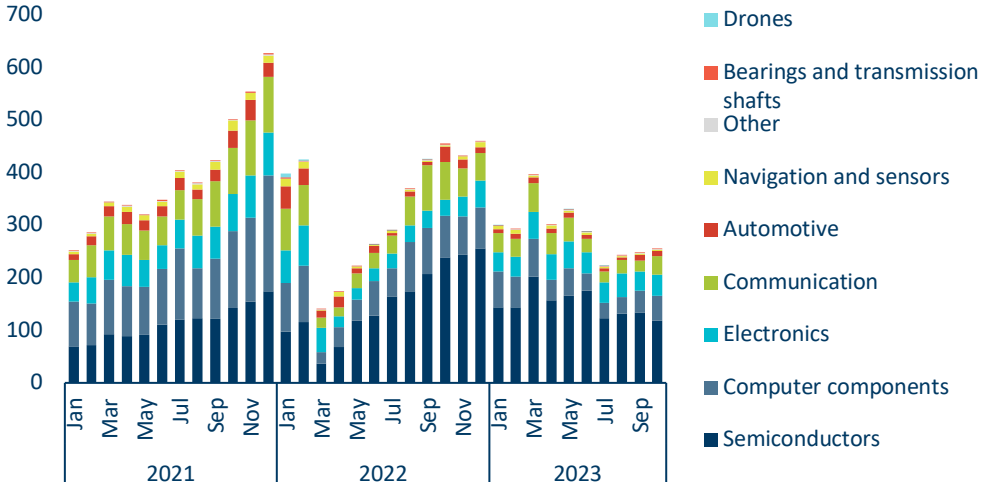
- Overall dynamics: Imports of critical components from selected companies displayed similar dynamics in 2022 as the broader samples: a sharp drop in the immediate aftermath of the imposition of export controls, and a noticeable rebound in the second half of the year as Russia adapted to the restrictions. Throughout 2023, however, trade values fell significantly, reaching only $242 million per month in July-October—a 24% decline vs. H1 2023, and 40% decline vs. H2 2022 and the pre-sanctions period.

[22] See "Inconsistency in Action: A Case of Sanctioning the Russian Military Industry," NAKO.

[23] See the NACP's (National Agency on Corruption Prevention, Ukraine) database on foreign components in Russia weapons here.

- Composition of goods: In this subset, semiconductors and integrated circuits account for the largest share by far at 52% ($1.49 billion) of the total trade in January-October 2023. This is in line with the structure of components found on the battlefield, where these parts also play the most important role. We observe encouraging dynamics for many categories (see Figure 17). Imports of semiconductors and integrated circuits in the first ten months of 2023 were 30% lower than in H2 2022—and those of computer components 39% lower. Electronics, however, increased by 19%. And, importantly, trade with semiconductors and integrated circuits is still substantial. In fact, monthly imports ($150 million) in 2023 are still much higher (33%) than pre-sanctions. Imports are declining—but not fast enough.[24]

**Figure 17: Imports of critical components from selected companies by type, in $ million**




*Source: KSE Institute*

- Producers and production: Companies headquartered in the United States play the largest role, by far. In January-October 2023, they accounted for 61% ($1.76 billion) of all critical components from our sample of selected entities. Producers from the EU were responsible for only 8% and those from South Korea, Japan, and Taiwan for 6-7% each. Comparing the location of headquarters (see Figure 18) and location of production (see Figure 19), we see that the products are mostly produced outside of coalition countries. China (35%, $991 million in January-October 2023) and Malaysia (13%, $370 million) made up the largest shares. Within the coalition, the largest amounts are accounted for by Taiwan (13%, $367 million), the U.S. (8%, $238 million), South Korea (5%, $147 million), and the EU (5%, $144 million).

**Figure 18: By country of producer, in $ million**

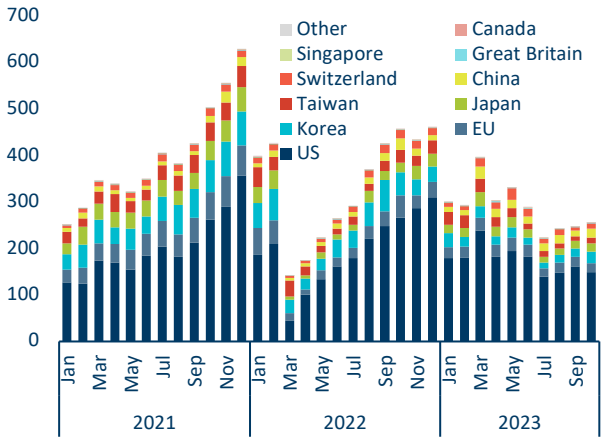
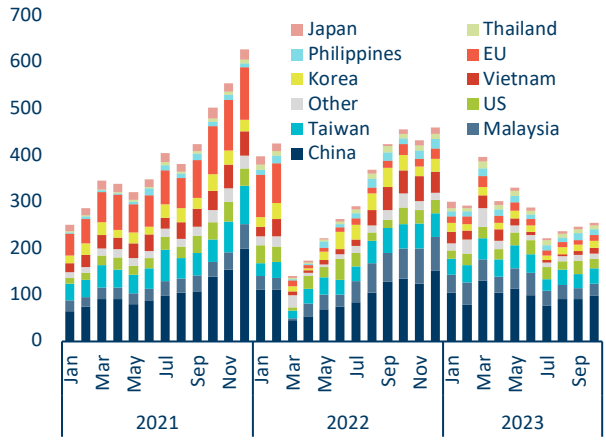



**Figure 19: By country of origin, in $ million**




*Source: KSE Institute*

[24] In Box 2, we take a closer look at a specific category of goods that plays a key role for Russia's military capacity: CNC machines.

- Sellers and dispatchers: When it comes to final sales (see Figure 20) and shipments (see Figure 21) to Russia, changes since early 2022 are quite dramatic. The EU has essentially disappeared, and two jurisdictions now account for the overwhelming shares: Hong Kong (42% of sales and 43% of shipments in January-October 2023) and China (26% and 34%, respectively). Other countries that deserve attention are Turkey and the UAE. Figure 22 summarizes dynamics on different stages of the supply chain.

**Figure 20: By country of seller, in $ million**

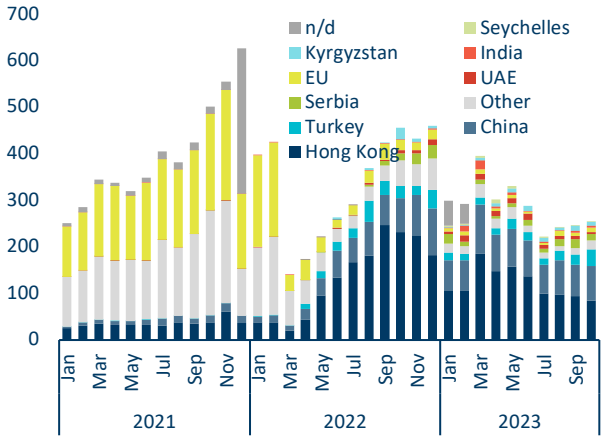
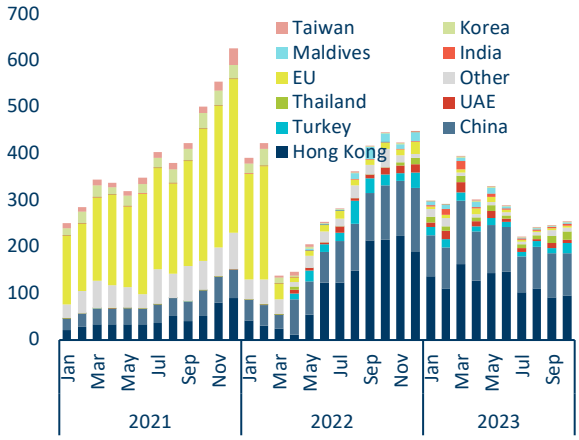
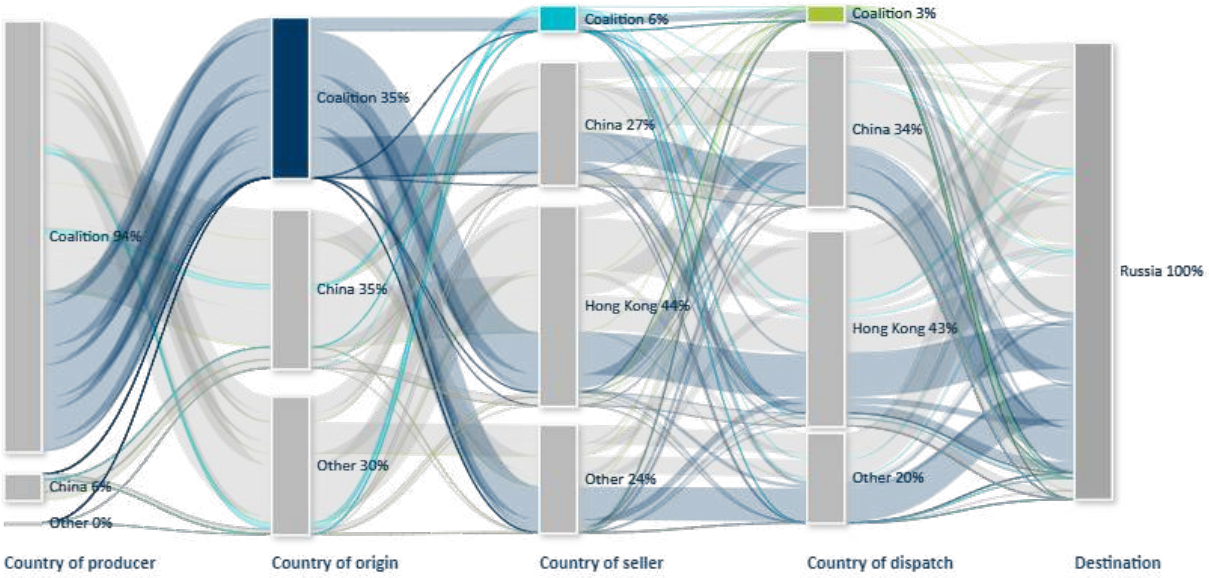



**Figure 21: By country of dispatch, in $ million**




*Source: KSE Institute*

**Figure 22: Mapping of Russian imports of critical components from selected coalition companies**




Includes data for January-October 2023. Percentages in this chart differ from the ones reported in the remainder of this chapter as well as in Appendix 3 since only transactions with data for all stages of the supply chain are included here.

*Source: KSE Institute*

- Company dynamics: Many of the companies featuring prominently as far as components in Russians weapons as well as trade with Russia are concerned have, in fact, increased their supplies compared to the pre-sanctions period—knowingly or not (see Figure 23). But, in some cases, there are indications that this is changing in 2023. For instance, Intel's monthly supplies to Russia rose from $45 million in 2021 to $64 million in 2022 before falling to $39 million in January-October 2023. For many others, however, 2023 totals are likely to come in above 2022 numbers, including Analog Devices, Texas Instruments, STMicroelectronics, Microchip Technology, and NXP Semiconductors (see Box 1).

- A closer look at monthly developments (see Figure 24) shows which companies have increased their supplies to Russia the most in percentage terms. Analog Devices, whose components are often found in Russian weapons, clearly stands out here. The company's average monthly supplies of critical components to Russia (of $27 million) in January-October 2023 were 51% higher than in 2022 and 162% higher than in 2021. Compliance efforts are clearly insufficient. NXP Semiconductors and STMicroelectronics sales have also risen, but developments in recent months show improvements.

**Figure 23: By producer (top-15), in $ million**

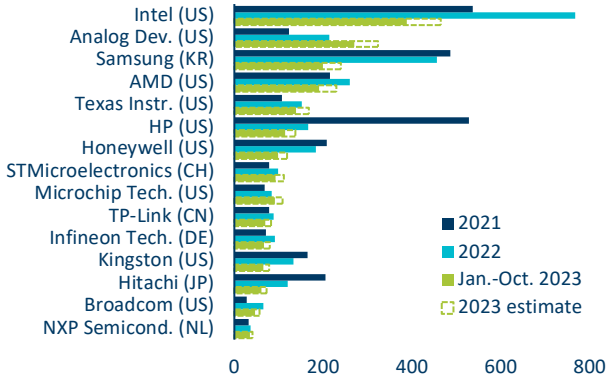
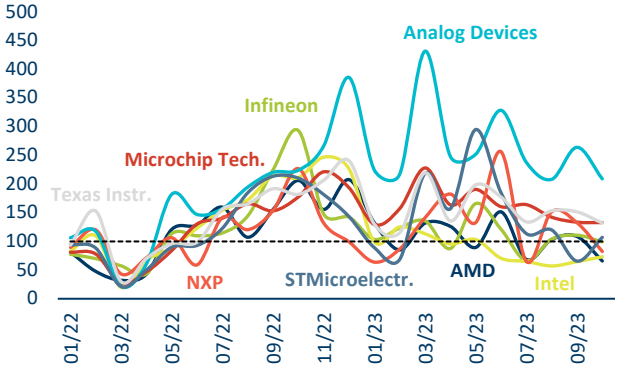



**Figure 24: By producer, index (100 = 2021 avg.)**




*Source: KSE Institute*

- Third-country intermediaries: As mentioned before, final sellers are much more fragmented, but a closer look at this stage of the supply chain still allows us to draw important conclusions (see Figure 25). Most of the largest suppliers are located in China and Hong Kong—consistent with our findings above—but companies from other countries appear as well, including from Serbia (e.g., Soha Info, Avala Informatika, and TTS Logistics). In addition, while their numbers are relatively small, we also find entities from coalition countries such as Mykines (United Kingdom) and Telperion (Lithuania).
- Buyers in Russia: Many of the ultimate buyers of critical components from our sample of selected companies are under sanctions by the United States, and some are sanctioned in additional jurisdictions as well (see Figure 26). However, companies such as NPP Itelma ($91 million), Vneshekostil ($74 million), Lanprint ($59 million), VMK ($39 million), and others continue to be able to acquire substantial amounts of such goods, which shows the aforementioned loopholes of an inconsistent sanctions regime.

**Figure 25: By seller (2023, top-15), in $ million***

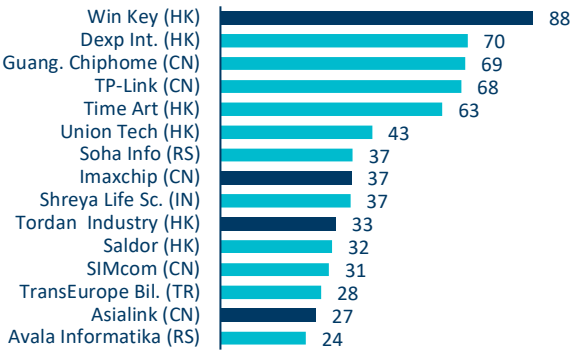
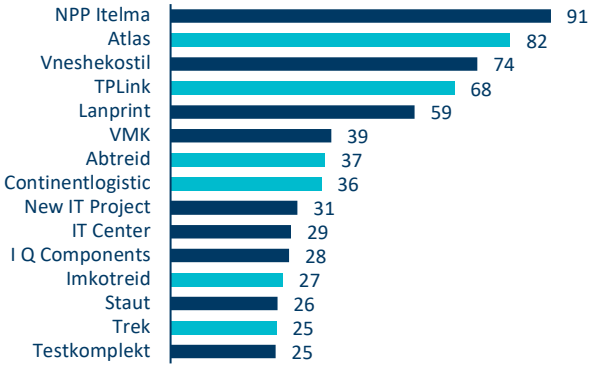



**Figure 26: By buyer (2023, top-15), $ million***




*Source: KSE Institute *dark blue = sanctioned by the United States*[25]

[25] Staut also sanctioned by the U.K.; Testkomplekt also sanctioned by Switzerland and the U.K.; Tordan Industry also sanctioned by Switzerland; VMK also sanctioned by Switzerland.

