Working Group Paper #12

Strengthening Sanctions to Stop Western Technology from Helping Russia's Military Industrial Complex

The International Working Group on Russian Sanctions

July 3, 2023

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

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 or entity. All members of this working group participate in their private capacities. Like other papers produced by this working group, our aim is not to produce a consensus document, but instead to provide a menu of possible additional measures to be considered by governments, multilateral institutions, and private actors. The implications of every sanction have not been thoroughly analyzed, and not everyone necessarily agrees with every specific sanction or action proposed.

This paper was first drafted by Olena Bilousova, Oleksii Gribanovskiy, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, and Vladyslav Vlasiuk.

Contents

II. Russia's Military Capabilities in 2023 9

Overall Assessment of Military Capabilities 10

Analysis of Russian Military Equipment 14

Trade Channels: Rise of China 20

Company Analysis: Business with Russia Continues 22

I. Executive Summary

Western-imported Technology Components are Critical Enablers of Russia's Military Capacity

On June 13, 2023, a Russian Kh-101 missile killed 11 people, including one child, in a five-story residential building in Kryvyi Rih. This missile carried 53 critical components sourced and imported from democratic countries. After 15 months of war and tens of thousands of sanctions, how could components produced by democratic countries be the key enabler of such missile attacks on Ukrainian civilians? This paper offers evidence that Western parts continue to enable Russia in its full-scale invasion of and war against Ukraine. This missile represents just one item in Russia'sarsenal, which has committed a number of similarly atrocious acts. Since February 22, 2022, Russians have launched more than 6,000 rockets against Ukraine, hitting 3,387 civic objects and killing 1,734 civilians.

Strikingly, components that have been identified by the Ukrainian authorities in these Russian missiles are linked to many of the same companies whose components have appeared in other intercepted weapons on Ukrainian territory since April 2022: US Analog Devices, US Texas Instruments, US Microchip Technology, US Intel corporation, US AMD, German Infineon Technologies, Korean Samsung, Switzerland STMicroelectronics, US Vicor, USA XILINX, USA ZILOG, US Maxim Integrated, and USA Cypress Semiconductor.

These components are not from old stocks. In December 2022, Conflict Armament Research (CAR) analyzed the remnants of two Russian Kh-101 missiles in Kyiv and concluded with near certainty that these missiles had been manufactured within the previous two months (i.e., before November 2022). We offer more evidence collected by the International Working Group on Russian Sanctions and KSE Institute in this report "Russia's Military Capacity and the Role of Imported Components" and offer policy recommendations on how to stop leakage of critical missile inputs from democratic countries to Russia. If implemented, these recommendations will severely constrain Russia's ability to produce new missiles and replenish its exhausted stockpile. The immediate policy recommendation is to stop completely the transfer to Russia of technologies used to produce weapons from democratic countries. The longer-term goal is to further isolate Russia from trading with democratic countries, with the exception of several humanitarian categories and unsanctioned energy products.

Russian Military Capacity and its Dependence on Western Technology

Russia began its February 2022 invasion of Ukraine with a massive armed force and extensive stockpiles of Soviet-era equipment, including artillery shells, tanks, and armored vehicles. Moreover, Russia extensively modernized its conventional military forces over the past 15 years, spending hundreds of billions of dollars on new arms. As a result, Russia's military equipment stocks were estimated to be one of the largest in the world. In 2021, its defense budget amounted to $62.2 billion. Its defense spending amounted to 3.8% of GDP.

However, 16 months into the all-out invasion, Russia's more advanced post-Soviet systems, such as missiles and sophisticated armored vehicles, are already in short supply. Cutting-edge military equipment, such as Armata tanks, have not been seen on the battlefield, despite the Russian authorities' claims of significant stockpiles. During the conflict, it also has become apparent that some types of weapons are not as modern and effective as their stated characteristics.

Russia's key weapon production and warfare components hinge heavily on Western technology. If severed from Western components, computer numeric control machines, and corresponding software, Russia would struggle to sustain its modern military capacities. The backbone of Russia's contemporary military apparatus relies heavily on sophisticated electronics sourced from countries such as the United States, United Kingdom, Germany, the Netherlands, Japan, Israel, and China. A subset of these components are civilian dual-use goods, which are commercially available and thus harder to regulate through export controls.

Sanctions Have Significantly Reduced Russia's Capacity to Wage War in Ukraine

The combination of sanctions and the voluntary withdrawal of foreign businesses from Russia has significantly impacted the country's capabilities to produce weapons and fund the war more generally, demonstrating that economic and diplomatic pressure can translate into tangible effects on a nation's military strength and performance. Notwithstanding the sanction-evasion strategies, smuggling practices, and attempts to substitute Western components with Russia`s own production, there is growing evidence of the impact of already implemented sanctions on Russia's military capabilities.

In May 2023, Kyiv School of Economics (KSE), the Ukrainian Ministry of Defense, and the Jamestown Foundation estimated that as of June, Russia had only 12% of its Iskander 9M723 missiles, 11% of its Kalibr missiles, and 5% of its Kh-101 missiles remaining in its stockpiles. The International Institute for Strategic Studies (IISS)'s 2023 Military Balance estimated a drop in the number of modern main battle tanks in Russia by 50%.

New Evidence on Loopholes in the Sanctions Regime

According to our research and more comprehensive analysis conducted by the Kyiv School of Economics, Russia employs a range of evasion strategies in order to continue accessing essential components and defy the intent of the sanctions. An analysis of 1,057 foreign components of Russian military equipment produced by 155 companies and a detailed dataset on Russian trade pinpoints that Russia's military supply chain has continued to access Western critical technologies since the beginning of war, throughout 2022, and the first quarter of 2023.

The study identified that critical components found on the battlefield since April 2022 belong to a wide range of weapons and missiles, including Islander-K and Kalibr missiles; drones including Orlan and Korsar; armored vehicles and artillery including T-72 tanks, Tornado-G rockets, Typhoon-K vehicles; helicopters, electronic warfare stations, electronic warfare equipment, small electronic devices and others. The critical components include microchips, microprocessors, transistors, memory devices, voltage regulators, capacitors, transceivers, among others. These 155 companies – whose products were identified in Russian weapons – accounted for $2.9 billion of critical component sales to Russia in 2022. Despite sanctions, imports of these components have not stopped; after the initial drop of imports in April-May 2022, the volumes recovered to levels commensurate with trade from before the beginning of the war.

Moreover, the delivery has almost entirely been routed via third countries, whose share of indirect sales rose from 54% in 2021 to 98% in the fourth quarter of 2022. In the fourth quarter of 2022, more than three-fourths of sales to Russia were conducted via an intermediary in China, while in 2021, the corresponding amount had only been 22%. Consistent with earlier findings, the products are manufactured outside of China to a considerable extent.

The largest number of components are produced by US Analog Devices, US Texas Instruments, US Microchip Technology, US Intel Corporation, US AMD, German Infineon Technologies, and Korean Samsung. The export (dual use - with the exception of civilian products) of US critical components to Russia produced by Intel Corporation accounted for over USD 700 million in 2022, increasing from USD 500 million. Other estimates include USD 500 million for Samsung KR, USD 190 million for US Analog Devices, USD 180 million for US Texas Instruments, and USD 160 million each for US AMD and Xilnx.

The headquarters of many of these companies are located in the United States. Other locations include Japan, Germany, Switzerland, Taiwan, the Netherlands, and China. While the sellers to Russia mainly are from China, a small proportion also are in the European Union, South Korea, Vietnam, and Turkey. The producers are China, Vietnam, Malaysia, EU, and Taiwan.

In this study, we focus on two key dimensions of Russia's full-scale invasion of Ukraine, which is now entering its seventeenth month: (1) Russia's overall military capabilities in terms of key weapons systems, and (2) the extent of its continued reliance on imported components for military production. We have tried to identify the specific foreign components found in Russian equipment in Ukraine. We rely on a unique, comprehensive dataset on Russian international trade to reveal schemes to circumvent and/or violate sanctions, i.e., on dual-use and military goods export controls.

Key Findings:

1. **Reduced overall military capabilities.** Due to the critical role of imported components in Russian military production, international sanctions are having an impact on Russia's ability to manufacture key weapons systems, including armored vehicles, artillery, and missiles.
2. **Russia continues to wage war on Ukraine.** At the same time, Russia is clearly still able to produce key weapons systems. This is due to a combination of factors: (i) large stocks of key components; (ii) evasion of restrictions due to inconsistencies in export controls regimes; and (iii) sanctions violations and insufficient enforcement.
3. **Some high-tech inputs are missing.** Although Russia appears to have found ways to acquire many important inputs, they are not necessarily of the same quality and may also cost more. Thus, the lack of specific high-tech components has emerged as a major constraint.
4. **Western components are still appearing in Russian weapons.** We rely on the analysis of Russian weaponry captured on the battlefield – in total, 58 pieces of equipment, ranging from missiles and drones to armored vehicles and artillery – and find 1,057 individual foreign components with microchips and processors still used in manufacturing these weapons.
5. **Continued imports of critical Western components.** Using a comprehensive dataset on Russian international trade, we investigate imports of these "critical components" and find that they rebounded relatively quickly in 2022, within weeks, following an initial drop in the immediate aftermath of the imposition of sanctions.
6. **Russian ability to find alternative suppliers.** By the end of last year, imports of what we define as "critical components" had fully recovered and, in fact, risen above pre-sanction levels

for key items such as semiconductors.[1] China plays a key role – as an intermediary for shipments from other places as well as an alternative supplier.

7. **Initial indications in the first quarter of 2023 indicate a deceleration.** For a subset of critical components, we find that Russian imports declined in the first quarter of 2023 (see Box 1) – by 14% compared to the last quarter of 2022. This could indicate growing challenges regarding their acquisition – or more successful efforts to conceal transactions.
8. **Acquisition of Western goods via third countries.** We find that products of several specific companies in sanctions coalition countries continue to be shipped to Russia, mainly via China but also via Hong Kong and Turkey. In fact, imports from this subset have fully recovered in value terms.
9. **The export control regime is not as effective as needed.** Too many components from Western producers are finding their way to Russia, even if we recognize that some circumvention of export controls is unavoidable as entities in third countries may be outside the direct reach of the sanctions coalition.

Policy Recommendations:

Sanctions evasion cannot go unpunished. Companies that are registered in third countries presently serve as conduits, highlighting the inadequacy of current enforcement measures. Sanctions to reduce this tech transfer must be strengthened. Specially, we recommend comprehensive sanctions to specifically target trade categories that contain dual-use items and critical components in order to further disrupt Russia's military production capacity.

1. **Improve information exchange.** The first step to enforcing more effectively sanctions regarding military and dual-use goods export controls is better information. Detailed data on transactions should be made available in a timely manner, in particular for sensitive trade activities such as those with critical military or dual-use components. This includes data from customs services in sanctions coalition countries as well as data from third countries that can be acquired directly or through independent providers such as Export Genius. Authorities should set up systems through which information can be shared effectively. In addition, authorities in the 40+ country sanctions coalition should cooperate closely when it comes to investigations of sanctions violations or circumvention.
2. **Utilize financial sanctions and AML framework.** Restrictions regarding Russian (and third country) financial institutions – as well as cross-border transactions more generally – can be used to improve the implementation and enforcement of the export controls regime. Specifically, further restricting channels for transactions would allow for better monitoring and increased transparency. Schemes to violate or circumvent sanctions, including export controls, are similar to those that are being used for money laundering for which a regulatory framework is already in place to a substantial extent and should be applied to the area of export controls.
3. **Persuade key companies to voluntarily stop exporting to Russia.** Governments in the sanctions coalition should engage directly with the companies whose products are being exported to Russia. They should make these companies aware of how their products are being used to help kill Ukrainians. They should threaten to make public this data unless these

[1] In our analysis, we treat integrated circuits (HS code 8542) as part of semiconductors more broadly.

companies take more proactive measures to stop these tech transfers. Many large companies have extensive risk management and compliance structures, which would allow them to minimize the risk of unknowing violation of export controls. What is missing now is a sense of urgency. Major, publicly-traded companies should be interested in avoiding having their products identified in Russian weaponry found on the battlefield and/or being used for attacks on Ukrainian civilians. Small and medium-sized enterprises with less developed risk management systems may require technical assistance from authorities to improve their compliance.

4. **Enforce existing sanctions more effectively.** Sanctions implementing agencies need to demonstrate greater commitment to preventing and/or prosecuting violations. Simply opening investigations of major companies, and making the fact of these investigations public, would be a good first step.
5. **Align and broaden export control regimes.** Export controls target categories of dual-use goods with the highest likelihood of use for military purposes. However, this leaves loopholes through which Russia may be able to access critical inputs by misclassifying goods. Export controls should be expanded to cover broader categories to make circumvention harder and enforcement easier. It is also critical to align export controls across jurisdictions and enforce measures consistently to close loopholes in the regime.
6. **Tighten documentary evidence requirements.** Enhanced documentary requirements are key as well. For export controls, authorities should require end user agreements from all exporters, including companies under sanctions coalition jurisdiction that produce their products in, and export them from, third countries. Although legal enforcement of such agreements can be problematic, this requirement would encourage companies to undertake proper due diligence before engaging in any trade in military and dual-use goods.
7. **Target third-country intermediaries.** In addition to reducing the transfers of high-tech products from sanctions coalition countries, companies serving as the conduits for this transfer based in third countries must also be sanctioned. We recognize the relative ease (and low cost) with which new entities (i.e., shell companies) can be set up in third countries. These schemes represent a major challenge to the sanctions coalition. But these companies are helping Putin's war machine and can no longer be ignored; they must become targets of sanctions as well unless the change their behavior.
8. **Expand export controls coalition.** While several key countries still resist participating in the overall sanctions regime, we urge Ukraine's partners to intensify efforts to broaden the coalition specifically in the area of export controls. More cooperation should be achieved regarding the issue of dual-use goods, as these components directly contribute to Russia's targeting of civilians in Ukraine.

The urgency of implementing more and stricter measures to weaken Russia's capacity to wage war could not be greater. It is shameful that companies based in the democratic world are still providing technologies to Russia that help Putin and his army kill Ukrainians in an unprovoked war of aggression. In fact, most of the casualties from these weapons that incorporate Western technology are Ukrainian civilians. That must stop now.

II. Russia's Military Capabilities in 2023

Critical Role of Imported Components

Almost all of Russia's modern military hardware is dependent on complex electronics imported from the US, the UK, Germany, the Netherlands, Japan, Israel, and China.[2] In some instances, these components are civilian dual-use goods that can be procured commercially and whose transfer to Russia is harder to constrain via export controls.

The Royal United Services Institute (RUSI) estimates that Russia's military uses over 450 different types of foreign-made components in 27 different equipment systems. Many of these components are made by well-known US companies that create advanced microelectronics for the US military. In fact, only ten companies are responsible for more than 200 components (close to half of the total). And, most importantly, over 80 of these components are subject to US export controls – but Russia's military has nevertheless managed to obtain them, possibly through third-country intermediaries.[3]

While Russian weapons continue to contain these components, it is uncertain whether the companies producing these components were aware of their products' ultimate use by the Russian military. Russia has developed channels to conceal the origins of these items as well as their ultimate destination (Russia) by using third countries as intermediaries. For instance, a significant share of computer components found in Russian ballistic and cruise missiles are purportedly bought for non-military use in Russia's space program. Thus, ROSCOSMOS has been utilized by Russia as a means of acquiring technologies with both civilian and military applications. Additionally, there are numerous companies, including in the Czech Republic, Serbia, Armenia, Kazakhstan, Turkey, India, and China, that are willing to take substantial risks to fulfill Russian procurement demands.

A Nikkei[4] investigation has found that, since the start of the full-scale invasion in 2022, 75% of the US obtained by Russia were supplied through Hong Kong or China, while the manufacturers state that they have suspended all the operations and trade with Russia. Nikkei highlights that smaller, lesser-known chip traders and shell companies are able to evade US sanctions on Russia more easily, as they are not subject to the same level of scrutiny as larger, established distributors. Some of such distributors are already sanctioned by the US, but a majority still are operating.

For instance, Russian entities connected to a company called STC (Специальный технологический центр) in St. Petersburg have been importing Western-made components. STC produces the Orlan-10 drone and has close ties to the Russian government. Financial records and other sources suggest that a company called SMT-iLogic in St. Petersburg is purchasing many imports of critical Western-made components on behalf of STC. In the past, the US government has sanctioned STC for supporting Russia's interference in the 2016 U.S. presidential election.[5]

These components play a crucial role in Russia's drone production, enabling Russia to conduct cost-effective yet efficient coordinated reconnaissance and bombing of targets in Ukraine. The components are being shipped to Russia by companies based in the United States, Europe, China, South Korea, and Hong Kong. Some of these exporters appear to be run by Russian nationals or expatriates based abroad with limited public profiles.

[2] RUSI, Operation Z: The Death Throes of an Imperial Delusion, 2022
[3] RUSI, Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine, 2022
[4] Nikkei, Special report: How U.S.-made chips are flowing into Russia, 2023
[5] RUSI, The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV, 2022

It is worth noting that Russian companies must prove to the Russian Ministry of Defense that there is no domestic alternative before they can use foreign components in military equipment.[2]

According to the Free Russia Foundation[6], the sanctions regime created by the US and EU was able to disrupt the access to Western technology only in the short term. Russia has established alternative routes (mainly through China, Turkey, Cyprus, and the UAE) fairly quickly with imports of dual-use goods now exceeding pre-war levels. Russia's imports of microprocessors/semiconductors increased from $1.82 billion in 2021 to $2.45 billion in 2022 (for the year as a whole). In 2022, records indicate the import of unmanned aerial vehicles (UAVs) from China, Hong Kong, India, Turkey, and also European countries: the Netherlands and Germany.

The Free Russia Foundation report also states that there is a great deal of uncertainty, even among industry experts and association representatives, regarding the scope of the US ban on exporting chips to Russia, including which types of chips are subject to the ban.