## Box 1. Analog Devices and Texas Instruments

Analog Devices and Texas Instruments are two important producers of critical inputs for Russian military equipment. Their products are found in almost all types of weapons on the battlefield and account for 14% and 13%, respectively, of all foreign components that have been identified. Thus, implementation of better compliance procedures by these two companies could significantly impact Russia's military production capacity. Their activities should also be regularly scrutinized by enforcement agencies to understand common schemes of sanctions evasion. Here, we take a closer look at how trade with their products has changed over time.

For both companies, we find significant increases in trade values vs. the pre-sanctions period since the second half of 2022 (see Figures 27 and 28). However, it is also critical to investigate how prices have changed for their products. While our data do not contain volume information for all transactions in critical components, it is available for most imports from Analog Devices and Texas Instruments, which exclusively sell semiconductors and integrated circuits. The analysis reveals that prices have increased 2.2 times for Analog Devices and 2.6 for Texas Instruments products. In volume terms, this means that the increase in Russian imports from the former is significantly smaller, and Texas Instruments sales have actually fallen. The price effects we observe can be attributed to a combination of several factors:

- The complexity of supply chains has increased due to export controls largely eliminating direct supplies of certain goods to Russia. Each intermediary assisting Russia in evading export controls retains a margin and, as this trade often includes up to five intermediaries, the final price rises considerably.
- Russia may have started to purchase more advanced products from these companies as demands of the military industry vs. civilian sectors have increased. Such a shift in the product mix could also contribute to higher average prices. Price increases also reflect general market trends.

**Figure 27: Imports of Analog Devices products**

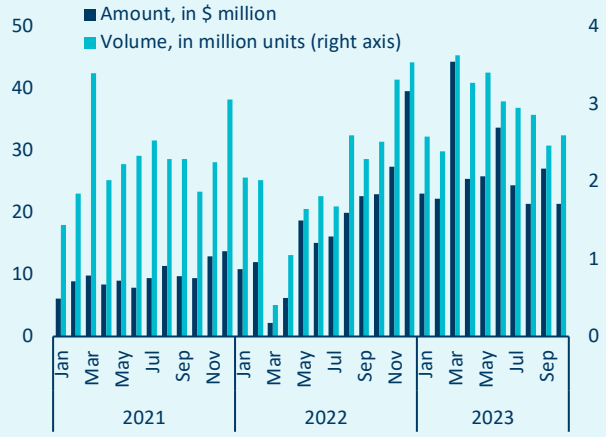
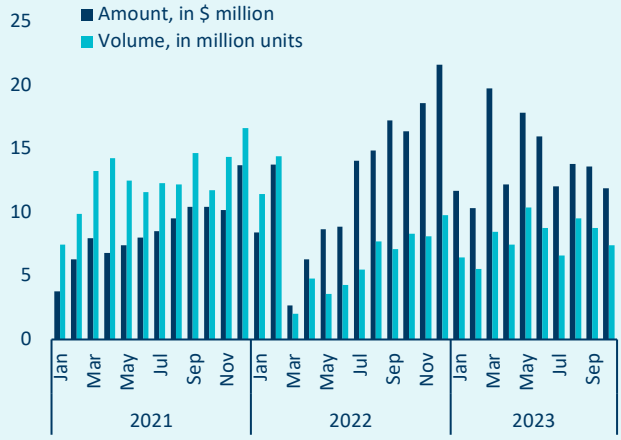



**Figure 28: Imports of Texas instruments products**




*Source: KSE Institute*

While the two companies are headquartered in the United States, only a small share of their products is actually manufactured there—8% for Analog Devices and 7% for Texas Instruments. This is the result of efforts to establish production facilities offshore. In recent years, the share of production in China, Malaysia, the Philippines, and Thailand has risen from 47% to 75% for Analog Devices and from 49% to 80% for Texas Instruments. Conversely, the share of production in the EU and Taiwan has decreased for both.

Consistent with our analysis of overall trade dynamics above, China, Hong Kong, Turkey, and the UAE serve as the most important countries from where the companies' products are ultimately sold and shipped to Russia. But other locations are also worth mentioning when it comes to physical shipments: Kazakhstan, the Kyrgyz Republic, Serbia, the Virgin Islands, Mongolia, and the Maldives. India also features prominently.

One of the most important suppliers of Analog Devices and Texas Instruments goods to Russia is Hong Kong-based *Tordan Industries*. The company—which is already sanctioned by the United States, the European Union, and Switzerland—accounted for $16.5 million in sales in January-October 2023. This case illustrates how Russia establishes shell companies to preserve its access to critical components: At the same address, we find *First Company of Consulting and Secretarial Services*, a Russian company that, according to its website, provides services to Russian companies in China and Hong Kong. It also offers services to nominal founders and/or shareholders (e.g., Chinese-controlled companies) and assists in obtaining licenses.

In 2023, at least 18% of Analog Devices products and 16% of Texas Instruments products where purchased, in Russia, by companies with established links to the military industry. As the list of buyers continues to evolve and new ones appear every month, it is critical to investigate buyers' links to the military.

## Box 2. CNC Machines

***What Are CNC Machines***

Computer Numerical Control (CNC) machines are fully automatized industrial tools that are widely used in different industries such as aerospace, automotive, metalworking, and electronics. Due to their unique features and accuracy, CNC machines are also critical for the military industry in many countries, especially for the production of weapon hulls, aircraft parts, missile and drone/UAV components, and microelectronics. Simply put, it is hard—or even impossible—to find types of modern weaponry that do not require the use of CNC machines in their production. Weapons producers are, thus, also the key consumer of CNC machines in Russia. Between 70-80% of all such machinery is used by the military-industrial complex. This dependency represents a unique opportunity for the sanctions coalition to take advantage of strategic vulnerabilities and curb the aggressor's capacity to wage its brutal war on Ukraine.

***What Restrictions Are in Place***

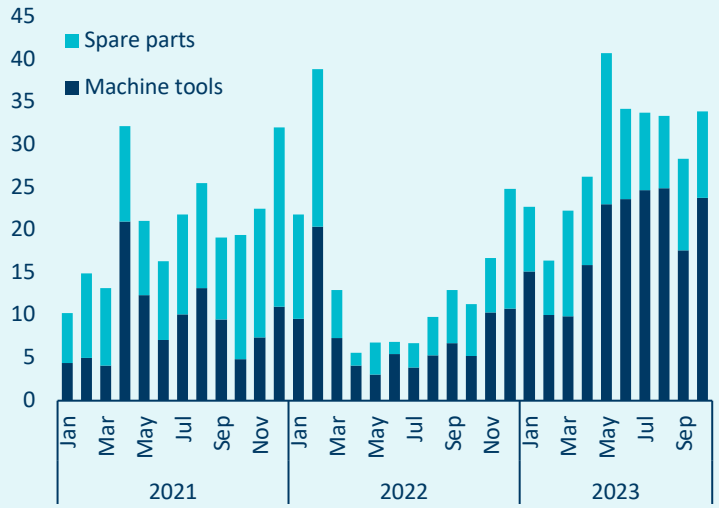
Recognizing the critical role of CNC machinery, some coalition jurisdictions have imposed export controls on these goods. For instance, on December 18, 2023, the European Union expanded the list of restricted items that could contribute to the technological advancement of Russia's defense and security sectors to include CNC machine tools as well as spare parts. This means a ban on the sale, supply, transfer, or export. In addition, the 12th sanctions package prohibits the export of software for production process control as well as industrial design, including CAD (computer-aided design) and CAM (computer-aided manufacturing) programs used on CNC machinery. Together with a ban on the transit of such goods through the territory of the Russian Federation, these measures are an important step towards exploiting critical vulnerabilities within Russia's military industry by limiting access to certain critical goods. Importantly, Japan, home of many companies in the CNC machinery sector, has imposed comprehensive export controls as well. We expect that it will become much more complicated—and more expensive—for Russia to acquire CNC machinery and spare parts going forward and will continue to monitor if this materializes in the data. However, we urge additional countries that play an outsized role for CNC machine production and have seen their sales to Russia increase in recent months , including South Korea, to impose comprehensive restrictions as well so that Russia will not be able to switch to alternative suppliers from coalition countries.

***Current Trade with CNC Machines***

Since the beginning of the full-scale invasion, Russia's use of CNC machinery has been investigated using a broad range of open-source information, including publicly accessible data on procurement, report on import substitution in Russia, as well as photos and videos from military production facilities. According to the Economic Security Council of Ukraine (ESCU), 38 producers of CNC machinery are of particular importance for Russia, including, among others, DMG Mori and FANUC. We use this list of companies as a starting point for our analysis of transaction-level data on Russian imports to investigate if these entities continue to supply CNC machinery and/or spare parts—directly or indirectly—, and how trade values have developed over time.

As with our broader subsets of goods, we find that Russian imports of CNC machinery and spare parts dropped sharply in the immediate aftermath of the imposition of export controls, followed by a strong rebound towards the end of 2022 (see Figure 29). In January-October 2023, Russia imported CNC machinery worth $189 million and spare parts worth $103 million. This means that monthly average imports are 88.3% higher than in the pre-full-scale invasion period for CNC machinery and 14.3% lower for spare parts. In our view, trade dynamics indicate that Russia has been trying to significantly expand its military production in 2023 and that the country has been able to obtain the machinery necessary for this purpose.

**Figure 29: Russian imports of CNC machinery from 38 key companies, in $ million**




*Source: KSE Institute*

In terms of the supply chain, we see some interesting differences compared to the broader "battlefield goods" and "critical components" subsets. *First*, producers from export controls coalition countries account for a much larger share of the total trade in CNC machines and spare parts that are deemed to be particularly important for Russia—97.8% in January-October 2023. These companies are also concentrated in a small number of countries, including Germany (42.3%), South Korea (20.7%), Taiwan (19.5%), the United States (7.1%), and Japan (6.9%). *Second*, the production of these items is also overwhelmingly located in coalition countries—76.7% in January-October 2023—with Germany (28.0%), Taiwan (20.4%), and South Korea (15.9%) playing the biggest roles. We see China's role as a country of production growing somewhat to 22.1%, largely replacing manufacturing in EU countries. More noticeable is that Taiwanese companies and factories are responsible for most of the increase in Russian imports in 2023 (see Figures 30 & 31).

As far as the final seller's location and the place of shipment are concerned, dynamics are similar to the ones observed for battlefield goods and critical components; most of the goods are sold and/or shipped to Russia by entities in China, Hong Kong, and Turkey (see Figures 32 & 33). Coalition entities/countries only accounted for 10.6% of sales and 21.7% of shipments in January-October 2023. In particular European sellers and dispatchers, which had previously played a significant role, have essentially disappeared, meaning that export controls enforcement becomes much more challenging for coalition customs services. However, there are still some direct shipments from coalition countries, most notably from EU countries (8.6%), South Korea (7.5%), and Taiwan (5.5%). Within the EU, we find the largest shares for Finland, Poland, Germany, Lithuania, and Latvia. It is worth mentioning that Turkey's role with regard to CNC machines and spare parts is much more pronounced than for the broader product subsets.

ESCU emphasizes a noticeable trend pointing to a decline in the share of western-made CNC machines with a noticeable increase of Chinese counterparts. While China holds a prominent position as the world leader in the production of low- and medium-precision CNC machines, there is a gap in the production of high-precision machines. It is important to note that certain components of Chinese CNC machines are still sourced from Western countries and Western allies. Moreover, imported Chinese machine tools may have Western brands but are manufactured in China, adding an additional layer of complexity to the dynamics of the CNC market.

We hope that strengthened export controls with regard to CNC machines and spare parts will make a noticeable difference in the coming months. It should be pointed out that the trade in CNC machines is naturally easier to control, as the items are much bigger in size than many other dual-use goods. This makes smuggling them much harder and should allow for tracking of physical shipments with geolocation features. Producers may also be able to remotely control machinery already supplied to Russia (including machines

supplied before the full-scale invasion) or at least stop supporting/updating the software. We acknowledge that Russia will undertake a concerted effort to procure CNC machinery and spare parts from alternative suppliers should export controls enforcement be tightened significantly. However, so far, observers have not seen Chinese machines actually being used in facilities of the Russian military industry.

**Figure 30: By country of producer, in $ million**

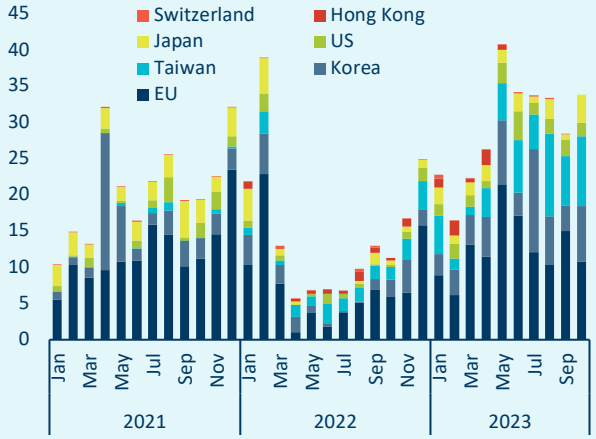
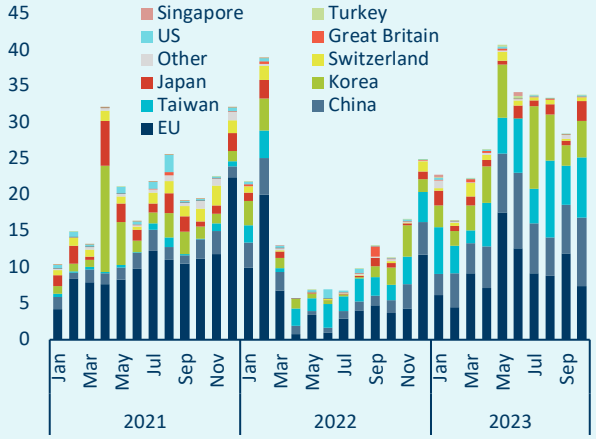



**Figure 31: By country of origin, in $ million**




*Source: KSE Institute*

**Figure 32: By country of seller, in $ million**

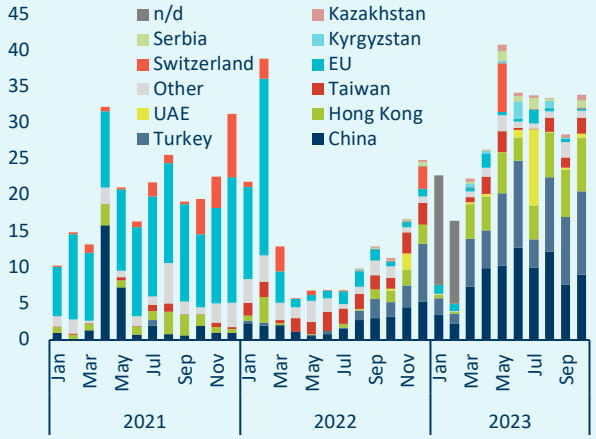
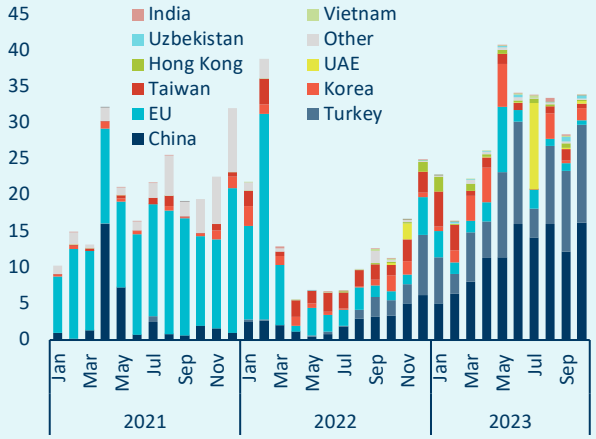



**Figure 33: By country of dispatch, in $ million**

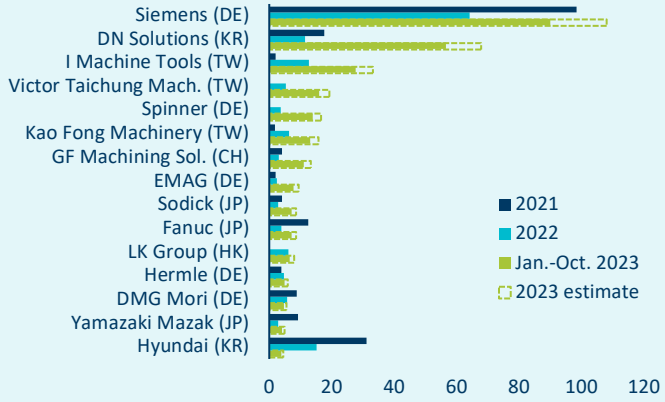



*Source: KSE Institute*

Our analysis shows that most of the producers included in this sample have significantly expanded their trade with Russia since the start of the full-scale invasion (see Figure 34). In fact, for many of them, sales in January-October 2023 were already higher than in the entirety of 2022—or even 2021. This includes top producers such as, among others, Siemens (Germany), DN Solutions (South Korea), I Machine Tools (Taiwan), Spinner (Germany), and Victor Taichung Machinery Works (Taiwan). Some companies have, however, reduced their exposure to Russia, including Hyundai (South Korea), Fanuc (Japan), and DMG Mori (Germany). Similar to the broader goods categories discussed above, the analysis shows that companies can effectively control their supply chains if they choose to implement proper due diligence procedures.

Figures 35 and 36 provide some information about the final sellers of CNC machines as well as their final buyers in Russia. An analysis of historical contracts, public procurement records, and trade data reveals a discernible pattern wherein the majority of these companies demonstrate clear connections to Russian military entities. SFT, Baltic Industrial Company, Sois Konsalt, Simeks, Periton Engineering, Ay Mashin Technology, Avbis, Spetsmorstroy, and Promenergo Avtomatika from the top-15 list are definitely linked with military production. Most of the sellers also have indirect links with Russian military entities through the aforementioned buyers.

**Figure 34: By producer (top-15), in $ million**




*Source: KSE Institute*

**Figure 35: By seller (2023, top-15), in $ million***

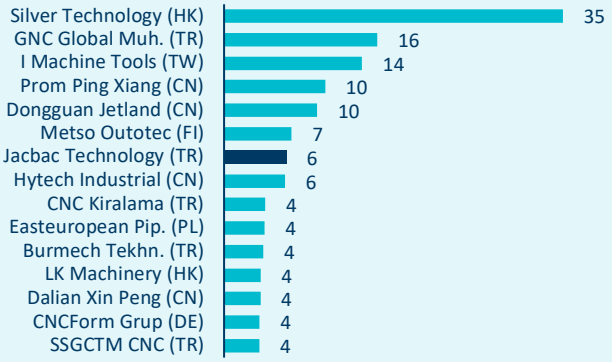
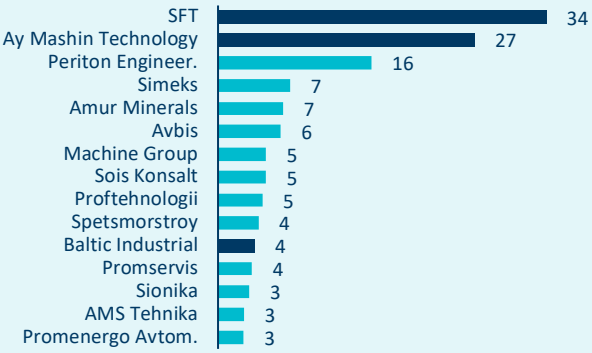



**Figure 36: By buyer (2023, top-15), in $ million***




*Source: KSE Institute *dark blue = sanctioned by U.S.*

## III. Next Steps: Strengthening the Export Controls Regime

Shortly after Russia's full-scale invasion of Ukraine in February 2022, a coalition of countries determined to halt the aggression implemented severe export controls on Russia and Belarus. The measures are unprecedented in scope as well as size of the targeted economy. They primarily focus on dual-use goods—items serving both military and civilian purposes—and apply across the entire economy, prohibiting the shipment of goods with potentially military applications to Russia while allowing the free flow of consumer goods into the country.

A noteworthy aspect of the export controls regime with regard to Russia is that the entire country is now subject to the U.S. Foreign Direct Product Rule (FDPR). Under this rule, dual-use goods produced outside of the United States but incorporating U.S. components, intellectual property, or software fall under the same restrictions as goods produced within the U.S. This marks only the second instance of the FDPR being applied to an entire country—previously, it had been aimed at Iran—and it turns the Russia case into a test of the U.S. FDPR's overall effectiveness.[26] [27] Furthermore, some countries, including the United States, have imposed additional export controls on Russia's military, essentially amounting to an embargo. While some of these measures have been in place since 2014, they had not been rigorously enforced until now.

Multilateral cooperation is absolutely critical for export controls implementation and enforcement with regard to Russia and Belarus, given that no single country possesses an absolute advantage with regard to products and technologies relevant to the Russian military. And it must be emphasized that many countries, including large economies such as China, do not participate in the sanctions regime, which poses key challenges. The current case marks the first instance since the end of the Cold War of a coalition of countries collectively applying an extensive set of export controls to undermine a country's industrial and military capacity.[28]

During the Cold War, the West regulated the export of strategic goods to the Soviet Union and its allies through the Coordinating Committee for Multilateral Export Controls (CoCom), which ceased operations in the early 1990s. Subsequently, multilateral agreements have primarily focused on military goods and issues related to nuclear non-proliferation. Specifically, the Wassenaar Arrangement established a voluntary export controls regime among member states to facilitate the exchange of information regarding the trade in conventional weapons as well as dual-use goods and technologies. Unlike CoCom, the Wassenaar Agreement explicitly emphasizes that its objective is not to restrict the export of controlled items to any specific state. Instead, all participants are regarded as equal partners and decisions are taken unanimously. Notably, Russia is a member of the agreement and also participates in other multilateral coordination groups.

Export controls have achieved partial success by forcing Russia to rely on more expensive supply routes and make do with lower-quality products.[29] However, authorities must remain vigilant in terms of policy design, implementation, and enforcement in light of critical loopholes and systematic circumvention efforts. As we show in this report as well as in our previous publication, Russia's military still depends on products from coalition countries and has maintained continued access to them.[30] Notably, during the first ten months of 2023, Russia imported $8.77 billion in battlefield goods, which have been identified by the European Union, U.S., and others as enforcement priorities—an increase of 20.5% compared to the corresponding period of 2022. For the broader set of critical components, total imports in January-October 2023 reached $22.29 billion (+4.8%).

---

[26] See "The New Russia Export Controls," Emily Kilcrease, CNAS.

[27] The FDPR has also been applied to a specific company (Huawei). See here.

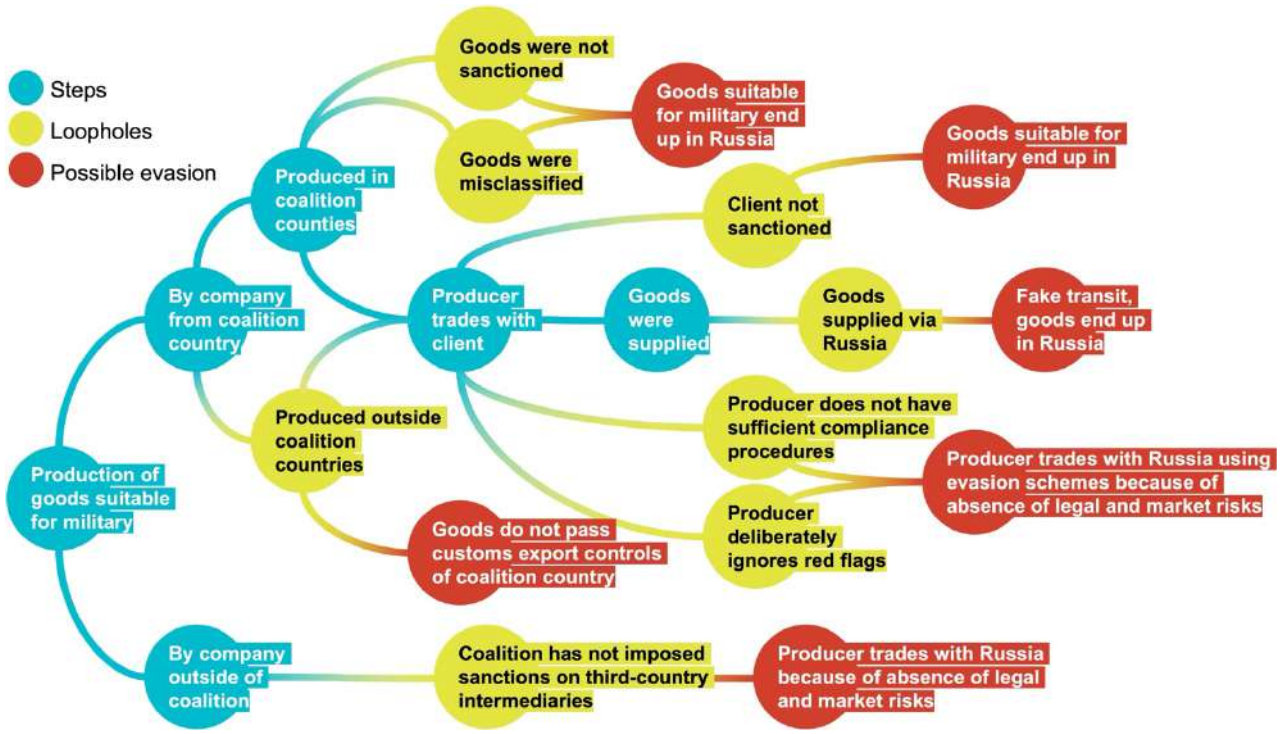
[28] See "Technology Controls Can Strangle Russia—Just Like the Soviet Union," Maria Shagina, Foreign Policy.

[29] See "Western Sanctions Are 'Beginning to Bite' Into Russia's Military, But not quite enough to check Russian President Vladimir Putin's war in Ukraine," Jack Detsch and Robbie Gramer, Foreign Policy, and "The shadowy network smuggling European microchips into Russia". Financial Times.

[30] See "Russia's Military Capacity and the Role of Imported Components," International Working Group on Russian Sanctions & KSE Institute, "Foreign Components in Russian Military Drones," International Working Group on Russian Sanctions & KSE Institute, and "Russia's War Machine Is Still Running on Western Equipment," Elina Ribakova, Barrons.

Export controls need to adapt and stay ahead of Russian efforts to circumvent them. Measures need to consider distinct challenges that exist on various stages of the supply chain and require very specific solutions. Figure 37 attempts to visualize the complexity of this undertaking. Export controls enforcement is hindered by several factors, including inadequate compliance efforts by entities located in coalition countries, the absence of sanctions imposed on third-country intermediaries engaged in export controls evasion schemes, inconsistent and/or insufficient regulations with regard to sanctioned items, and jurisdictional issues within the coalition.

**Figure 37: Map of export controls loopholes**




*Source: KSE Institute*

We propose the following steps in order to (1) close policy gaps in the existing exports controls regime; (2) strengthen government institutions tasked with its implementation and enforcement; (3) incentivize and empower the private sector to step-up compliance; (4) target circumvention schemes that allow Russia to import goods via third countries; and (5) improve multilateral cooperation in the field of export controls.

### *III.1. Closing Export Controls Policy Gaps*

While export controls imposed on Russia by Ukraine's allies are comprehensive in nature, there continue to be inconsistencies in the regime that allow for circumvention schemes and help Russia acquire dual-use goods. Thus, we believe that it is critical to **close policy gaps by aligning, simplifying, and expanding regulations** across jurisdictions. This includes addressing issues with licensing procedures and derogations. More broadly, we also need to take a closer look at regulations that define the reach of technology sanctions such as the Foreign Direct Product Rule in the U.S. In the Russia case, the standards for the application of U.S. export controls to manufacturing in third countries appear to be weaker than in other circumstances. And in other places such as the European Union, similar legal frameworks need to be established to address the large share of goods that never physically enter the jurisdiction of countries that have imposed restrictions.

1. **Align, expand, and simplify export controls.** Critical inconsistencies continue to exist within the Russia export controls regime, which hinder effective enforcement and allow for circumvention. In addition, we believe that important inputs for the Russian military industry are not yet export controlled. Ultimately, we propose to extend export controls to all critical components (see Appendix 2).

a. Export controls need to be harmonized across coalition jurisdictions. Although some progress has been made in this regard, including with the joint high-priority list of battlefield goods published by the EU, UK, U.S., and others, important differences persist. Adopting a centralized approach for developing dual-use goods lists will enhance the regulation of trade in critical goods and allow for better enforcement. We believe that it is critical to classify the same items as "dual use" in all coalition jurisdictions and to always include HS codes in the interest of more effective monitoring. In addition, while restrictions on Belarus have been strengthened and somewhat aligned with those regarding Russia, inconsistencies still exist, allowing Russia to import certain goods from coalition countries via its western neighbor and close ally.

b. The current focus on specific products leaves similar goods unregulated, allowing considerable room for circumvention schemes. Limitations to physical inspections of cargoes and the need for highly-specialized expertise with regard to export-controlled products (especially, advanced microelectronics) hinder the effective enforcement of narrowly-defined export controls. Using broader categories, at least on the six-digit HS code level—on which trade codes are standardized—would close loopholes and simplify implementation. Governments should also regularly review the list of export-controlled items—based on evidence from investigations of and new findings regarding foreign inputs to the Russian military industry.[31] [32]

c. Another key issue concerns increasing interlinkages between the traditionally separate civilian and military sectors of the economy—a development that we also observe with regard to China and that is actively facilitated by the government.[33] Thus, sanctions aiming to constrain military capacity need to also target non-military entities that play a crucial role in this regard. Overall, we see a need to expand and align measures already in place. For instance, the entire Russian military-industrial complex comprises about 1,500 individual enterprises, many of which are not subject to comprehensive restrictions, meaning that they are not sanctioned in all coalition jurisdictions or not sanctioned at all.[34] Exceptions from export controls, including for entities such as Rosatom, should be eliminated to prevent sales being redirected to the war effort. In the U.S., entity lists should also capture third-country subsidiaries of companies (see Box 3).[35] Furthermore, private actors should be mandated to investigate possible corporate ties of their counterparties to companies on the entity list.