However, some researchers are more positive about the effectiveness of sanctions. The Center for Strategic and International Studies (CSIS) writes in a report that shortages of certain higher-end components are forcing the Russian Ministry of Defense to substitute them with lower-quality alternatives.[7] These findings are based on usage patterns of Russian military equipment on the battlefield, for example, the use of less effective missiles outside of their intended purpose (for example, the use of the S-300, originally designed as a surface-to-air missile, in a surface-to-surface role). Overall, CSIS points to the following components, whose lack impedes Russian military production: advanced optical systems, bearings, engines, and microchips.

Overall Assessment of Military Capabilities

Although Russia has been implementing import substitution programs since 2014 with the goal of reducing the country's reliance on foreign components, particularly in its defense industry, its continued use of foreign-sourced high-tech components highlights a substantial ongoing dependence, which makes it susceptible to the imposition of export controls.

However, the impact of export controls is limited by several factors:

- **Long-term stocks.** Researchers found that Russia stores stocks for the execution of long-term contracts equivalent to approximately three years of production.[8] As a result, any restrictions targeting the production of military equipment will have a delayed impact. However, considering that production needs are much higher in wartime, Russia will likely have to expend such stocks this year.
- **Smuggling and other "gray schemes".** As discussed above, a number of cases have been identified that demonstrate sanctions evasion schemes. These include: (1) using intermediaries in countries, which are not under sanctions; (2) restructuring companies to conceal entities – or individuals – under sanctions; and (3) purchasing components and moving final assembly to Russia instead of buying finished sanctioned goods. Western components have also been found in drones supplied to Russia by Iran, which should have fallen under sanctions on the latter.
- **Inconsistent export controls and insufficient enforcement.** Evasion schemes such as the ones discussed above can only succeed due to weaknesses in the sanctions and export controls regimes. Insufficient enforcement, in particular as the identification of products' end users are

[6] Free Russia Foundation, Effectiveness of U.S. Sanctions Targeting Russian Companies and Individuals, 2023
[7] CSIS, Out of Stock? Assessing the Impact of Sanctions on Russia's Defense Industry, 2023
[8] The Jamestown Foundation, The Skyrocketing Costs for Russia's War Effort, 2022

concerned, are partly to blame. Enforcement is further complicated by the fact that the list of dual-use goods is not consistent among the sanctions coalition countries and does not align to the customs codes of the Harmonized System (HS). As a result, it is often difficult to determine whether a particular shipment is, or should have been, subject to sanctions. The US recently published a list of HS codes that warrant special attention.[9] We expect the EU to follow suit with its list of priorities soon.

While Russia's substantial stocks make military production somewhat resilient to sanctions and export controls, the lack of specific high-tech components has emerged as a major constraint. While Russian defense companies have been able to ramp up production through 24-hour operations, not all weapons and equipment now being produced contains state-of-the-art advanced electronics, leading to decreased effectiveness on the battlefield.

1. Tanks and Other Armored Vehicles

Uralvagonzavod is the only producer of tanks in Russia. In March 2022, the company was forced to halt operations due to a lack of components (mainly, bearings) following the imposition of export controls.[10] But by now, according to Rostec, production has, in fact, increased with the plant operating on a 24-hour basis.[11] To address a lack of qualified employees, 12-hour shifts have been implemented. Russia's ability to procure inputs from alternative sources is critical; in the case of bearings, Turkey was the largest supplier in 2022.

The plant's main task is not actually the production of new equipment, but, rather, modernization of the large number of older tanks Russia has pulled out of storage, as well as repair of damaged equipment. According to the Russian press, a key issue is the lack of Sosna-U multi-channel thermal imaging gunner's sights, meaning that the majority of tanks do not have this type of equipment.[12]

The situation is similar with regard to infantry fighting vehicles (IFVs). The main producer, Kurganmashzavod, now operates on a 24-hour basis as well and is mainly tasked with modernizing the large number of IFVs coming out of storage.[13]

Despite Russia's concerted efforts to increase capacities and acquire critical inputs through alternative channels, the number of tanks and IFVs has fallen considerably since the start of the full-scale invasion. The International Institute of Strategic Studies (IISS) analyzed a 39% reduction in active tanks and 20% drop in active IFVs, with the corresponding numbers for such vehicles in storage 51% and 53%, respectively (see Figure 1).

---

[9] Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts https://www.bis.doc.gov/index.php/documents/enforcement/3272-fincen-and-bis-joint-alert-final-508c/file, 2023

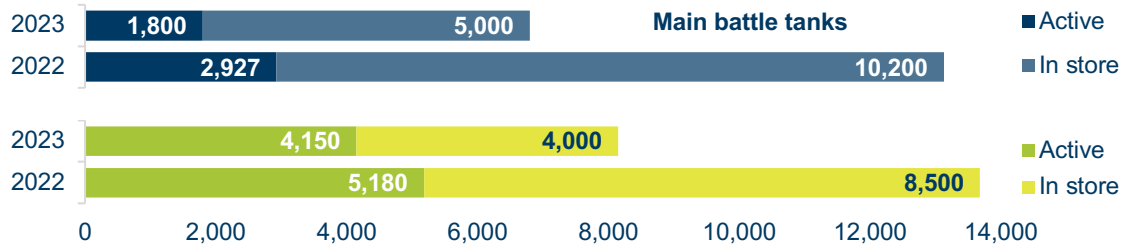
[10] Russian companies specializing in tank repair suspend operations due to supply shortages. https://kyivindependent.com/russian-companies-specializing-in-tank-repair-suspend-operations-due-to-supply-shortages/, 2022

[11] Russian Defense Chief Says Military Factories Working 'Around the Clock' https://www.themoscowtimes.com/2023/01/02/russian-defense-chief-says-military-factories-working-around-the-clock-a79864, 2023

[12] TopWar, New T-80BVM tanks for a special operation: it looks like they had to save on sights, 2023

[13] Ростех передал Минобороны РФ новую партию БМП-3 https://rostec.ru/news/rostekh-peredal-minoborony-rf-novuyu-partiyu-bmp-3/, 2023

Figure 1: Main battle tanks and infantry fighting vehicles



Source: International Institute for Strategic Studies, KSE Institute[14]

2. Artillery

Russia's military appears to encounter difficulties with the supply of artillery shells. The number of artillery rounds fired per day is down sharply – around 75% – from last summer, when the Russian military fired 40,000-50,000 rounds per day in the Donbas region.[15] However, remaining stocks are considerable, even if some are old and less reliable. Russia has already depleted ammunition stockpiles from Belarus, which is a further indicator that a renewed large-scale offensive from Belarussian territory is unlikely in the coming months.

3. Missiles

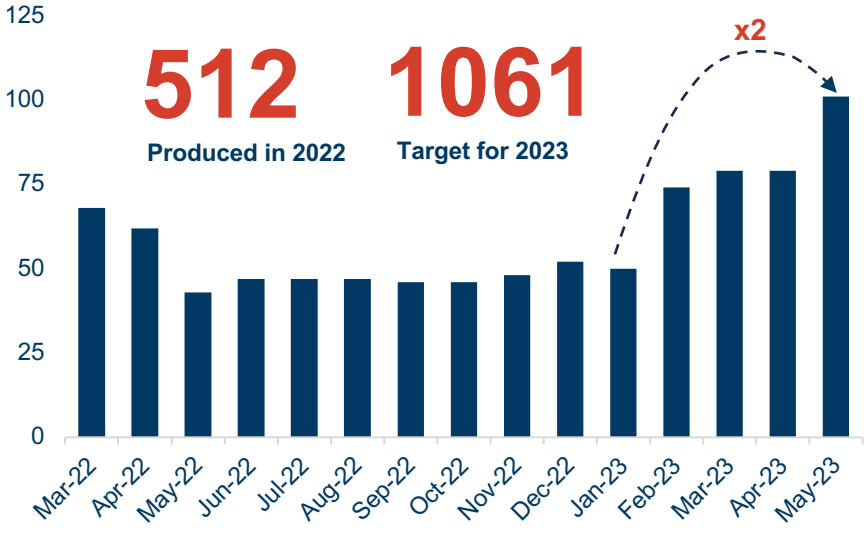
The intensity of missile attacks on the territory of Ukraine (critical infrastructure and civil and residential buildings) had decreased earlier in 2023. However, since the beginning of May, Russia has conducted constant attacks on civilian infrastructure with missiles and drones in response to the counteroffensive of the Ukrainian Armed Forces.

For this purpose, Russia is trying to ramp up production (see Figure 2) and reportedly is seeking to buy missiles from North Korea as well as additional drones from Iran, which are much lower cost in comparison.