2. **Enforce Foreign Direct Product Rule.** Given the large share of Russian imports of export-controlled goods produced on behalf of companies headquartered in coalition countries but manufactured and

[31] We also recommend that the EU strengthen and clarify its "principal elements rule" in Annex I of the EU Dual-Use Regulation, according to which an item that is not dual-use in nature but contains a component listed in the dual-use goods regulation may still be subject to export controls when the controlled component or components are the principal element of the goods and can feasibly be removed or used for other purposes. Specifically, provisions with regard to how this is determined appear too vague and discretionary and leave excessive room for misleading self-assessments by the exporter. It is also not entirely clear which authority is ultimately responsible for making the determination. We propose that the EU amend its regulations to impose export controls on any products containing dual-use items and establish clear minimum-content requirements.

[32] Coalition countries should also discontinue the production of any microelectronics enabled for use with Russia's GLONASS satellite navigation system.

[33] In July 2022, the Russian parliament enacted federal law No. 272-ФЗ ("On Amending Certain Legislative Acts of Russian Federation"), whereby businesses in Russia cannot refuse entering into governmental procurement contracts in general and military procurement contracts in particular, if they are deemed necessary by the government to ensure the conduct of foreign counter terrorism and other operations by the Russian armed forces. For the China angle, see "Military-Civil Fusion and the People's Republic of China," U.S. Department of State.

[34] See "Inconsistency in Action: A Case of Sanctioning the Russian Military Industry," NAKO.

[35] The entity list's approach to subsidiaries should at least by aligned with OFAC's 50% rule, whereby entities are considered blocked if they are owned by 50% or more, directly or indirectly, by one or more blocked persons.

shipped from other locations, it is crucial to ensure that export control provisions cover such scenarios. Currently, most countries lack explicit policies in this regard and/or improvements are needed.

a. In the United States, the focus should be on enforcement of the Foreign Direct Product Rule. The U.S. stands out in this regard as clear regulations exist that ensure export controls are applied to goods with significant U.S. contributions no matter where they are produced or traded. However, this report demonstrates that a notable portion of goods produced on behalf of U.S.-based companies find their way to Russia via intermediaries. Authorities appear to be lacking data for cross-checking voluntary corporate reporting to monitor FDPR compliance or conduct effective on-side checks. Furthermore, there is a possibility that certain aspects of the FDPR (e.g., application to production in Europe) have been diluted during negotiations with partners.[36]

b. There is some debate about the existence of FDPR-like regulations in other places. For instance, in the EU, the 11th sanctions package introduced restrictions regarding the intellectual property of EU persons or entities. The exact legal implications are unclear, however, and these EU measures certainly do not ensure the same extraterritorial application of export controls that the FDPR triggers (see Appendix 1). We believe that all export controls coalition countries need to establish regulations that ensure the application of restrictions to goods containing certain inputs, independent of where the actual manufacturing and/or sales take place.

3. **Review De-Minimis level for Russia.** We see a need to lower the De-Minimis threshold—the share of U.S. content that triggers the application of U.S. export controls—for all technology products going to Russia. Above this threshold, a BIS license is needed for items that contain components originating in the U.S. or containing U.S. technology. For dual-use goods exported to Russia, this threshold is 25%, while for Group E1 countries (e.g., Iran, North Korea, Syria), it is 10%. Recent China-related export control rules impose a 0% de-minimis requirement for lithography equipment.[37] Moreover, for items with satellite-related or military content going to, among other places, China and Russia, the threshold is 0%. We recommend a 0% De-Minimis level for all shipments to Russia. This would also send a strong message that Russia is being considered together with a group of countries that are under the most-stringent restrictions: Iran, North Korea, and Syria (country group E:1).

4. **Strengthen licensing process and limit derogations.** We acknowledge that certain derogations from export controls are required, such as for goods that have medical applications. However, the process needs to be rules-based, transparent, and harmonized across jurisdictions. For instance, in the European Union, export licenses apply across the common market, and companies may obtain them from those authorities that apply the least-strict standards (i.e., "license shopping").[38] Improvements are also needed in the United States.[39] We also propose that the EU remove certain grounds for

[36] See "Effectiveness of the FDPR," Emily Kilcrease, Thomas Krueger, and Elina Ribakova, CNAS (forthcoming). The US has waived the FDPR as far as the EU is concerned for dual-use items and certain advanced technology items. Please see here (p.26).

[37] See here.

[38] According to the EU's dual-use goods regulations, individual and global export authorizations are issued by the competent authority of the member state where the exporter is a resident or legally established as an entity. However, for multinational corporations with subsidiaries in different member states, it is still possible to take advantage of less-strict procedures for their issuance. Furthermore, there is no consistent, EU-wide list with regard to the documentation required for reviewing whether conditions for exemptions or derogations are met. Rather, such requirements are established by member state authorities and may include contracts, intergovernmental agreements, as well as self-declarations from the exporter.

[39] See "Challenging China's Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators", Emily Kilcrease, CNAS.

exemptions or derogations from export restrictions applicable to Russia as they represent important loopholes through which Russia continues to be able to import controlled goods.[40]

5. **Criminalize sanctions violations and establish negligence provisions.** Another element of a more consistent export controls regime concerns the criminalization of violations and clear definition of what negligence entails. We acknowledge the progress that is being made in the European Union with regard to the former[41] and urge policy makers to swiftly finalize new rules on the latter which are aligned with similar provisions in the United States.[42] Empowering enforcement agencies across coalition jurisdictions to penalize natural or legal persons not only if they *knew* but also if they *should have known* that their actions could result in a violation will address an important gap in the export controls regime. It will also play a key role regarding incentives for corporates to undertake proper due diligence.

### *III.2. Strengthening Government Institutions*

Export controls have played and will continue to play a crucial role in impeding Russia's access to dual-use goods. However, the scope of these measures is unprecedented and export controls are being imposed and implemented in an environment that is dramatically more complex in terms of supply chains than during the Cold War, when they gained prominence for the first time. Consequently, our institutions are not adequately prepared for the challenge, especially outside of the U.S., where experience with export controls is generally limited. Authorities in coalition countries currently lack the necessary resources to effectively implement and enforce the sanctions regime. Recognizing that export controls, especially on high-tech goods, represent a new frontier in economic statecraft and will only grow in importance, **strengthening capacities is paramount**. This goes beyond financial resources and staffing, but also involves addressing structural issues.

1. **Current institutional resources are insufficient for effective enforcement.** The existing Russia export controls regime presents a big challenge for those agencies tasked with its implementation. Specifically, we believe that the number of individual transactions—more than 800,000 for the battlefield goods subset in January-October 2023 alone—is too large to allow for the kind of comprehensive investigations needed to identify circumvention schemes and penalize violators. Since export controls are here to stay as a critical element of the economic statecraft toolbox, public sector capacity building is urgently needed to ensure their effectiveness and credibility in the medium to long term.

    a. United States: In the U.S., more than in other jurisdictions, enforcement structures for export controls already exist—as do those for the implementation of financial sanctions. However,

[40] See the Official Journal of the European Union here. Specifically, we believe that the following derogations should be removed from Council Regulation 833/2014 as they are the most vulnerable to manipulation: intergovernmental cooperation in space programs; civilian non-publicly available electronic communications networks; items aimed at ensuring cybersecurity and information security for natural and legal persons, entities and bodies in Russia; and items for the exclusive use of entities owned, or solely or jointly controlled, by a legal, person or entity which is incorporated or constituted under the law of member state or a partner country. We find the EU's approach towards cybersecurity and information security items particularly concerning as a competent authority may decide to grant a global export authorization (i.e., an authorization that may be valid for exports to one or more specific end users and/or in one or more third countries), which may also cover subsequent updates and/or upgrades.

[41] See the European Commission's statement from December 12, 2023, here. "The new rules will include a list of criminal offences related to the violation and circumvention of EU sanctions, such as for example (...) providing prohibited or restricted economic and financial services (...). The new rules will also establish common basic standards for penalties for both natural and legal persons, including imprisonment of at least five years for certain offences and enhanced rules on freezing and confiscation of proceeds and assets subject to EU sanctions."

[42] Generally, under U.S. law, the definition of "knowledge" (including variations such as "know", "reason to know," or "reason to believe") in the context of export controls denotes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts. See here. As to the threshold of knowledge in EU law, Article 12 of Council Regulation (EU) No. 833/2014 prohibits "knowingly and intentionally" participating in activities the object or effect of which is to circumvent restrictive measures.

these agencies do not possess the financial and human resources to address challenges emerging from the much broader scope of modern-day export controls.[43]

b. European Union: The current approach in the EU of leaving sanctions implementation to the member states will not be able to cope with the increasingly complex challenges related to 21st century sanctions regimes. Export controls have turned out to be particularly challenging due to the jurisdictional questions arising from transactions that do not involve the physical transport of goods through coalition countries. As a result, customs services—which generally possess considerable resources—have little or no role to play. With regard to agencies able to monitor corporate compliance and financial transactions, the European landscape is fragmented at best.

c. United Kingdom: We see the recent announcement in the UK related to the establishment of OTSI—a new agency tasked with implementation of trade sanctions, including export controls—as an encouraging development.[44] OTSI (Office for Trade Sanctions Implementation) will focus on measures that go beyond the traditional auspices of OFSI (Office for Financial Sanctions Implementation) and specifically deal with companies that are avoiding sanctions.

2. **Capacity building to also include technological solutions.** While certainly a complex undertaking, it may be technologically possible to set up systems for the tracking of goods throughout the supply chain. Such efforts should start with larger items but can ultimately extend to small-scale components such as semiconductors and other microelectronics. This should also include mandatory implementation of tamperproof identifiers such as serial numbers as these have been found to be erased in many recent cases of weapons found on Ukrainian territory. In addition, systems could be implemented to remotely disable items should they somehow make their way to Russia. This would address one of the key challenges of export controls enforcement: to act in time before the goods reach their destination.

### *III.3. Bolstering Corporate Responsibility*

We believe that our findings illustrate a key weakness of the existing export controls regime insofar as the private sector, especially non-financial corporates, does not play a big enough role in its implementation. That a substantial share of the dual-use goods that Russia has been able to import in recent months are products of companies based in export controls coalition jurisdictions illustrates that internal procedures have not been adequate to monitor and control supply chains. We advocate for **improved compliance efforts within the corporate sector** akin to those taken by the financial industry regarding issues such as anti-money laundering (AML) and anti-terrorist financing. Cleaning up distribution networks is certainly a resource-intensive task for corporations. Governments will need to create proper incentives by demonstrating the ability and willingness to investigate transactions and impose meaningful penalties, provide clear guidance to the private sector, and create a legal framework that allows corporates access to the information needed for proper due diligence. Strengthening enforcement and compliance is vital to maintain the effectiveness of sanctions.[45]

1. **Alter corporates' incentive structure through investigations and fines.** To enhance corporate accountability, we propose to modify incentive structures by authorities' demonstrating both willingness and ability to investigate dual-use goods-related transactions and impose significant monetary penalties in the case of export controls violations. Currently, companies engaged in the trade with such goods lack sufficient motivation for undertaking compliance efforts that effectively address the circumvention patterns we have documented above. The complexity of supply chains makes this a quite challenging undertaking—but it also illustrates why coalition country-based corporates are so crucial for better enforcement. Once a good has been sold by these companies to an intermediary, it becomes increasingly difficult to trace its whereabouts and ensure that it doesn't reach Russia.

[43] See "Want to Help Ukraine? Fund This U.S. Government Agency," Emily Benson, Foreign Policy.
[44] See the UK government's public statement on the establishment of OTSI here.
[45] See "Economic sanctions risk losing their bite as a US policy weapon," Elina Ribakova, Financial Times.

a. Given the multi-jurisdictional nature of the trade in export-controlled goods, coalition authorities should closely collaborate on investigations. Transparency is crucial and information on ongoing inquiries, enforcement decisions, and fines should be publicized, if possible, without jeopardizing investigations and legal proceedings. This would demonstrate a clear commitment to uncovering and penalizing of sanctions violations and clearly communicate to the private sector that the risk of discovery is real. Without it, businesses will not be properly incentivized to comply.

b. Penalties imposed by authorities on corporates should be increased as well. They need to be proportional to the profits generated by the underlying illicit transactions in order to have a deterring effect. Similarly, settlements with corporates—often the outcome of legal proceedings related to sanctions violations—should include significantly higher amounts (see Box 4). Only sufficiently-severe consequences—monetary or otherwise—, together with a bigger risk of their materializing, will change businesses' risk calculations when it comes to compliance.[46] Overall, we propose that all coalition jurisdictions criminalize sanctions violations and urge governments to consider prosecution for aiding and abetting war crimes in certain cases (see Box 5).

c. A key overall challenge of sanctions-related incentives is that legal proceedings are notoriously slow, often taking many years before a final decision/settlement is reached and penalties materialize.[47] This approach to sanctions enforcement is ill-suited for an active war, where the compromised effectiveness of restrictive measures directly results in death and destruction. We strongly urge coalition authorities to consider the application of provisional penalties, in particular with regard to the suspension of licenses and similar steps. A more proactive approach could meaningfully reduce the flow of export-controlled goods to Russia.

d. Another critical part of a proper incentive structure is to clearly define the procedural steps that participants in the trade with dual-use goods have to conduct as part of due diligence efforts. We believe that this should include mandatory periodic post-execution investigations of distribution companies. While major microelectronics producers occasionally conduct such inquiries, for instance meetings with registered end users or inspections of storage facilities, they only do so on a case-by-case basis, typically in response to obvious red flags. In our view, it is reasonable to assume that many illicit transactions escape such procedures. To address this gap, we propose mandating regular inspections for all transactions involving export-controlled goods and end-users from high-risk jurisdictions (as defined and regularly reviewed by authorities).

2. **Apply lessons from the financial industry regarding "know-your-client" practices.** While supply chain complexity represents a challenge, the financial sector has demonstrated that such issues can be overcome. Specifically, financial institutions have developed effective compliance structures in recent years, incorporating processes like "Know Your Client" (KYC) and understanding their clients' clients. Notably, regulators have compelled entities to adopt such systems and facilitated information sharing, particularly in areas such as anti-money laundering (AML). Non-financial corporates should learn from these experiences in the export controls field, and authorities should make adjustments to the legal framework to mandate proper due diligence procedures and permit the exchange of information for this purpose. This will significantly enhance accountability and risk management.

3. **Provide the private sector with clear guidance on export controls.** To alleviate the impact of stepped-up compliance requirements, authorities need to provide explicit guidance to all participants in the

[46] In particularly serious cases, U.S. export controls agencies have the authority to deny export privileges to companies incorporated in the United States. In the EU, EU Regulation 2021/821 allows to annul, suspend, modify, or revoke a previously-granted export authorization.

[47] For example, the plea settlement and imposition of penalties in the ZTE Technologies case (see Box 6) were the result of a five-year investigation and the activities in question actually took place between 2010 and 2015. Financial penalties were ultimately imposed in 2017 and ZTE deprived of export privileges in 2018 – only after repeated export controls violations had been discovered.

trade involving export-controlled goods. This guidance should clearly define the products in question (using HS codes), outline mandatory procedural steps, specify exceptions from the sanctions regime, and detail any reporting obligations. The simplification of export control regulations discussed above would not only enhance enforcement by implementing agencies but also simplify compliance for private sector entities. Authorities can also advise as to the use of latest technologies (e.g., artificial intelligence) in identifying "red flags" with the objective of reducing compliance costs.[48]

4. **Advocate for and support capacity building in the private sector.** While larger companies often possess dedicated compliance departments to ensure proper due diligence, this is not necessarily the case for all entities involved in the production, sale, or shipment of export-controlled goods. Although most battlefield goods and critical components ultimately come from large multinational corporations, smaller entities are often involved in their distribution. Authorities should engage with SMEs to advocate for and support capacity building throughout the supply chain. For smaller entities, clear guidance regarding the scope of export controls, exceptions, legal requirements, etc. is particularly important.