The use of some missiles in an unorthodox fashion is a further indication for equipment constraints (see Figure 3). For example, attacks on the territory of Ukraine have been conducted using S-400 (and S-300) missiles, which were originally designed as air defense weapons – and are extremely imprecise when being used to hit targets on the ground. Another sign of the serious lack of cruise missiles in Russia's arsenal is the quick use of newly produced missile systems. Militaries prefer to use older missiles in stock before they use missiles produced more recently. The analysis of debris has shown that Russia has used cruise missiles in recent attacks that were produced in the first three months of 2023 – suggesting extremely low stocks.[16]

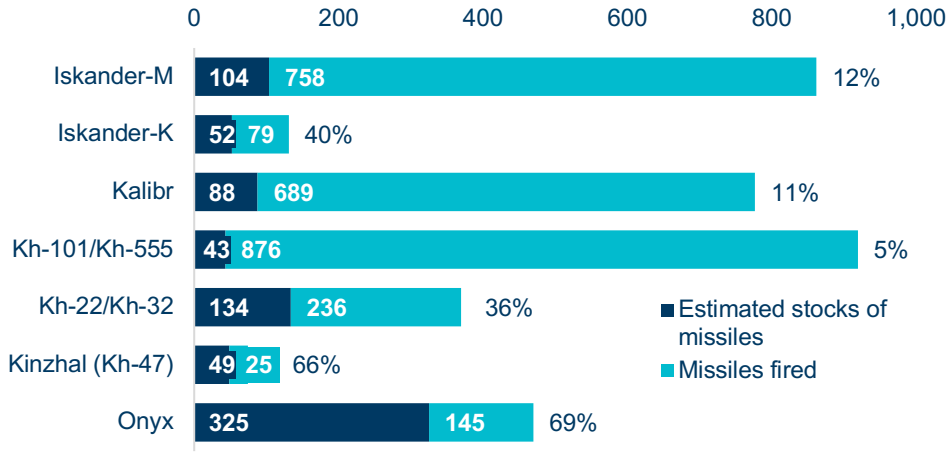
[14] IISS, Military Balance 2022 and Military balance 2023
[15] CNN, Russian artillery fire down nearly 75%, US officials say, in latest sign of struggles for Moscow, 2023
[16] RBC Ukraine, The hunt for Patriot and the failure of the counteroffensive. How Russia changed the targets of missile strikes, 2023

Figure 2: Russian Missile Production



Source: KSE Institute

Figure 3: Estimated Russian Missile Stocks as of 1 June 2023



Source: Ministry of Defense, RBC Ukraine, Jamestown Foundation, KSE Institute

In conclusion, Russia's military capacity seems to be impacted most by rapid usage and extraordinary losses on the battlefield. Given its inability to increase production significantly in the short term and limited access to some critical components, Russia is currently unable to rebuild its stocks fast enough to replace weapons that is has expended. However, due to the unprecedented scope of military and dual-use goods export controls, the effect should have been more pronounced. We believe that this indicates that restrictions may be violated and/or circumvented. To be able to identify specific issues associated with the export controls regime, we undertake a detailed analysis of trade with goods that we consider to be "critical".

III. Russian Imports of Critical Components

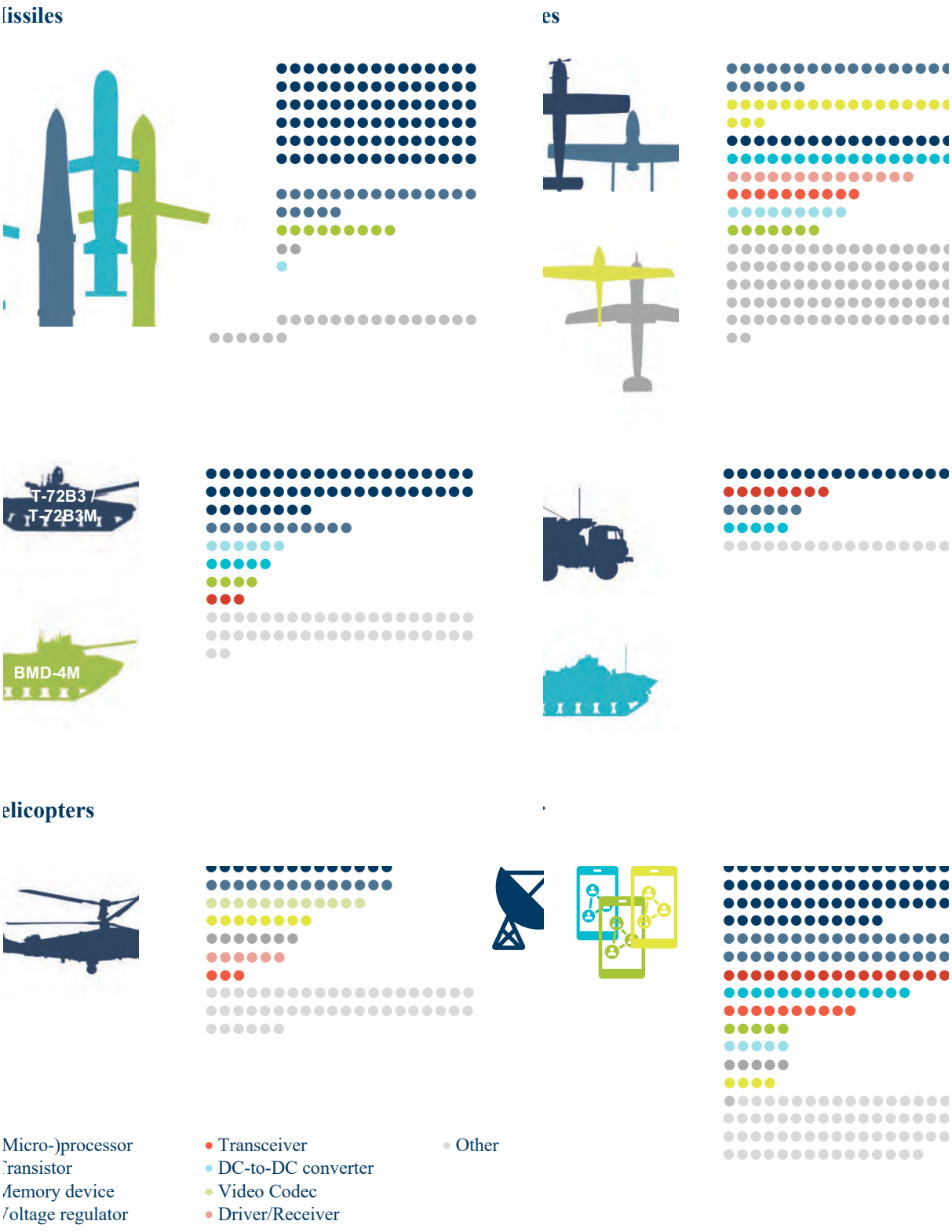
Analysis of Russian Military Equipment: Methodology and Key Findings

For our comprehensive analysis of trade trends regarding military and dual-use goods, we use information on Russian military equipment recovered on Ukrainian territory since the start of the full-scale invasion (see Figure 4) to develop a definition of "critical components".

1. In **58** pieces of Russian military equipment (see Figure 5a), we find a total of **1,057** individual foreign components.[17] Microchips and (micro-)processors together account for close to half of all components (see Figure 5b).
2. **155** companies are identified as producers of these components (see Figure 5c), with headquarters in **19** different countries (see Figure 5d).[18] Entities based in the United States are responsible for roughly two-thirds of the components found.
3. We identify all shipments from this subset of companies to Russia in 2022 by relying on a comprehensive, micro-level dataset on Russian trade. Trade data used in this analysis may not reflect all transactions between Russia and the countries of the Eurasian Economic Union, e.g., Belarus and Kazakhstan, as direct passing of the physical border of these countries to Russia are reflected in a separate database.
4. All 1,185 HS codes found in these transactions are analyzed on a case-by-case basis to determine which goods should be considered potential inputs for Russian military production and which are purely civil in nature.
5. We arrive at **385** ten-digit HS codes that define the set of "critical components" for our analysis of trade activities and potential export control violations.[19] Of these codes, only 170 – less than half – are included in the European Union's dual-use goods list.[20]

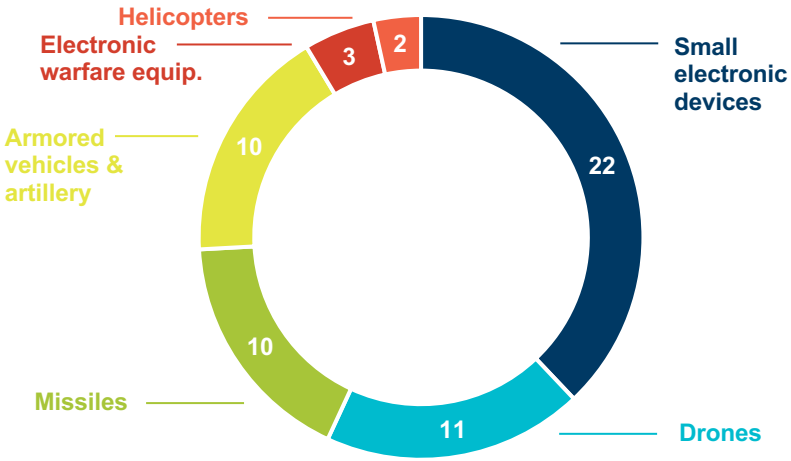
[17] Also includes 22 small electronic devices with 268 components. For details, see Appendix 1.
[18] For a full list of companies, see Appendix 2.
[19] For a full list of HS codes, see Appendix 3.
[20] For the EU list, see here. The comparison was undertaken at the 8-digit level.