5. **Engage the financial industry in tracking of transactions.** As mentioned above, financial institutions have considerable experience with compliance efforts in fields such as AML and anti-terrorist financing. We believe that due diligence procedures related to export controls face similar challenges—opaque ownership structures, frequent institutional changes, and reliance on less-strict jurisdictions—and would benefit from leveraging banks' expertise. Utilizing existing frameworks (e.g., AML), coalition authorities can strengthen enforcement efforts, particularly where the tracing of structures and activities in third countries are concerned. And, importantly, relying on the financial transactions-side of this trade, it may be possible to stop certain goods from reaching Russia in the first place. Modifications to the legal framework are critical to grant financial institutions access to additional information, including details about the specific goods involved in transactions outside of trade financing, where they are already available. Currently, a lack of information is constraining their ability to leverage existing procedures.

6. **Establish a database of business partners to simplify compliance efforts.** Companies engaged in the trade with export-controlled goods would benefit from a database containing information about potential business partners. It should include details about company structures, beneficial ownership, related parties, coverage by sanctions, and any previous sanctions violations. We believe that the individuals behind intermediaries need to be a major focus of compliance efforts. While new entities can be established with relative ease in many jurisdictions—resulting in a "cat and mouse" game between sanctioning authorities and circumventors—the individuals behind them represent a real constraint. Ensuring convenient and timely access to this information would lower the cost of companies' due diligence procedures, particularly for SMEs. Governments should support the establishment of such a database, including by creating the necessary legal framework for information sharing.

#### *III.4. Targeting Third-Country Circumvention*

While the Russia export controls are unprecedented in their scope, not all countries have aligned themselves with the measures. These jurisdictions play a key role for Russia's continued ability to import goods that it needs for its military industry. In many cases, battlefield goods and critical components *neither* physically pass through export controls coalition countries *nor* are entities from these jurisdictions involved in the transactions. Strengthening of export controls therefore also requires **targeting third-country intermediaries** with coercive measures, while also reaching out to the public and private sectors to improve cooperation. Should evasion

[48] In March 2023, the U.S. Department of Commerce, Department of the Treasury, and Department of Justice published a so-called Tri-Seal Compliance Note titled "Cracking Down on Third-Country Intermediaries Used to Evade Russia-Related Sanctions and Export Controls." The note describes red flags that indicate attempts to circumvent export controls. This list can be supplemented based on recently-established regulations related to the export of advanced microchips to China. For example, companies should closely monitor instances where the good in question is typically, predominantly, or often used in the production of military items, but the customer makes representations that this is, in fact, not the case.

efforts turn out to be systemic in nature—and the aforementioned measures insufficient to address existing challenges—broader trade restrictions should be considered to deprive Russia of alternative supply routes.

1. **Sanction third-country entities.** Sanctions, including asset freezes and transactions bans, should be imposed on companies that are found to have violated export controls. As this concerns entities located outside of the immediate jurisdiction of coalition countries, such measures may go beyond *primary* sanctions. For instance, restrictions on a Russian company require entities or individuals within the imposing countries to comply with the measures, but do not impact third-country intermediaries. However, there are legal mechanisms through which those can be reached as well.

    a. United States: U.S. authorities have considerable experience with the extraterritorial application of sanctions, or so-called *secondary* sanctions. Their effectiveness is fundamentally a function of the critical importance that access to the U.S. market and financial system plays for many businesses around the world. When imposing secondary sanctions, authorities make continued access to both conditional on compliance with U.S. sanctions, which, in most cases, does not leave actors with any real choice but to comply. For example, European companies were forced to abandon business ties with Iran after the U.S.'s departure from the Iran nuclear deal in 2018 despite the fact that their own governments were still party to the agreement. Similarly, companies involved in the construction of Nord Stream 2 ended their activities following the imposition of secondary sanctions by the U.S. Congress starting in 2017.[49]

    b. European Union: While the EU considers secondary sanctions contrary to international law and prohibits companies from complying with such measures via its blocking statute[50], the 11th sanctions package, agreed upon in June 2023, has created a new mechanism through which third-country entities can be reached.[51] This anti-circumvention tool allows the EU to impose restrictions on companies that have been found to violate EU sanctions—and, if such measures are deemed to be insufficient to stop the flow of export-controlled goods, to restrict the sale, supply, transfers, or export of sanctioned goods and technology to certain third countries who are considered to represent a continued and particularly high risk of circumvention.[52]

2. **Restrict exports to countries with systemic problems.** If it is not possible to reach individual actors involved in export controls violations with sanctions, broader restrictions should be considered.

    a. Export quotas: They could take the form of quotas, where exports of specific goods to specific countries that surpass benchmarks from the pre-full-scale invasion period are prohibited—or are, at least, subject to increased scrutiny.[53] Such measures could help address the issue of transshipments via countries where entities may be beyond the reach of sanctions.

    b. Export bans: Should quotas prove to be insufficient to stop the flow of export-controlled goods to Russia, the coalition should consider banning exports of specific goods to specific countries in their entirety. As mentioned above, the European Union, with its anti-circumvention tool, has established a mechanism that would allow it to do so if systematic issues are identified.

[49] For more information about U.S. sanctions on companies involved in the construction of North Stream 2, see here.

[50] See "Countering economic coercion: How can the European Union succeed?," Elina Ribakova and Benjamin Hilgenstock, CEPS.

[51] See the Official Journal of the European Union here.

[52] This measure is stated to be an exceptional and last-resort option, and, so far, the EU has not made use of it. The EU should also ensure that restrictive measures apply to third-country subsidiaries of EU-based entities. Currently, the EU states (see Question 34 here) that such subsidiaries are governed by the respective host state. Only if a subsidiary's decision was approved by an EU parent company, the situation would be different.

[53] We acknowledge that a full ban of exports will likely not be a practicable solution for countries that play an integral role in global supply chains for electronics, e.g., China. In such cases, authorities should target specific intermediaries instead.

c. Market access: Countries refusing to assist in the implementation of export controls could be denied access to markets of coalition countries, while those that are found to cooperate closely could receive preferential treatment when it comes to such issues.

d. Expanded in-use checks: Authorities should significantly expand checks in third countries to send a message to participants that violations of contractual terms with regard to the use of the goods (e.g., by on-shipment to Russia) are being investigated and will be discovered.

3. **Engage public and private sector in third countries.** The export controls coalition should continue to reach out to authorities as well as businesses in third countries to improve compliance with the sanctions regime. Some key deliverables are political commitments to stop export controls violations and circumvention efforts, initiatives to improve the sharing of information (e.g., third-country trade data) with coalition governments, efforts to strengthen administrative capacities (e.g., within third-country customs services), and the provision of technical assistance to third-country private sector entities.

### *III.5. Improving Multilateral Cooperation*

The complexity of global supply chains and scope of modern-day export controls will also require **improved cooperation across jurisdictions**. Otherwise, gaps in the sanctions regime—and its enforcement—will always allow circumvention at a scale that renders restrictions ineffective and erodes their credibility. We believe that better exchange of information is one key to making the system work better, in particular as the ultimate objective of export controls is to stop shipments of dual-use goods to Russia before they occur. But more fundamentally, if technology sanctions are truly the new frontier in economic statecraft, more permanent structures may be needed, for instance in the form of multilateral export controls treaties.

1. **Improve exchange of information.** In addition to capacity building, an efficient and timely exchange of information is also needed. Comprehensive and timely transaction data, especially for sensitive trade involving critical military or dual-use components, should be shared among coalition countries. There is a wealth of information available to monitor such trade, including publicly-available data but also going way beyond. If this information is properly utilized, it would allow for an in-depth understanding of how Russia continues to be able to acquire critical components for its military production—and to identify enforcement priorities. Effective information sharing should also provide opportunities for the academic and think tank community to provide data and findings.

2. **Undertake joint investigations.** Coalition authorities need to cooperate closely when it comes to investigations of export controls violations due to the multi-jurisdictional nature of the trade in critical components. Authorities must proactively monitor developments—leveraging all available data sources—to identify evolving schemes and react to adaptation strategies.

3. **Enter into multilateral export controls treaty.** Currently, multilateral export controls on conventional weapons, dual-use goods, and technology are regulated by the Wassenaar Arrangement (see Box 7). However, this approach—originally instituted to replace the Cold War-era Coordinating Committee for Multilateral Export Controls (CoCom) and bring Russia to the table—has not been able to fulfill its mandate and respond to current geopolitical challenges. In 2022, it failed to update regulations on microelectronics and other critical technologies—reportedly due to Russia's veto. Therefore, there is a need to establish a binding, multilateral export controls regime, where participating countries can promptly react to security threats—including those posed by Russia and China. Importantly, any multilateral system should allow the suspension of a member's vote on issues related to its own conduct if it reaches the threshold of breaches of international law or human rights violations.

### Box 3. Listing Subsidiaries: SenseTime

In 2019, the BIS added Chinese facial recognition technology developer SenseTime to the EAR Entity List. Reports had indicated that the company's patent filing suggested an ability to distinguish between Uyghur and non-Uyghur individuals, allowing the identification of the former in a crowd. As a result of the listing, shipments to the company required a license, which could be granted with conditions or denied. Shortly after, however, SenseTime directly acquired advanced chips through unlisted subsidiaries. In fact, the company maintains that the BIS designation had minimal to no impact on its business.

The latest round of China semiconductor export controls specifically addresses this loophole. The newly adopted Advanced Chips Rule imposes a worldwide licensing requirement based on the identity of the end user, necessitating licensing for all countries other than those listed in Country Groups D:1, D:4, or D:5 when destined to an entity that is headquartered in, or whose ultimate parent company is headquartered in certain areas. The Advanced Chips Rule does not define the terms "headquartered in" or "ultimate parent company," however, the BIS has requested comments on the definitions of these terms.

We suggest expanding the EAR Entity List to include all subsidiaries or affiliates known to U.S. authorities. Exporters of controlled goods should be obligated to conduct due diligence to identify other subsidiaries.

### Box 4. Illicit Gains vs. Financial Penalties: Microsoft Settlement

In April 2023, OFAC and the BIS reached a settlement with Microsoft concerning the company's violations of export controls related to Russia and other sanctioned jurisdictions, under which the company agreed to pay **$3.3 million**. This is not only a negligible sum in the context of Microsoft's operations, but also only a fraction of the illegal transactions' value. The violations, which took place over a seven-year period, concerned the export of software and services to sanctioned persons, entities, or countries worth **$12 million**. This case illustrates why former law enforcement officials and industry practitioners believe that companies often see penalties for sanctions and export controls violations simply as the cost of doing business.

Aside from the broader issue of illicit gains vs. financial penalties, the Microsoft settlement case is pertinent to this report's policy recommendations for several reasons:

- While Microsoft sold software licenses, activated software licenses, and/or provided related services to sanctioned persons or entities in several countries, including Cuba, Iran, and Syria, most violations involved blocked Russian entities or persons located in the Crimea region of Ukraine.
- According to OFAC, violations by Microsoft were caused partially by a lack of complete or accurate information on the end users of the company's products, especially in cases where final sales were made by intermediaries and Microsoft failed to obtain information from distributors/resellers.
- At times, Microsoft Russia employees appear to have intentionally circumvented internal screening controls to prevent other Microsoft affiliates from discovering the identity of end users. For example, following OFAC's 2014 designation of Stroygazmontazh, a Russian company operating in the oil and gas industry and Microsoft's initial rejection of one of this entity's subsidiaries as a potential customer, certain employees successfully used a pseudonym to arrange orders on behalf of the SDN.
- Furthermore, there were shortcomings in Microsoft's restricted-party screening. For example, when Microsoft Ireland was made aware of the end user by a distributor or reseller, internal systems did not ensure company-wide and cross-database access to information such as names, addresses, and tax identification numbers. In a number of cases Microsoft also failed to timely screen and evaluate pre-existing customers following changes to OFAC's SDN List and implement corrective measures to avoid continued dealings with SDNs or blocked persons.
- Microsoft's screening also did not identify blocked parties not specifically listed on the SDN List, but owned 50 percent or more by SDNs, or SDNs' Cyrillic or Chinese names, even though many customers in Russia and China supplied order and customer information in their native scripts.

### Box 5. Human Rights Violations: Doe vs. Cisco Systems

In July 2023, the U.S. Ninth Circuit court allowed human rights claims brought against Cisco by Chinese human rights activist groups to proceed. The plaintiffs are practitioners of Falun Gong, a religion originating in China in the 1990s, and allege that they or family members were victims of human rights abuses committed by the Chinese Communist Party and Chinese government officials. Importantly, they claim that these abuses were enabled by technological assistance from Cisco Systems and two Cisco executives. According to the plaintiffs, the surveillance and internal security network Golden Shield was designed and implemented in the United States and maintained with the help of Cisco Systems from U.S. territory. Furthermore, technology manufactured by Cisco such as integrated circuit chips played a key role in Golden Shield.

This case is of importance for the current situation regarding Russia as these goods, technologies, or services were not under sanctions at the time of the relevant contracts. Although U.S. law in this area will not be fully settled until the Supreme Court rules on the matter, the Ninth Circuit case articulates certain important principles applicable to possible future claims against U.S. technological companies:

- Aiding and abetting human rights violations is a violation of international law that is actionable in U.S. courts under the Alien Tort Statute (ATS). Aiding and abetting cases can also be brought against company executives under the Torture Victim Protection Act and it might be possible to extend the court's logic to the War Crimes Act of 1996.
- The court rejected Cisco's argument that customary international law requires that a defendant's conduct was "specifically directed" toward the commission of a crime, Instead, the court found that knowledge, rather than purpose, satisfies the mens rea requirement for aiding and abetting. The court stressed that U.S. government entities and news media widely reported on the torture and detention of Falun Gong adherents in China.
- The court also rejected Cisco's assertion that the technology it provided could have been used lawfully, so Cisco's assistance cannot be considered to have a substantial effect on the commission of illegal activity. The court stated that actions that are not themselves criminal can lead to aiding and abetting liability, depending on the circumstances.

### Box 6. Repeated Violations after Initial Penalty: ZTE Corporation

In 2017, ZTE Corporation, China's largest telecommunications equipment company at the time, entered into a plea agreement with the U.S. Department of Justice and settlement agreements with the BIS and OFAC for violations of U.S. sanctions and export controls with regard to Iran, as well as making false statements to the U.S. government and obstruction of justice. The combined civil and criminal penalties payable by ZTE under the charges brought by several authorities amounted to a record $1.19 billion.

ZTE had either or indirectly shipped U.S.-origin items worth approximately $32 million to Iran between January 2010 and January 2016. While doing so, ZTE had packaged the items together with self-manufactured ones to hide their origin. The company also did not include the U.S. items on customs forms although they were noted on packing lists inside the shipments. Finally, to insulate itself from civil or criminal liability in the U.S., ZTE had established new "isolation companies" which were to enter into contracts with Iranian customers.

In January 2016, ZTE was placed on the BIS entity list but its export privileges were later restored via a series of temporary licenses. Under the 2017 settlement agreement with the BIS, ZTE was also placed under a three-year period of corporate probation, during which an independent corporate compliance monitor would review and report on ZTE's export controls compliance program. In March 2017, a denial of export privileges was imposed on ZTE for a period of seven years but later suspended subject to probationary conditions.

In 2018, the BIS discovered that ZTE had failed to comply with certain conditions of its probation and, in fact, submitted false letters to the agency in order to conceal these violations. They included failures to review some of the company's practices and penalize employees responsible for prior misconduct. Some of these violations occurred during the settlement negotiations in 2016 as well as the subsequent probation period. Upon discovery, the BIS activated a previously-suspended export denial order in full and removed export privileges for ZTE until March 2025.

The ZTE case demonstrates that certain companies continue to engage in the trade with controlled items and sanctioned jurisdictions and/or violate previously-reached settlements with authorities even after paying considerable financial penalties. Thus, in a case of an ongoing war, measures amounting to a denial of export privileges are needed as soon as information related to the export of controlled items to aggressor states becomes known to authorities.

## BOX 7. LOOKING AHEAD: MULTILATERAL EXPORT CONTROLS

Most national export controls regimes are based on four multilateral frameworks that establish common control lists and practices for participating jurisdictions: the Wassenaar Arrangement (42 members), the Nuclear Suppliers Group (48 members), the Australia Group (43 members), and the Missile Technology Control Regime (35 partners). Russia is a member of three of the four regimes and plays the same destructive role in the decision-making process as it does in the UN Security Council.

***The Wassenaar Arrangement***

The Wassenaar Arrangement establishes a voluntary export controls regime among member states, who exchange information on transfers of conventional weapons and dual-use goods and technologies. Unlike the Cold War-era Coordinating Committee for Multilateral Export Controls (CoCom), the agreement does not aim to limit exports of controlled items to any specific state – or impede bona fide civil transactions; rather, all participants are treated as equal partners and all decisions are adopted unanimously.

The Wassenaar Arrangement is "intended to enhance co-operation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behavior of a state is, or becomes, a cause for serious concern to the Participating States". In the wake of the 9-11 terrorist attacks against the United States, the mandate of the Wassenaar Arrangement was expanded in 2001 to include the prevention of the acquisition of conventional arms, dual-use goods, and technologies by individual terrorists, terrorist group, and terrorist organizations. Further, the Arrangement includes specific information exchange requirements: the states are obligated to submit, on a semi-annual basis, notifications of arms transfers, covering seven categories based on the UN Register of Conventional Arms. Members are also required to report transfers or denials of transfers of certain controlled dual-use items.

Although the Wassenaar Arrangement seems somewhat informal and establishes only voluntary export controls, most states base their national legislation on Wassenaar documents. Specifically, the EU lists of controlled items mirrors that of the Wassenaar system and revisions to the EU list are made to align its list with the Wassenaar-approved list. Only the U.S. goes beyond the goods agreed within the Arrangement.

***Shortcomings of Wassenaar***

- Revisions to the policies and lists of control items happen only once a year at a plenary meeting in December. There is no procedural possibility to adopt policy documents on a rolling basis when circumstances require such intervention.
- The Wassenaar Arrangement was instituted in the 1990s to prevent the proliferation of WMDs; however, it is not capable of addressing modern security challenges posed by disruptive technologies. This failure is to a significant extent caused by Russia's veto.
- The agreement was partly established to bring Russia to the table and build partnerships. As Russia's repeated gross violations of international law in Georgia, Syria, across Africa, and in Ukraine demonstrate, Russia can no longer be treated as a reliable partner. And Wassenaar is clearly not able to deliver on its mandate to "prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behavior of a state is, or becomes, a cause for serious concern to the Participating States".
- To make matters worse, the Wassenaar Arrangement provides for certain information sharing and reporting requirements that is likely to give Russia access to sensitive information related to other states' defense capabilities.

***Russia's destructive role***

As a member of Wassenaar Arrangement, Russia blocks decisions that would regulate trade in sensitive technologies essential for its war on Ukraine. This behavior mirrors Russia's actions on the UN Security Council, where it has used its right to veto more often than any other permanent member, oftentimes to exonerate itself from international responsibility. Most recently, at the December 2022 plenary meeting, Russia blocked the adoption of an updated dual-use goods list aimed to reflect current technological developments. As a result, respective lists of around 40 states, many of whom are leading technology exporters, will likely continue to have important loopholes. Specifically, Russia blocked updates of controls on microelectronics, emerging and foundational technologies, and other items of strategic concern, which were informally agreed by allied producer countries. Neither the U.S. nor other allies of Ukraine appear to have made any serious effort to exclude Russia from the Wassenaar Arrangement.

***A new multilateral treaty***

A new model can be partly based on the Coordinating Committee for Multilateral Export Controls (CoCom), which was an informal multilateral organization where Western allies coordinated national controls applied to the export of strategic materials and technology to the USSR and its partners. A new binding multilateral framework should govern export controls of arms, dual-use goods, and sensitive technology with regard to Russia, China, and other states found to be perpetrators of gross human rights violations or to violate the prohibition of aggression under the UN charter. Foundational documents should allow the suspension or exclusion of a member state's voting rights regarding issues related to its conduct in cases when such a state was found to violate Article 2 (4) of the UN Charter by the UN General Assembly.

## APPENDIX 1: SUMMARY OF EXISTING EXPORT CONTROLS MEASURES

**United States**

On 24 February 2022, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) amended the Export Administration Regulations (EAR) to apply strengthened export control rules to Russia and Belarus including extended scope of the Foreign Direct Product (FDP) Rules. The EAR applies extraterritorially to items subject to the EAR and "follows the goods" anywhere in the world. The EAR regulates exports, re-exports, and in-country transfers of covered items globally, even if a transaction does not involve U.S. entities and takes place outside the U.S. Items subject to the EAR can include: items anywhere in the world produced or manufactured in the U.S.; items in or exported from the U.S., regardless of where they were manufactured; items manufactured outside the U.S. that include more than de minimis of controlled U.S.-origin content; items manufactured outside the U.S. that are the direct product of certain controlled U.S. technology or software, or are manufactured by a plant, or a major component of a plant, that is itself a direct product of such technology or software.

Therefore, an EAR license is required for the export, re-export, or transfer (in country) of all items subject to the EAR with Export Control Classification Numbers (ECCNs) on the Commerce Control List (CCL) to or within Russia and Belarus when the parties know, or have reason to know, that a foreign-produced item meeting the direct product criteria destined for Russia or Belarus or will be incorporated into or used for production/development of parts, components, or equipment that is produced in or destined for Russia or Belarus unless a license exception applies. License applications are subject to a policy of denial. In February 2022, the BIS issued a statement clarifying how the FDPR applies to Russia and Belarus.[54] In February 2023, a new Iran Foreign Direct Product Rule was published to address the use of Iranian unmanned aerial vehicles by Russia in its war against Ukraine.

BIS has five lists of parties of concern: (1) Denied persons list—a list of individuals and entities that have been denied export privileges; (2) Entity Llist—a list of foreign parties that are prohibited from receiving some or all controlled items unless export license is granted. License applications in this case are normally subject to policy of denial; (3) Unverified List—a list of parties whose bona fides BIS has been unable to verify. No license exceptions may be used for exports, reexports, or transfers (in-country) to unverified parties; (4) Military End User List—a list of foreign parties that are prohibited from receiving controlled items unless export license is granted. The Military End User List is not exhaustive, and, according to BIS position exporters, re-exporters, or transferors must conduct their own due diligence for entities not identified as military end users; (5) Consolidated Screening List—a searchable and downloadable file that consolidates export screening lists of the Departments of Commerce, State and the Treasury into one document.

In June 2022, BIS announced the reformed and enhanced administrative enforcement program, whereby, on February 16, 2023, the Department of Justice (DOJ) and Commerce Department announced the creation of the Disruptive Technology Strike Force with a mission to prevent nation-state "adversaries" including Russia from acquiring "disruptive" technologies. The strike force will bring together the DOJ's NSD, BIS, the Federal Bureau of Investigation, Homeland Security Investigations, and 14 US Attorneys' Offices in 12 metropolitan regions. According to the official press release, the strike force's work will focus on investigating and prosecuting criminal violations of export laws, enhancing administrative enforcement of U.S. export controls, fostering partnerships with the private sector, leveraging international partnerships to coordinate law enforcement actions and disruption strategies, utilizing advanced data analytics and all-source intelligence to

[54] "To restrict Russia and Belarus' abilities to acquire certain foreign-produced items, the Russia/Belarus FDP rule establishes a control over foreign-produced items that are: (i) the direct product of certain U.S.-origin software or technology subject to the EAR; or (ii) produced by certain plants or major components thereof which are themselves the direct product of certain U.S.-origin software or technology subject to the EAR. This control applies when it is known that the foreign-produced item is destined to Russia or Belarus or will be incorporated into or used in the production or development of any part, component, or equipment produced in or destined to Russia or Belarus" U.S. Department of Commerce & BIS Russia and Belarus Rule Fact Sheet.

develop and build investigations, conducting regular trainings for field offices, and strengthening connectivity between the strike force and the Intelligence Community.

In June 2023, it was announced that the U.S. and its partners in the Five Eye initiative—Australia, Canada, New Zealand, and the United Kingdom—will formalize coordination and information sharing on export controls enforcement to restrict Russia's access to technologies. Additionally the U.S. established a framework of allied partner export controls against Russia and Belarus, which includes 38 jurisdictions such as EU member states, the U.K., and Taiwan. According to Supplement No. 3 to Part 746,the listed countries have committed to implementing substantially similar export controls on Russia and Belarus under their domestic laws and are consequently excluded from certain requirements of U.S. export controls.

**European Union**

In the EU, export control rules are provided by both EU legislation and member state regulations stipulated at a national level. Export control rules are enforced at the national level, leading to certain variations in their practical application. The general framework for dual-use export controls in the EU is provided for by the EU Dual-Use Regulation. It stipulates EU-wide rules that are directly applicable in all EU member states, including controls on specifically listed dual-use items and in respect of exports relating to controlled end use, as well as general provisions for granting individual and global export licenses ("authorizations''). As to enforcement, the dual-use regulation instructs Member States to take appropriate measures to ensure proper enforcement, including penalties that are effective, proportionate and dissuasive. Export controls in relation to military Items are controlled by EU member states individually. There is an EU common military list, which is adopted annually by the Council, pursuant to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment. However, this list is non-binding, and it is within the competence of the member states to legislate for national military export controls.

Specific export restrictions with regard to Russia are set forth by Council Regulation (EU) No. 833/2014, which stipulates restrictions on the sale, supply, transfer, or export of a large number of listed items to any natural or legal person, entity or body in Russia or for use in Russia. The covered items include: dual-use items as listed in Annex I to Regulation (EU) No. 2021/821 of the European Parliament and of the Council (EU Dual Use Regulation); energy-related items as listed in Annex II to Council Regulation (EU) No. 833/2014; items "which might contribute to Russia's military and technological enhancement, or the development of the defense and security sector" as listed in Annex VII to Council Regulation (EU) No. 833/2014; products for use in oil refining and liquefaction of natural gas as listed in Annex X to this Regulation; items aimed for use in aviation or the space industry as listed in Annex XI to this Regulation; maritime navigation and radio-communication items as listed in Annex XVI to this Regulation; luxury goods as listed in Annex XVIII to this Regulation (items valued above EUR 300 per item); jet fuel and fuel additives as listed in Annex XX to this Regulation; an extensive list of items "which could contribute in particular to the enhancement of Russian industrial capacities" as listed in Annex XXIII to this Regulation; banknotes denominated in any official currency of an EU Member State; and firearms, their parts and essential components and ammunition as listed in Annex I to Regulation (EU) No. 258/2012 of the European Parliament and of the Council (EU Firearms Regulation) and firearms and other arms as listed in Annex XXXV to Council Regulation (EU) No. 833/2014.

There are also express prohibitions on (i) the provision of technical assistance, brokering services and other services, (ii) the provision of financing or financial assistance and (iii) selling, licensing or transferring in any other way intellectual property rights or trade secrets as well as granting rights to access or re-use any material or information protected by means of intellectual property rights or constituting trade secrets, related to the listed items to any natural or legal person, entity or body in Russia or for use in Russia. Further, there is a prohibition on providing technical assistance, brokering services and financing or financial assistance related to the goods and technology listed in the EU Common Military List. The EU established the provisions with regard to the intellectual property of EU entities or persons in the context of the Russia export controls regime with its 11th sanctions package, enacted in June 2023.

**United Kingdom**

The UK export control regime comprises the Export Control Act 2002 and the Export Control Order 2008. Due to the UK's withdrawal from the EU, Council Regulation (EC) 428/2009 became retained legislation under the EU Withdrawal Act 2018, while the EU Dual-Use Regulation applies to the export, brokering, technical assistance, transit and transfer of dual-use items from the UK. The UK legislation restricts the export, supply, delivery or making available of listed items to or for use in Russia or to a person "connected with Russia." The relevant items include: military goods as listed in Schedule 2 to the Export Control Order 2008; defense and security goods according to Schedule 3C of the Russia Sanctions Regulations 2019; dual-use goods and technology as listed in Council Regulation (EC) No 428/2009 of 5 May 2009; critical-industry goods and technology as listed in Schedule 2A of the Russia Sanctions Regulations; aviation and space items according to Schedule 2C of the Russia Sanctions Regulations; oil refining goods and technology according to the Schedule 2D of the Russia Sanctions Regulations; quantum computing and advanced materials goods and technology as listed in Schedule 2E of Russia Sanctions Regulations; energy-related items according to Part 2 of Schedule 3 of the Russia Sanctions Regulations; luxury goods as listed in Schedule 3A of the Russia Sanctions Regulations; items identified as "G7 dependency and further goods list goods", according to Schedule 3E of the Russia Sanctions Regulations.

On 13 December 2022, the UK Export Control Joint Unit published a compliance code of practice for export licensing. The code is voluntary and intended to provide best practice guidance on how to develop export control compliance procedures. It outlines the following practical steps: committing to compliance; nominating responsible personnel; informing and training staff; developing company compliance procedures; handling suspicious enquiries or orders; record-keeping; provision for audits.

The Department for Business and Trade issued guidance related to the risks of circumventing UK trade sanctions. It outlines that exporters should conduct "strong due diligence on counterparties […] in relation to sanctions," and, for continuing contracts, to repeat due diligence "at intervals to ensure that the risk has not changed." The guidance also lists examples of "Key Risk Indicators," based on customer, product and location, and indicates that exporters should adapt due diligence and compliance procedures considering risks identified.