Figure 4: Russian Military Equipment Analyzed and Components Found



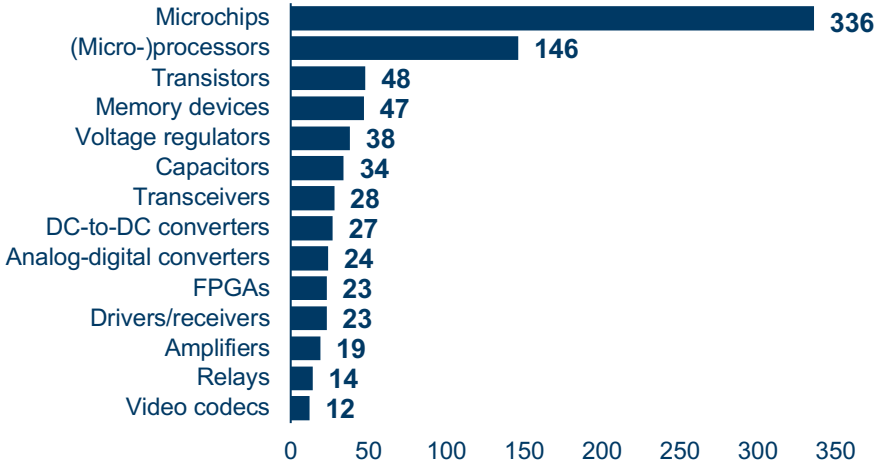
CSE | Institute

Figure 5a: Equipment by Type



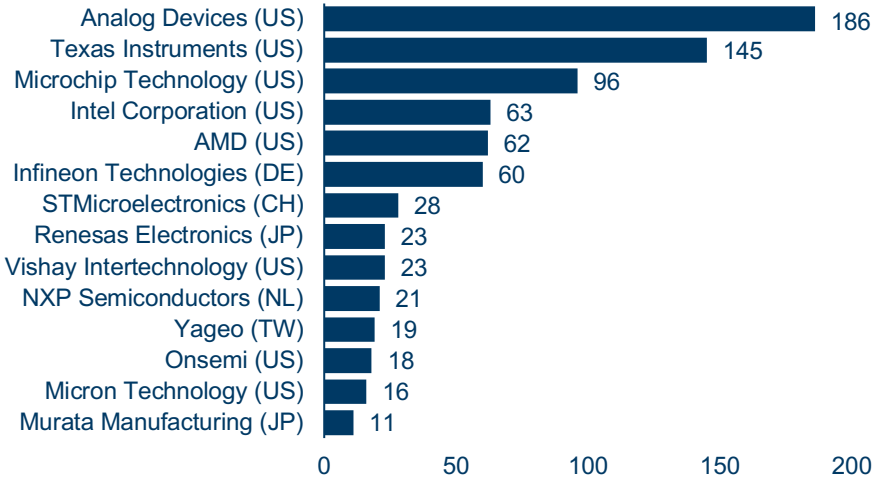
Source: KSE Institute

Figure 5b: Components by Type



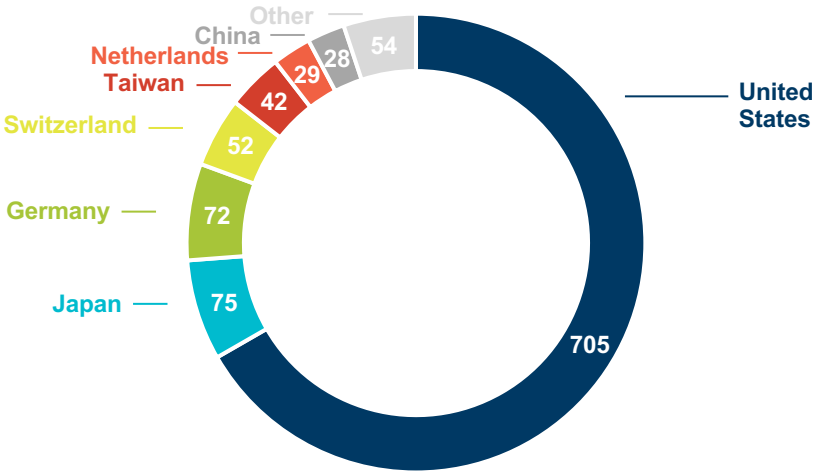
*Source: KSE Institute *not shown: 238 other components*

Figure 5c: Components by Producer



*Source: KSE Institute *not shown: 286 other components*

Figure 5d: Components by Headquarter



Source: KSE Institute

KSE | Institute

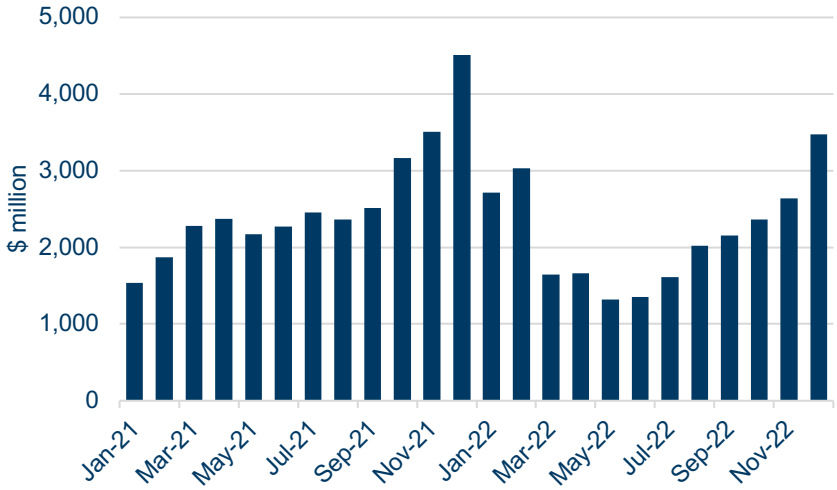
Analysis of Russian Imports of Critical Components

Overall Dynamics: Full Recovery by End-2022

In a first step, we analyze overall dynamics of "critical components" imports by Russia and find several key developments driven by Russia's full-scale invasion of Ukraine and the imposition of export controls by the sanctions coalition (see Figure 6).

1. **Build-up of stocks.** In the last quarter of 2021, imports of critical components picked up markedly, in particular in December – likely indicating the build up of stocks in anticipation of challenges regarding the acquisition of components critical for Russia's military production. Compared to the average of the first nine months of 2021 of $2.2 billion, imports were 44%, 59%, and 104% higher in October-December, respectively.[21]
2. **Post-sanctions drop.** Imports fell sharply in March-June 2022 as export controls were imposed by Ukraine's partners – by close to 50% compared to the January-February average of $2.9 billion when they had normalized following the end-2021 boom. This indicates that restrictions targeting Russia's defense sector, specifically military and dual-use goods export controls, clearly had an initial impact on trade activities.
3. **Recovery in the second half of 2022.** Starting in July, however, Russia appears to have adjusted. By the fourth quarter of 2022, imports of critical components reached close to $2.8 billion per month – up 9.3% compared to the 2021 average. Substitution of goods from sanctions-imposing countries may have played some role. But the absence of high-quality substitutes from alternative sources means that Russia likely succeeded in setting up schemes to import Western components through separate channels.
4. **Overall decline in full-2022.** For the year 2022 overall, critical components imports reached $26.0 billion – a 16% decline from the 2021 total of $31.0 billion. The drop is entirely due to the temporary collapse in March-June; imports in the fourth quarter of 2022 were $33.9 billion in annualized terms. Should imports remain at this level in 2023, this would mean a 30% increase over 2022 and 9% increase over 2021.

Figure 6: Imports of Critical Components



Source: KSE Institute

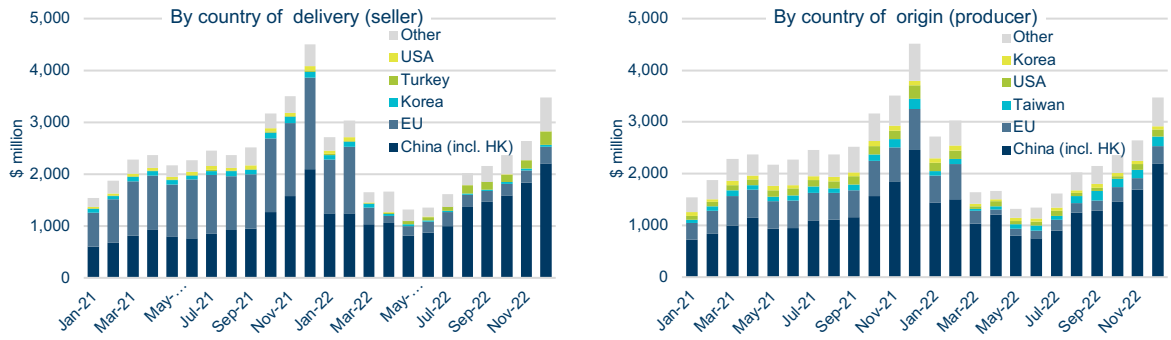
[21] We recognize that some of these dynamics may also at least partially represent a post-Covid recovery in trade.