## Appendix 2: Definition of "Battlefield Goods" and "Critical Components"

**HS codes included in "battlefield goods"**

***Tier 1 (4)***

| | |
|---|---|
| 8542.31 | Electronic integrated circuits: Processors and controllers, whether or not combined with memories, converters, logic circuits, amplifiers, clock and timing circuits, or other circuits |
| 8542.32 | Electronic integrated circuits: Memories |
| 8542.33 | Electronic integrated circuits: Amplifiers |
| 8542.39 | Electronic integrated circuits: Other |

***Tier 2 (5)***

| | |
|---|---|
| 8517.62 | Machines for the reception, conversion and transmission or regeneration of voice, images or other data, including switching and routing apparatus |
| 8526.91 | Radio navigational aid apparatus |
| 8532.21 | Other fixed capacitors: Tantalum capacitors |
| 8532.24 | Other fixed capacitors: Ceramic dielectric, multilayer |
| 8548.00 | Electrical parts of machinery or apparatus, not specified or included elsewhere in chapter 85 |

***Tier 3.A (16)***

| | |
|---|---|
| 8471.50 | Processing units other than those of subheading 8471.41 or 8471.49, whether or not containing in the same housing one or two of the following types of unit: storage units, input units, output units |
| 8504.40 | Static converters |
| 8517.69 | Other apparatus for the transmission or reception of voice, images or other data, including apparatus for communication in a wired or wireless network |
| 8525.89 | Other television cameras, digital cameras and video camera recorders |
| 8529.10 | Aerials and aerial reflectors of all kinds; parts suitable for use therewith |
| 8529.90 | Other parts suitable for use solely or principally with the apparatus of headings 8524 to 8528 |
| 8536.69 | Plugs and sockets for a voltage not exceeding 1 000 V |
| 8536.90 | Electrical apparatus for switching electrical circuits, or for making connections to or in electrical circuits, for a voltage not exceeding 1000 V (excl. fuses, automatic circuit breakers and other apparatus for protecting electrical circuits, relays and other switches, lamp holders, plugs and sockets) |
| 8541.10 | Diodes, other than photosensitive or light-emitting diodes (LED) |
| 8541.21 | Transistors, other than photosensitive transistors with a dissipation rate of less than 1 W |
| 8541.29 | Other transistors, other than photosensitive transistors |
| 8541.30 | Thyristors, diacs and triacs (excl. photosensitive semiconductor devices) |
| 8541.49 | Photosensitive semiconductor devices (excl. Photovoltaic generators and cells) |
| 8541.51 | Other semiconductor devices: Semiconductor-based transducers |
| 8541.59 | Other semiconductor devices |
| 8541.60 | Mounted piezo-electric crystals |

***Tier 3.B (9)***

| | |
|---|---|
| 8482.10 | Ball bearings |
| 8482.20 | Tapered roller bearings, including cone and tapered roller assemblies |
| 8482.30 | Spherical roller bearings |
| 8482.50 | Other cylindrical roller bearings, including cage and roller assemblies |
| 8807.30 | Other parts of aeroplanes, helicopters or unmanned aircraft |

| | |
|---|---|
| 9013.10 | Telescopic sights for fitting to arms; periscopes; telescopes designed to form parts of machines, appliances, instruments or apparatus of this chapter or Section XV |
| 9013.80 | Other optical devices, appliances and instruments |
| 9014.20 | Instruments and appliances for aeronautical or space navigation (other than compasses |
| 9014.80 | Other navigational instruments and appliances |

***Tier 4 (11)***

| | |
|---|---|
| 8471.80 | Units for automatic data-processing machines (excl. processing units, input or output units and storage units) |
| 8486.10 | Machines and apparatus for the manufacture of boules or wafers |
| 8486.20 | Machines and apparatus for the manufacture of semiconductor devices or of electronic integrated circuits |
| 8486.40 | Machines and apparatus specified in note 11(C) to this chapter |
| 8434.00 | Printed circuits |
| 8543.20 | Signal generators |
| 9027.50 | Other instruments and apparatus using optical radiations (ultraviolet, visible, infrared) |
| 9030.20 | Oscilloscopes and oscillographs |
| 9030.32 | Multimeters with recording device |
| 9030.39 | Instruments and apparatus for measuring or checking voltage, current, resistance or electrical power, with recording device |
| 9030.82 | Instruments and apparatus for measuring or checking semiconductor wafers or devices |

**HS codes included in "critical components"**

***Automotive components and equipment (83)***

| | | | | | |
|---|---|---|---|---|---|
| 8407100003 | 8411210009 | 8412298909 | 8501310000 | 8511100009 | 8708705009 |
| 8407211000 | 8411810001 | 8412310009 | 8501320008 | 8511300008 | 8708709909 |
| 8407219100 | 8411810008 | 8412390009 | 8501330008 | 8511400008 | 8708803509 |
| 8407219900 | 8411910001 | 8412808009 | 8501340000 | 8511500008 | 8708805509 |
| 8407290000 | 8411910002 | 8412904008 | 8501402004 | 8511800008 | 8708809909 |
| 8407321000 | 8411910008 | 8412908009 | 8501402009 | 8511900009 | 8708913509 |
| 8407343009 | 8411990019 | 8479899707 | 8501408009 | 8708109009 | 8708919909 |
| 8408209907 | 8411990091 | 8479907000 | 8501510001 | 8708299009 | 8708923509 |
| 8408906500 | 8411990098 | 8501101001 | 8501510009 | 8708309109 | 8708939009 |
| 8408906700 | 8412212002 | 8501101009 | 8501522001 | 8708309909 | 8708943509 |
| 8409910008 | 8412212009 | 8501109100 | 8501522009 | 8708405009 | 8708949909 |
| 8409990009 | 8412218008 | 8501109300 | 8501523000 | 8708409109 | 8708999309 |
| 8411110001 | 8412292009 | 8501109900 | 8501617000 | 8708409909 | 8708999709 |
| 8411123009 | 8412298109 | 8501200009 | 8501620000 | 8708509909 | |

***Bearings and transmission shafts (31)***

| | | | | | |
|---|---|---|---|---|---|
| 8482101009 | 8482500009 | 8483105000 | 8483402100 | 8483409000 | 8483908909 |
| 8482109001 | 8482800009 | 8483109500 | 8483402308 | 8483502000 | |
| 8482109008 | 8482990000 | 8483200000 | 8483402500 | 8483508000 | |
| 8482200009 | 8483102108 | 8483303209 | 8483402900 | 8483602000 | |
| 8482300009 | 8483102509 | 8483303809 | 8483403009 | 8483608000 | |
| 8482400009 | 8483102909 | 8483308007 | 8483405900 | 8483908100 | |

***Communications equipment (80)***

| | | | | | |
|---|---|---|---|---|---|
| 8517180000 | 8521900009 | 8523499900 | 8523809300 | 8526920008 | 8529106500 |

| | | | | | |
|---|---|---|---|---|---|
| 8517610002 | 8523210000 | 8523511000 | 8523809900 | 8527139900 | 8529106901 |
| 8517610008 | 8523291505 | 8523519101 | 8525500000 | 8527190000 | 8529106909 |
| 8517620002 | 8523291509 | 8523519109 | 8525600009 | 8527212009 | 8529108000 |
| 8517620003 | 8523293102 | 8523519300 | 8525819100 | 8527215909 | 8529109500 |
| 8517620009 | 8523293901 | 8523519900 | 8525819900 | 8527219800 | 8529902002 |
| 8517699000 | 8523293908 | 8523529001 | 8525891900 | 8527290009 | 8529906502 |
| 8517709009 | 8523419000 | 8523529009 | 8525893000 | 8527911900 | 8529906508 |
| 8517711100 | 8523492500 | 8523591000 | 8525899109 | 8527913500 | 8529906509 |
| 8517711500 | 8523493900 | 8523599101 | 8525899900 | 8527919900 | 8529909600 |
| 8517711900 | 8523494500 | 8523599109 | 8526100001 | 8527921000 | |
| 8517790001 | 8523495100 | 8523599300 | 8526100009 | 8527990000 | |
| 8517790009 | 8523495900 | 8523599900 | 8526912000 | 8529101100 | |

***Computer components (15)***

| | | | | |
|---|---|---|---|---|
| 8471410000 | 8471703000 | 8471708000 | 8471900000 | 8473308000 |
| 8471500000 | 8471705000 | 8471709800 | 8473302002 | 8473502000 |
| 8471702000 | 8471707000 | 8471800000 | 8473302008 | 8473508000 |

***Drones (5)***

| | | | | |
|---|---|---|---|---|
| 8806220001 | 8806920001 | 8807200000 | 8807300000 | 8807900009 |

***Electric and electronic equipment (159)***

| | | | | | |
|---|---|---|---|---|---|
| 8504102000 | 8504909200 | 8532100000 | 8536105000 | 8536700004 | 8544190009 |
| 8504108000 | 8504909800 | 8532210000 | 8536109000 | 8536900100 | 8544200000 |
| 8504210000 | 8505110000 | 8532220000 | 8536201007 | 8536901000 | 8544300002 |
| 8504229000 | 8505191000 | 8532230000 | 8536209007 | 8536908500 | 8544300003 |
| 8504230009 | 8505199000 | 8532240000 | 8536302000 | 8537101000 | 8544300007 |
| 8504312109 | 8505200000 | 8532250000 | 8536304000 | 8537109100 | 8544421000 |
| 8504312909 | 8505902009 | 8532290000 | 8536308000 | 8537109800 | 8544429003 |
| 8504318001 | 8506101100 | 8532300000 | 8536411000 | 8537109900 | 8544429007 |
| 8504318007 | 8506101801 | 8532900000 | 8536419000 | 8537209200 | 8544429009 |
| 8504320002 | 8506101809 | 8533100000 | 8536490000 | 8537209800 | 8544492000 |
| 8504320009 | 8506109100 | 8533210000 | 8536500400 | 8538100000 | 8544499101 |
| 8504330009 | 8506109809 | 8533290000 | 8536500600 | 8538901200 | 8544499108 |
| 8504340000 | 8506400000 | 8533310000 | 8536500700 | 8538909200 | 8544499309 |
| 8504403004 | 8506501000 | 8533390000 | 8536501109 | 8538909901 | 8544499501 |
| 8504403008 | 8506503000 | 8533401000 | 8536501509 | 8538909908 | 8544499509 |
| 8504403009 | 8506509000 | 8533409000 | 8536501904 | 8540208000 | 8544499900 |
| 8504405500 | 8506600000 | 8533900000 | 8536501906 | 8540710001 | 8544601000 |
| 8504408300 | 8506808000 | 8534001100 | 8536508008 | 8540710009 | 8544609009 |
| 8504408500 | 8507102003 | 8534001900 | 8536611000 | 8540810000 | 8544700000 |
| 8504408700 | 8507202000 | 8534009000 | 8536619000 | 8540890000 | 8545110089 |
| 8504409000 | 8507208001 | 8535100000 | 8536691000 | 8543200000 | 8545200009 |
| 8504409100 | 8507208008 | 8535210000 | 8536693000 | 8543400000 | 8545909000 |
| 8504502000 | 8507302009 | 8535290000 | 8536699002 | 8543703008 | 8548009000 |
| 8504509500 | 8507500000 | 8535302000 | 8536699008 | 8543708000 | 8549990000 |
| 8504900600 | 8507600000 | 8535400000 | 8536700001 | 8543709000 | |
| 8504901100 | 8507800001 | 8535900008 | 8536700002 | 8543900000 | |
| 8504901700 | 8507800009 | 8536101000 | 8536700003 | 8544119000 | |

***Navigation equipment and sensors (62)***

| | | | | | |
|---|---|---|---|---|---|
| 9002110000 | 9014800000 | 9025804000 | 9026802000 | 9030320009 | 9032102000 |
| 9002190000 | 9014900000 | 9025808000 | 9026808000 | 9030331000 | 9032108100 |
| 9002200000 | 9015101000 | 9025900003 | 9026900000 | 9030339100 | 9032108900 |
| 9002900009 | 9015109000 | 9025900008 | 9027500000 | 9030339900 | 9032200000 |
| 9013200000 | 9015309000 | 9026102100 | 9029100009 | 9030390009 | 9032810000 |
| 9013800000 | 9015401000 | 9026102900 | 9029203109 | 9030400000 | 9032890000 |
| 9013900000 | 9015900000 | 9026108100 | 9029203809 | 9030820000 | 9032900000 |
| 9014100000 | 9025118000 | 9026108900 | 9029900009 | 9030840009 | |
| 9014202009 | 9025192000 | 9026202000 | 9030100000 | 9030893000 | |
| 9014208001 | 9025198009 | 9026204000 | 9030201000 | 9030899009 | |
| 9014208009 | 9025802000 | 9026208000 | 9030310000 | 9030908500 | |

***Semiconductors (37)***

| | | | | | |
|---|---|---|---|---|---|
| 8541100001 | 8541410004 | 8541490000 | 8542319010 | 8542326100 | 8542399090 |
| 8541100009 | 8541410006 | 8541510000 | 8542319090 | 8542326900 | 8542900000 |
| 8541210000 | 8541410007 | 8541590000 | 8542321000 | 8542327500 | |
| 8541290000 | 8541410008 | 8541600000 | 8542323100 | 8542329000 | |
| 8541300009 | 8541410009 | 8541900000 | 8542323900 | 8542339000 | |
| 8541410001 | 8541420000 | 8542311001 | 8542324500 | 8542391000 | |
| 8541410002 | 8541430000 | 8542311009 | 8542325500 | 8542399010 | |

***Other components 13)***

| | | | | |
|---|---|---|---|---|
| 8486209009 | 9024809000 | 9031803400 | 9031809800 | 9031908500 |
| 8486901000 | 9024900000 | 9031803800 | 9031902000 | |
| 8486909008 | 9031499000 | 9031809100 | 9031903000 | |

## Appendix 3: Summary of Dynamics on Different Stages of the Supply Chain

**Russian imports in January-October 2023 by country of producer**

| | Battlefield goods | | | | Critical components | | |
|---|---|---|---|---|---|---|---|
| **Rank** | **Country** | **Value** | **Share** | **Rank** | **Country** | **Value** | **Share** |
| 1 | China | 3,600 | 44.6% | 1 | China | 9,157 | 41.2% |
| 2 | United States | 2,237 | 27.7% | 2 | United States | 3,353 | 15.1% |
| 3 | Taiwan | 612 | 7.6% | 3 | Taiwan | 1,037 | 4.7% |
| 4 | Germany | 259 | 3.2% | 4 | Germany | 813 | 3.7% |
| 5 | Hong Kong | 181 | 2.2% | 5 | Japan | 515 | 2.3% |
| 6 | Switzerland | 170 | 2.1% | 6 | South Korea | 450 | 2.0% |
| 7 | Japan | 133 | 1.6% | 7 | Hong Kong | 309 | 1.4% |
| 8 | Malaysia | 122 | 1.5% | 8 | Switzerland | 300 | 1.4% |
| 9 | South Korea | 76 | 0.9% | 9 | Malaysia | 153 | 0.7% |
| 10 | Netherlands | 75 | 0.9% | 10 | India | 151 | 0.7% |

**Russian imports in January-October 2023 by country of origin**

| | Battlefield goods | | | | Critical components | | |
|---|---|---|---|---|---|---|---|
| **Rank** | **Country** | **Value** | **Share** | **Rank** | **Country** | **Value** | **Share** |
| 1 | China | 5,528 | 63.1% | 1 | China | 13,043 | 58.7% |
| 2 | Taiwan | 699 | 8.0% | 2 | Taiwan | 1,118 | 5.0% |
| 3 | Malaysia | 513 | 5.8% | 3 | Germany | 865 | 3.9% |
| 4 | United States | 375 | 4.3% | 4 | United States | 836 | 3.8% |
| 5 | Vietnam | 219 | 2.5% | 5 | Malaysia | 676 | 3.0% |
| 6 | Germany | 148 | 1.7% | 6 | South Korea | 662 | 3.0% |
| 7 | South Korea | 120 | 1.4% | 7 | Turkey | 527 | 2.4% |
| 8 | Thailand | 103 | 1.2% | 8 | Japan | 469 | 2.1% |
| 9 | Philippines | 99 | 1.1% | 9 | Italy | 460 | 2.1% |
| 10 | Hong Kong | 99 | 1.1% | 10 | Vietnam | 402 | 1.8% |