Trade Channels: Rise of China

Second, we look at where critical components – as defined above – are acquired from. We find the following with regard to critical components' country of delivery, i.e., the country from which the goods were exported to Russia, and their country of origin, i.e., the country where the goods were produced (see Figure 7).

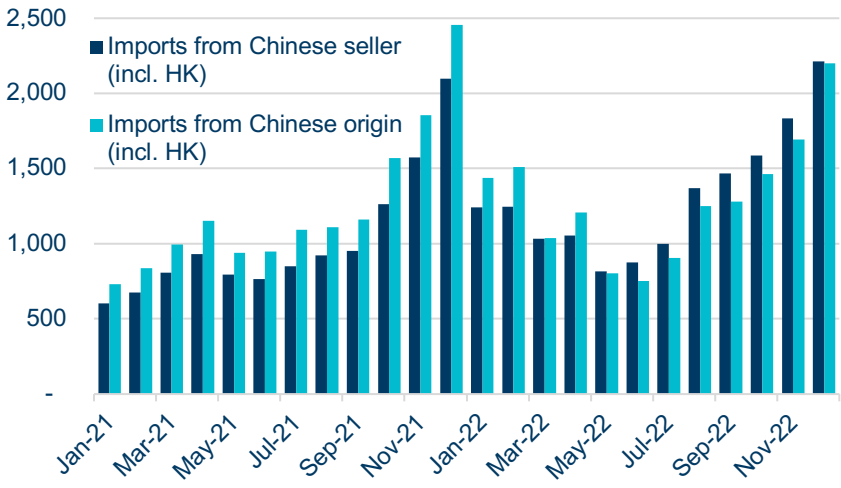
1. **Imports from China initially fell.** While China did not impose any export controls, Russian imports from the country also declined noticeably in the immediate aftermath of the full-scale invasion in February 2022. This was likely due to the fact that critical components either manufactured in China or sold via China are, ultimately, products of Western entities. Importantly, both categories are different from the country where the producer's headquarters are located geographically. Many companies, especially manufacturers of electronics, have relocated their factories to countries with lower costs, e.g., China.
2. **China's role expanded in 2022.** China's share of Russian imports of critical components has risen markedly since the imposition of export controls. By the fourth quarter of 2022, China's share as a country of delivery reached 53% (compared to 39% in 2021) and as a country of origin 63% (compared to 48% in 2021). The difference between the two suggests that a substantial share of Russian imports, around 10%, is now acquired from third-country manufacturers via Chinese and Hong Kong-based intermediaries (see Figure 8).

Figure 7: Imports of Critical Components by Country



Source: KSE Institute

Figure 8: Imports from China, Delivery vs. Origin



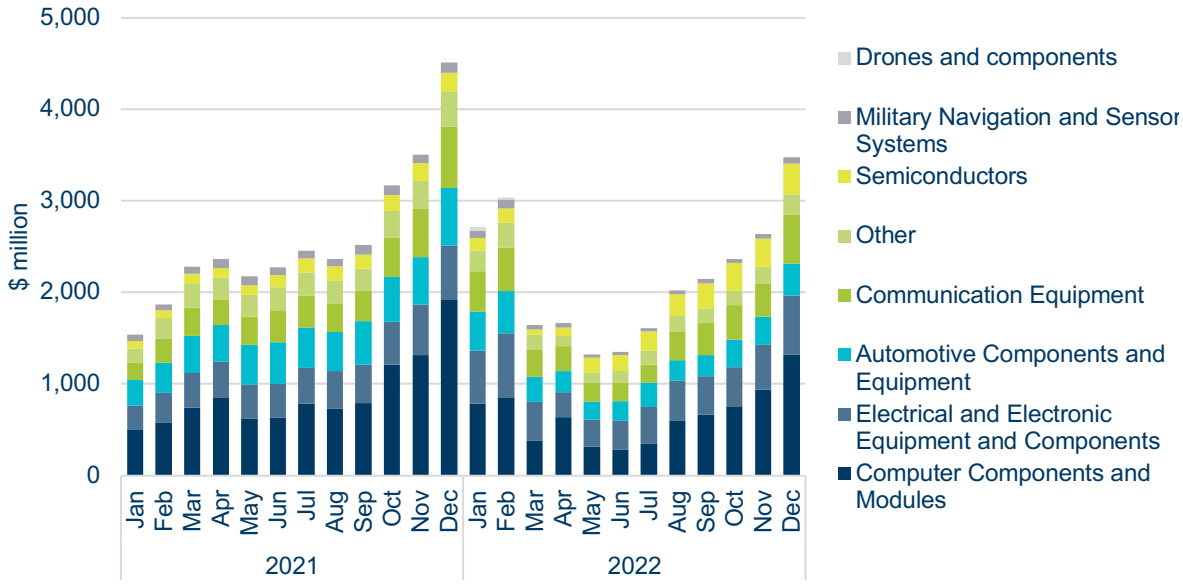
Source: KSE Institute

Import Composition: Semiconductors in Focus

Third, we investigate what types of critical components Russia has been importing and take a closer look at dynamics regarding semiconductors (and integrated circuits), a key target of export controls.

1. **Broad-based pickup in the second half of 2022.** The rebound in Russian imports of critical components towards the end of last year was relatively homogeneous across categories (see Figure 9). However, we find that some are of particular importance, e.g., computer components as well as electric and electronic equipment.[22]

Figure 9: Imports of Critical Components by Type



Source: KSE Institute

2. **Key role played by semiconductors**.[23] Semiconductors are of particular relevance for our analysis as they constitute the item most often found in Russian military equipment. In fact, Western-made microchips were identified in every type of equipment investigated by Ukrainian authorities. What sets these goods apart as well is that substitutes – for instance, Chinese ones – continue to lag Western products in technological advancement and quality.

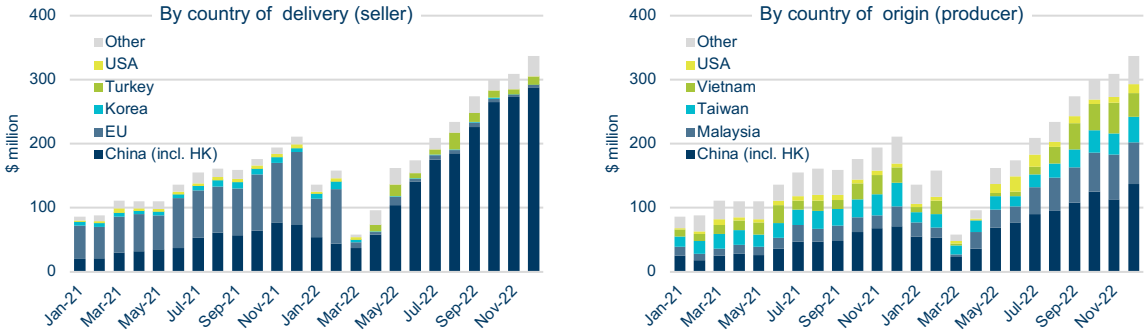
3. **Trends more pronounced.** For semiconductors, we identify similar developments as for overall critical components, including a late-2021 pickup (+56% in the fourth quarter vs the average of the first three quarters), a sharp drop in March-April (-48% vs. January-February), and a subsequent rebound (see Figure 10). However, two differences are noteworthy: (1) The drop following the imposition of export controls was even shorter-lived – imports had recovered to previous levels by May 2022. And (2), the surge in the second half of 2022 was much stronger – with imports in the fourth quarter of 2022 123% above the 2021 average. As a result, full-year imports in 2022 ($2.4 billion) came in 44% higher than in 2021 ($1.7 billion).

4. **Chinese intermediaries dominate.** In the fourth quarter of 2022, sellers from China (including Hong Kong) accounted for more than 87% of total Russian semiconductor imports, while the corresponding number for 2021 was only 33%. Importantly, the overwhelming share of goods

[22] In this group, we include items such as RAM modules, motherboards, graphics cards, and storage devices, which are widely used in commercial computers.
[23] Semiconductors here include integrated circuits (HS code 8542).

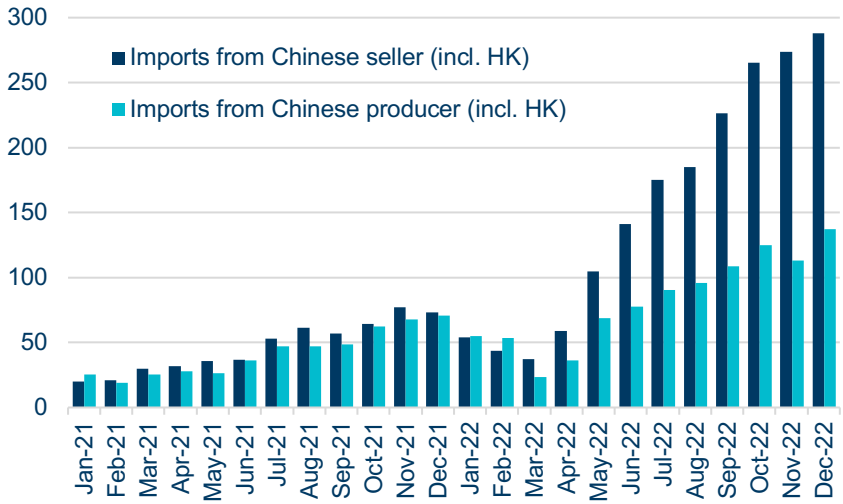
is not manufactured in China but rather shipped through Chinese and Hong Kong-based intermediaries, as a look at the country of delivery composition illustrates (see Figure 10). It appears that roughly 55% of semiconductors acquired from China (and Hong Kong) were in fact produced elsewhere (see Figure 11).

Figure 10: Imports of Semiconductors by Country



Source: KSE Institute

Figure 11: Semiconductor Imports from China, Delivery vs. Origin



Source: KSE Institute

Company Analysis: Business with Russia Continues

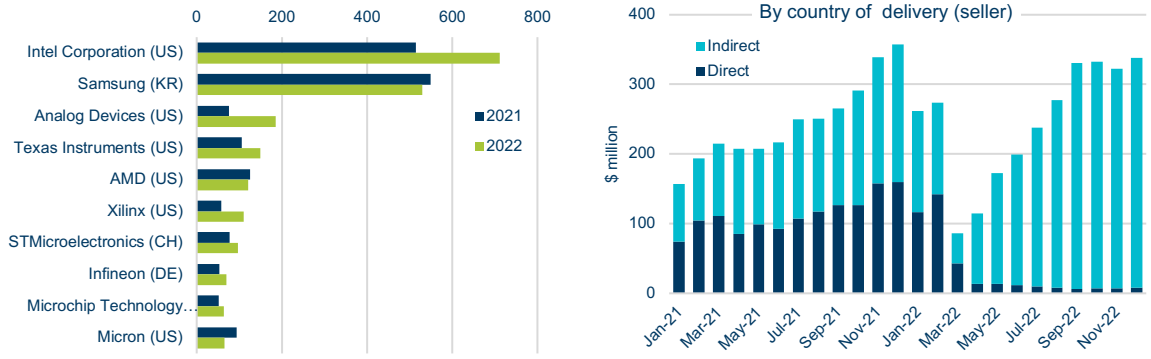
Fourth, we focus on the subset of 155 companies (including subsidiaries) whose products were identified in Russian weapons. These accounted for 11% of critical component sales to Russia in 2022 – or $2.9 billion.

1. **Sales to Russia rebound quickly.** For these companies – among them some of the biggest Western manufacturers of electronics – we, again, find the typical pattern in Russian imports of a late-2021 surge, March-April 2022 drop, and recovery in the second half of 2022 (see Figure 12). In fact, their exports of critical components to Russia stood 35% above their 2021 average in the final quarter of 2022. For the full year, this means essentially no change versus 2021.

2. **Business entirely through intermediaries.** Importantly, shipments are almost entirely routed via third countries now (see Figure 12) – the share of indirect sales rose from 54% in 2021 to

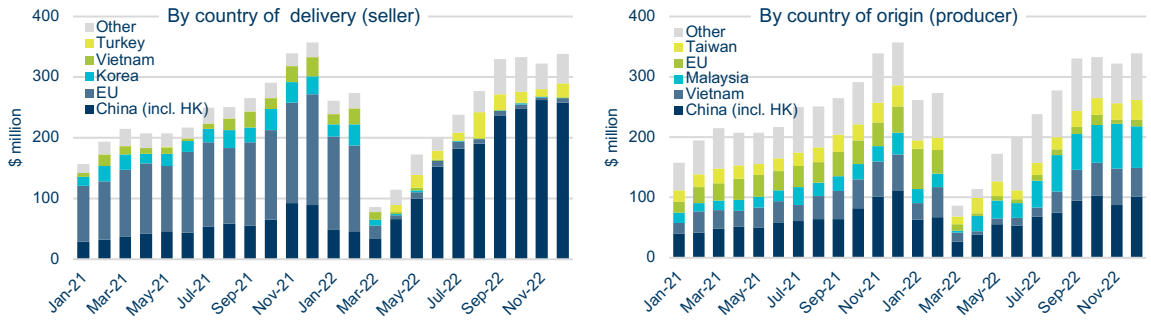
98% in the fourth quarter of 2022. China is, again, playing a critical role (see Figure 13). In the fourth quarter of 2022, more than three-fourths of sales to Russia were conducted via an intermediary in China; in 2021, the corresponding number had only been 22%. And, consistent with earlier findings, the products are, to a considerable extent, manufactured outside of China.

Figure 12: Composition of Imports from Select Companies



Source: KSE Institute

Figure 13: Imports from Select Companies by Country

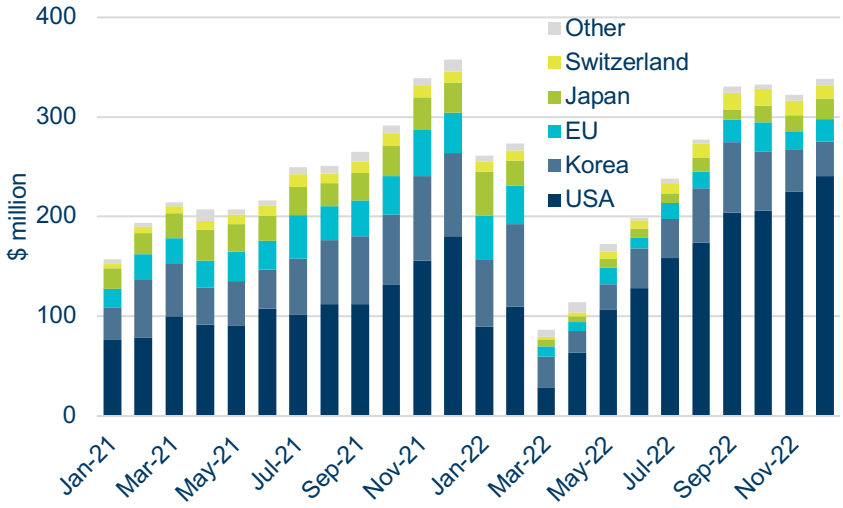


Source: KSE Institute

3. **US-based companies dominate.** A closer look at the companies involved shows that US-based entities represent the largest share – and it has in fact increased since the full-scale invasion (see Figure 14). In 2021, US companies accounted for 45% of Russia's imports; by the fourth quarter of 2022, this number rose to 68%. South Korean entities are the second-biggest player, but their share has fallen from 23% to 14%.

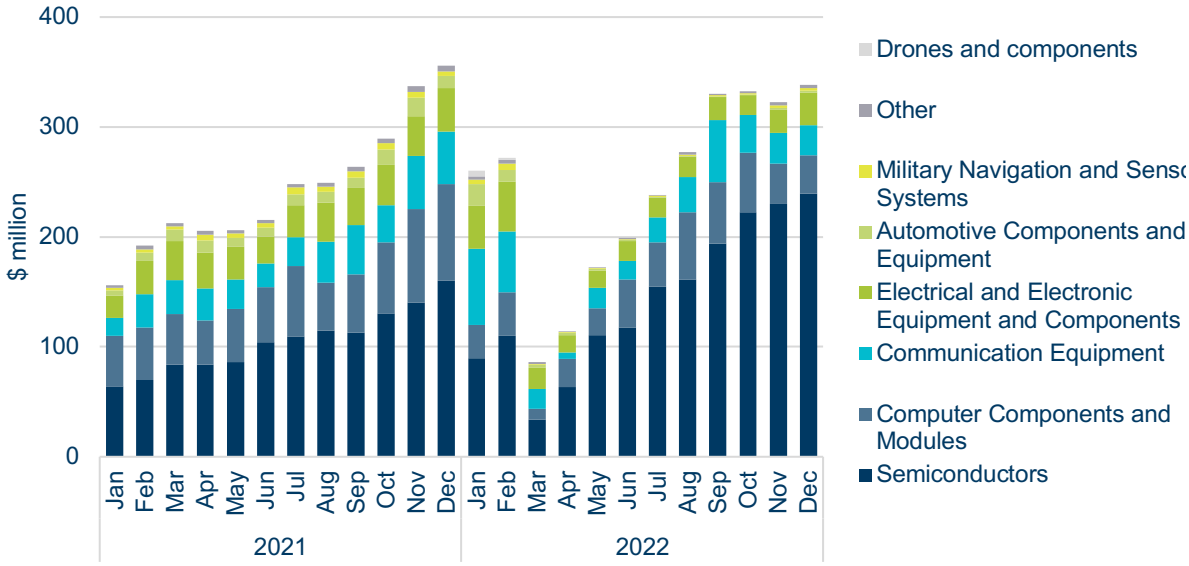
4. **Continued sales of semiconductors.** In line with our earlier finding that high-quality substitutes for Western semiconductors are difficult to find, we see that these products have grown in importance. Not only have their sales to Russia more than recovered from the post-sanction drop (+120% in the fourth quarter of 2022 vs. 2021 average), semiconductors make up a larger share of the total now – 70% in the fourth quarter of 2022 vs. 43% in 2021 (see Figure 15).