**Russian imports in January-October 2023 by country of seller**

| | Battlefield goods | | | | Critical components | | |
|---|---|---|---|---|---|---|---|
| **Rank** | **Country** | **Value** | **Share** | **Rank** | **Country** | **Value** | **Share** |
| 1 | China | 3,328 | 38.0% | 1 | China | 8,651 | 38.9% |
| 2 | Hong Kong | 2,706 | 30.9% | 2 | Hong Kong | 4,024 | 18.1% |
| 3 | Turkey | 604 | 6.9% | 3 | Turkey | ,870 | 8.4% |
| 4 | UAE | 293 | 3.3% | 4 | UAE | 932 | 4.2% |
| 5 | Switzerland | 186 | 2.1% | 5 | South Korea | 503 | 2.3% |
| 6 | Serbia | 171 | 1.9% | 6 | Serbia | 390 | 1.8% |
| 7 | Slovak Republic | 138 | 1.6% | 7 | Switzerland | 388 | 1.7% |
| 8 | Taiwan | 115 | 1.3% | 8 | Kyrgyz Republic | 305 | 1.4% |
| 9 | Kyrgyz Republic | 98 | 1.1% | 9 | Germany | 288 | 1.3% |
| 10 | Thailand | 78 | 0.9% | 10 | Italy | 258 | 1.2% |

**Russian imports in January-October 2023 by country of dispatch**

| | Battlefield goods | | | | Critical components | | |
|---|---|---|---|---|---|---|---|
| **Rank** | **Country** | **Value** | **Share** | **Rank** | **Country** | **Value** | **Share** |
| 1 | China | 4,665 | 53.2% | 1 | China | 11,916 | 53.8% |
| 2 | Hong Kong | 1,992 | 22.7% | 2 | Hong Kong | 2,853 | 12.9% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | Turkey | 465 | 5.3% | 3 | Turkey | 1,824 | 8.2% |
| 4 | UAE | 442 | 5.0% | 4 | UAE | 816 | 3.7% |
| 5 | Thailand | 215 | 2.5% | 5 | South Korea | 550 | 2.5% |
| 6 | Maldives | 122 | 1.4% | 6 | Thailand | 339 | 1.5% |
| 7 | Malaysia | 105 | 1.2% | 7 | Germany | 293 | 1.3% |
| 8 | Taiwan | 100 | 1.1% | 8 | India | 258 | 1.2% |
| 9 | India | 80 | 0.9% | 9 | Poland | 251 | 1.1% |
| 10 | South Korea | 75 | 0.8% | 10 | Maldives | 250 | 1.1% |

## Appendix 4: Subset of Companies for Analysis in Section II.4.

| Company (parent company) | Country | Company (parent company) | Country |
|---|---|---|---|
| Actel (Microchip Technology) | U.S. | Delta Electronics | Taiwan |
| Adesto Technologies | U.S. | Deyuan Technology | China |
| ADLINK | Taiwan | DFRobot Electronics | China |
| Advanced Micro Devices | U.S. | Digi International | U.S. |
| Advanced Monolithic Systems | U.S. | DMP Electronics | Taiwan |
| Advanced Technology International | U.S. | Dragon City Industries | H. Kong |
| Aimtec | Canada | Dynalogic | Netherl. |
| Alfa Rpar | Latvia | Dynatron | U.S. |
| Alinx | China | Eaton Corporation | Ireland |
| All Sensors | U.S. | Ebm-papst | Germany |
| Allegro Micro Systems | U.S. | EPCOS (TDK Corporation) | Japan |
| Alliance Memory | U.S. | Epson (Seiko Epson) | Japan |
| Altera Corporation (Intel Corporation) | U.S. | E-Tech Electronics | H. Kong |
| Amphenol Aerospace (Amphenol) | U.S. | Eudyna Devices | U.S. |
| Ampleon | Netherl. | Everlight Electronics | Taiwan |
| Amplus Communication | Taiwan | Fairchild Semiconductor (Onsemi) | U.S. |
| Analog Devices | U.S. | Faithful Link Industrial | Taiwan |
| Anaren (TTM Technologies) | U.S. | FLIR Systems (Teledyne Technologies) | U.S. |
| Anderson Electronics | U.S. | Freescale Semiconductor (NXP) | Netherl. |
| Apacer | Taiwan | Fujitsu | Japan |
| Apem (IDEC Corporation) | Japan | Futaba Corporation | Japan |
| Apex Microtechnology | U.S. | Future Technology Devices Int. | U.K. |
| ATMEL (Microchip Technology) | U.S. | Gennum Corporation | Canada |
| AXICOM | Switzerl. | GLEAD Electronics | China |
| Axis Communications (Canon) | Japan | Glenair | Germany |
| BCD Semiconductor (Diodes Incorp.) | U.S. | GlobalSat WorldCom | Taiwan |
| Bel Power Solutions (Bel Fuse) | U.S. | Golledge Electronics | U.K. |
| Bolymin | Taiwan | Greenliant Systems | U.S. |
| Bombardier | Canada | Guangzhou Kexin Ind. (Kexin Electr.) | China |
| Bourns | U.S. | Gumstix (Altium) | U.S. |
| Broadcom Corporation | U.S. | HALO Electronics | U.S. |
| Burr Brown (Texas Instruments) | U.S. | Harting | Germany |
| C&K (Littelfuse) | U.S. | Hemisphere GNSS (CNH Industrial) | U.K. |
| CADDOCK | U.S. | Hirose Electric | Japan |
| Canon | Japan | Hitachi | Taiwan |
| Catalyst Semiconductor | U.S. | Hitano Enterprise | Taiwan |
| Cervoz | Taiwan | HiTec RCD | U.S. |
| Cirocomm | Taiwan | Hittite Microwave Corp. (Analog Dev.) | U.S. |
| Clare (Littelfuse) | U.S. | Holt Integrated Circuits | U.S. |
| CML Microcircuits | U.K. | Honeywell International | U.S. |
| Coilcraft | U.S. | Hongfa | China |
| Coiltronics (Eaton Corporation) | Ireland | Hewlett Packard | U.S. |
| Connfly | Taiwan | IC-Haus | Germany |
| Cortina Systems (Marvell Technology) | U.S. | IEI Group | Taiwan |
| CTS Corporation | U.S. | iFlight | China |
| Cypress Semiconductor (Infineon) | Germany | Illinois Capacitor (Cornell Dubilier) | U.S. |

| Company (parent company) | Country | Company (parent company) | Country |
|---|---|---|---|
| Inchange Semiconductor Company | China | New Japan Radio (Nisshinbo) | Japan |
| Infineon Technologies | Germany | New Jersey Semiconductor | U.S. |
| Integrated Circuit Systems (Renesas) | Japan | Nexperie (Wingtech) | China |
| Integrated Device Tech. (Renesas) | Japan | NGK Spark Plug | Japan |
| Integrated Silicon Solutions | U.S. | Nic Components Corporation | U.S. |
| Intel Corporation | U.S. | NICOMATIC | France |
| International Rectifier (Infineon) | Germany | Nihon Dempa Kogyo | Japan |
| ISSI (Integrated Silicon Solutions) | U.S. | Nippon (NEC) | Japan |
| IXYS (Littelfuse) | U.S. | NLT Technologies | U.S. |
| JST Electronics | Singapore | Numonyx (Micron Technology) | U.S. |
| Kemet Electronic Components (Yageo) | Taiwan | NVE Corporation | U.S. |
| Kingston Technology Corporation | U.S. | Nvidia | U.S. |
| Kodenshi | Japan | NXP Semiconductors | Netherl. |
| Kyocera | Japan | OMRON | Japan |
| Lantronix | U.S. | Onsemi | U.S. |
| Lattice Semiconductor | U.S. | Panasonic | Japan |
| L-com | U.S. | Peak Electronics | Germany |
| LG Corporation | Korea | Philips | Netherl. |
| Ligitek Electronics | Taiwan | Phoenix Contact | Germany |
| LINAK | Denmark | Picor Corporation (Vicor) | U.S. |
| Linear Technology | U.S. | Planar Systems (Leyard) | China |
| Lite-On Technology | Taiwan | PLX Technology (Broadcom) | U.S. |
| Littelfuse | U.S. | PMC-Sierra (Microchip Technology) | U.S. |
| MACOM | U.S. | Power Mate Technology | U.S. |
| Macronix | Taiwan | Pulse Electronics (Yageo) | Taiwan |
| Marvell Semiconductor (Marvell) | U.S. | Qingdao Thundsea Marine Tech. | China |
| Maxim Integrated (Analog Devices) | U.S. | Qorvo | U.S. |
| Maxwell Technologies | U.S. | QST Corporation | China |
| Mercury Electronics | U.S. | Quectel | China |
| Merrimac Industries | U.S. | Quintech | Germany |
| Michelin | France | Ramtron International (Infineon) | Germany |
| Micrel Semicond. (Microchip Tech.) | U.S. | Raspberry Pi | U.K. |
| Micro Crystal (Swatch Group) | Switzerl. | Realtek | Taiwan |
| Microchip Technology | U.S. | Renesas Electronics | Japan |
| Micron Technology | U.S. | RF Micro Devices (Qorvo) | U.S. |
| MikroTik | Latvia | Ricci Microwave | Korea |
| Mini-Circuits | U.S. | RIFA | China |
| Mitsubishi Electric (Mitsubishi) | Japan | RN2 Technologies | Korea |
| Molex Electronics (Koch Industries) | U.S. | Rochester Electronics | U.S. |
| Mornsun | China | Rogers Corporation | U.S. |
| Mouser Electronics TTI) | U.S. | ROHM Semiconductor | Japan |
| Murata | Japan | Rotax (Bombardier) | Canada |
| Nanya Technology | Taiwan | Runcam | H. Kong |
| National Semicond. (Texas Instr.) | U.S. | SafeNet (Thales) | France |
| Nelson Digital Devices | H. Kong | Safran | France |
| NetSol | U.S. | Samsung | Korea |
| Netzer | Israel | SanDisk | U.S. |
| New Centress | Taiwan | Sawtek (Qorvo) | U.S. |

| Company (parent company) | Country | Company (parent company) | Country |
|---|---|---|---|
| Scorpion Power Systems | H.Kong | Thales | France |
| Semelab (TT Electronics) | U.K. | Thinki Semiconductor | China |
| Semiconductor Comp. Ind. (Onsemi) | U.S. | Ti Automotive (TI Fluid Systems) | U.K. |
| Semtech | U.S. | Token Electronics Industry | Taiwan |
| Silex Technology (Murata) | Japan | TOREX | Japan |
| Silicon Laboratories | U.S. | Toshiba | Japan |
| Silicon Sensing System | U.K. | TP-Link | China |
| Silicon Storage Tech. (Microchip Tech.) | U.S. | Traco | Switzerl. |
| SIMCom | China | Transcend | Taiwan |
| Sipex Corporation | U.S. | TriQuint Semiconductor (Qorvo) | U.S. |
| Sirenza Microdevices | U.S. | TT Electronics | U.K. |
| Skyworks Solutions | U.S. | TTM Technologies | U.S. |
| SMART Global Holdings | Kyrgyz R. | Tyco Electronics | Switzerl. |
| SMC Corporation | Japan | U-blox | Switzerl. |
| SMC Diode Solutions | China | UIY | China |
| SMSC (Microchip Technology) | U.S. | UN Semiconductor | Taiwan |
| Sonitron | Belgium | Unisonic Technologies | Taiwan |
| Sony | Japan | Vbsemi | Taiwan |
| Souriau (Eaton Corporation) | Ireland | Vicor | U.S. |
| Spansion (Infineon Technologies) | Germany | Vishay | U.S. |
| STMicroelectronics | Switzerl. | Visionhitech | Korea |
| Sumida Corporation | Japan | Voltage Multipliers | U.S. |
| Switronic | Taiwan | Weigao | China |
| Synocean | Taiwan | Winbond | Taiwan |
| Tai-Saw Technology | Taiwan | WIZnet | India |
| TSMC | Taiwan | Wolfspeed | U.S. |
| Tallysman | U.S. | Won-Top Electronics | Taiwan |
| Taoglas | Ireland | Wurth Electronics | Germany |
| TDK Corporation | Japan | Xilinx (Advanced Micro Devices) | U.S. |
| TE Connectivity | Switzerl. | XP Power | Singapore |
| TechWell Corporation | U.S. | Yageo | Taiwan |
| Telpod | Poland | YXC | China |
| Tengfei | China | Z-Communications | U.S. |
| Texas Instruments | U.S. | Zilog (Littelfuse) | U.S. |

*Note: The inclusion of affiliations is for identification purposes only and does not represent an endorsement of shared views with the co-signer.*

**Dr. Anders Åslund**, Senior Fellow, Stockholm Free World Forum.

**Alex Bashinsky,** LLM, Certified Global Sanctions Specialist, Co-Founder at Global Sanctions Training Institute (GSTI).

**Torbjörn Becker,** Director of Stockholm Institute of Transition Economics.

**Olena Bilousova,** Research Fellow, Kyiv School of Economics.

**Tymofii Brik,** Rector, Kyiv School of Economics.

**Tatyana Deryugina**, Associate Professor, Department of Finance, University of Illinois - Urbana-Champaign; Co-organizer of the Economists for Ukraine group.

**Anastassia Fedyk**, Assistant Professor of Finance, the Haas School of Business, University of California - Berkeley; Co-organizer of the Economists for Ukraine group.

**Yuriy Gorodnichenko**, Quantedge Presidential Professor of Economics, Department of Economics, University of California - Berkeley; Co-organizer of the Economists for Ukraine group.

**Benjamin Hilgenstock,** Senior Economist, Kyiv School of Economics.

**James Hodson,** CEO, AI for Good Foundation; Co-founder, Economists for Ukraine

**Denys Jatsyshyn**, Director, Corporate Relations, U.S.-Ukraine Business Council (USUBC).

**Eric Johnson**, Former Managing Director, Cambridge Associates; Former National Security Council Staff, White House Situation Room.

**Tom Keatinge,** Director of the Centre for Financial Crime & Security Studies at RUSI

**Craig Kennedy**, Center Associate, Davis Center for Russian and Eurasian Studies, Harvard University.

**Tyler Kustra,** Assistant Professor of Politics and International Relations, University of Nottingham.

**Michael McFaul**, Director, Freeman Spogli Institute for International Studies (FSI), Professor of Political Science, and Hoover Institution Senior Fellow, Stanford University; Coordinator, International Working Group on Russian Sanctions.

**Benjamin Moll**, Professor, London School of Economics and Political Science.

**Tymofiy Mylovanov,** President of the Kyiv School of Economics; Associate Professor, University of Pittsburgh.

**Jacob Nell,** Senior Research Fellow, Kyiv School of Economics

**Craig Pask,** Director, Truver Limited, Founder, Ukrainians Help, Contributor, International Working Group on Russian Sanctions

**Steven Pifer**, Affiliate, Center for International Security and Cooperation, Stanford University, and Former U.S. Ambassador to Ukraine.

**Lukasz Rachel,** Assistant Professor of Economics, University College London

**Elina Ribakova,** Nonresident Senior Fellow, Peterson Institute for International Economics; Nonresident Fellow, Bruegel; Vice President for Foreign Policy, Kyiv School of Economics.

**Dr. Benjamin L. Schmitt**, Senior Fellow, Kleinman Center for Energy Policy, University of Pennsylvania; Associate, Harvard-Ukrainian Research Institute; Senior Fellow, Center for European Policy Analysis (CEPA); Rethinking Diplomacy Fellow and Space Diplomacy Lab Co-Founder, Duke University.

**Nataliia Shapoval**, Vice President for Policy Research, Kyiv School of Economics.

**Anna Vlasyuk,** Research Fellow, Kyiv School of Economics.

**Vladyslav Vlasiuk,** PhD, Secretary of Ukrainian Working Group on Russian Sanctions.