Figure 14: Imports by Location of Headquarter



Source: KSE Institute

Figure 15: Imports from Select Companies by Type



Source: KSE Institute

Key Companies: How Western Critical Components Reach Russia

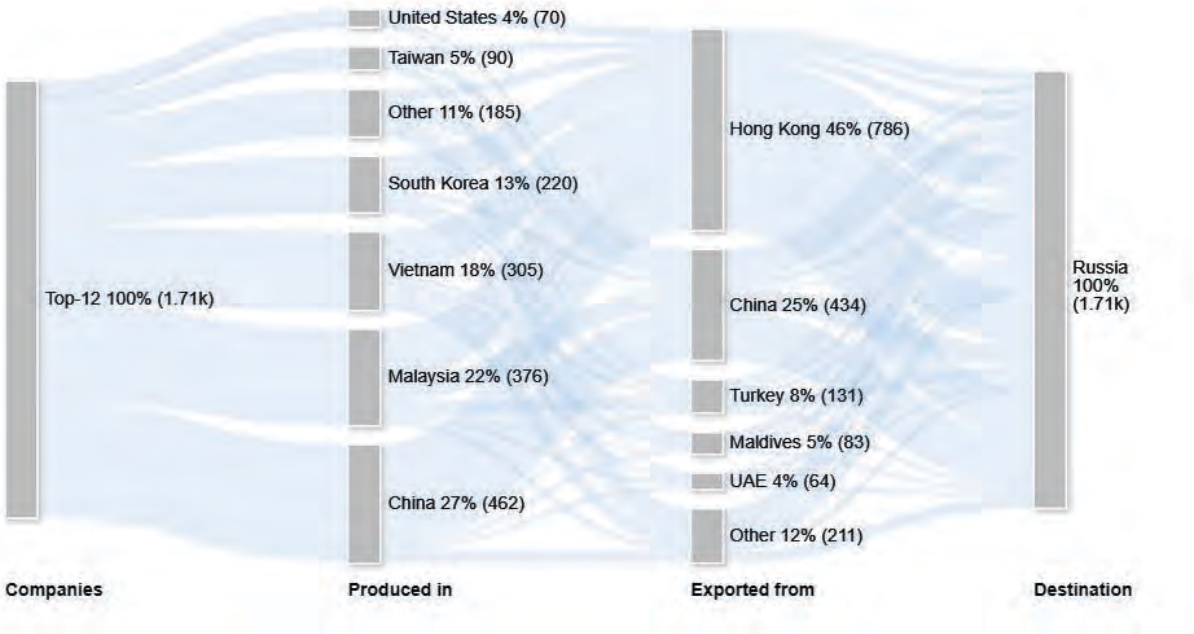
Finally, we analyze how goods produced on behalf of major Western companies reached Russia in March-December 2022 (see Figure 16):[24]

1. **Production locations.** Close to 80% of all critical components were produced in four countries: China (27%), Malaysia (22%), Vietnam (18%), and South Korea (13%).

[24] The sample of 12 companies includes AMD, Analog Devices, Infineon, Intel, LG, Microchip Technology, Renesas, Samsung, Safran, STMicroelectronics, Texas Instruments, and Thales, which accounted for roughly $1.7 billion in Russian imports of critical components in March-December 2022.

2. **Export locations.** In terms of the countries from which these goods were ultimately exported to Russia, three are of particular importance and together account for, again, close to 80% of the total: Hong Kong (46%), China (25%), and Turkey (8%).
3. **Structures differ across companies.** We do not find a common pattern; goods from different producers are manufactured in different locations and reach Russia through different countries and intermediaries (see Appendix 4).

Figure 16: Flow of Major Companies' Goods to Russia in March-December 2022



Source: KSE Institute

** Charts show Russian imports of critical components from the twelve largest suppliers in March-December 2022; percentages show distribution on each level and numbers in parentheses denote trade values in $ million in March-December 2022*

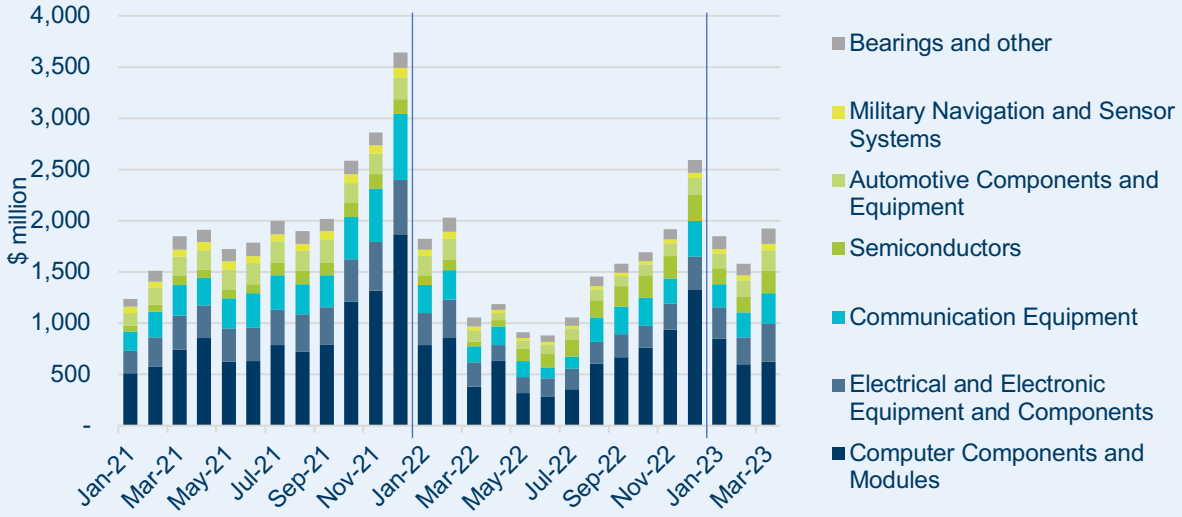
Box 1. Components Trade in 2023

Based on partial data for a subset of goods – 223 of the 386 10-digit codes included in our main analysis – we can investigate how trade with certain "critical components" developed in the first quarters of 2023.[25] In the first three months of the year, Russian imports of these products reached $5.4 billion, a 14% drop compared to the last quarter of 2022 (see Figure 17). While this may indicate a reduced ability to acquire key inputs for military production, it could also represent more successful concealment of transactions.

While we see a decline in imports in the first quarter of 2023 overall, some subcategories recorded significant increases, including electrical and electronic equipment and components (+18% vs. the fourth quarter of 2022), automotive components and equipment (+24%), military navigation and sensor systems (+27%), and bearings and similar parts (+28%).

For one of the most important categories of "critical components" – semiconductors[26] – we find a 23% decrease from the fourth quarter of 2022 to the first quarter of 2023.[27] 44% of their first quarter of 2023 imports were produced in – and 83% shipped to Russia from – China, including Hong Kong (see Figure 18). While China dominates in these categories, it is important to emphasize, again, that these goods are to a large extent manufactured by companies with headquarters in the West, including in the US and EU., using their global production infrastructure.

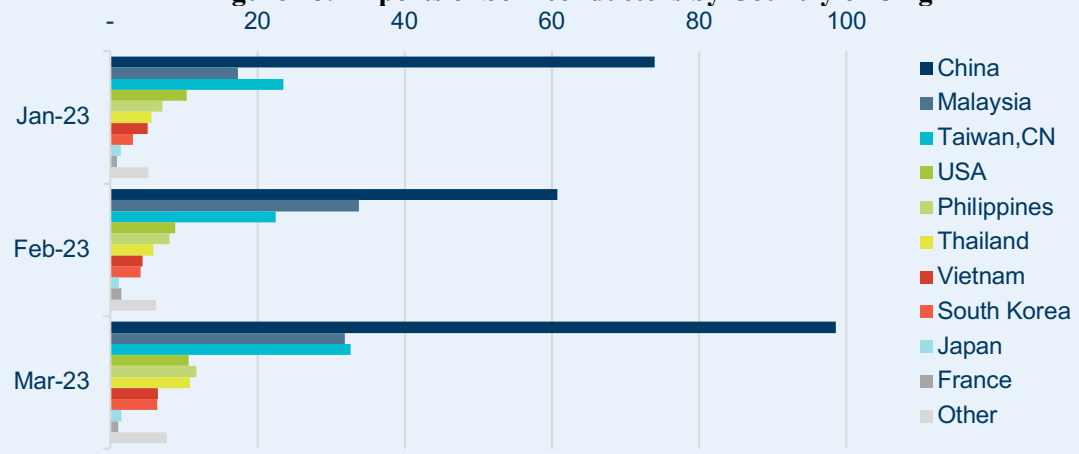
Figure 17: Imports of Critical Components by Type



Source: KSE Institute

[25] Russian imports of this subset amounted to $6.2 billion in the fourth quarter of 2022 – close to 70% of the total for all 386 codes ($8.5 billion). For full-2022, the share was also 70% ($18.2 billion vs. $26.0 billion).
[26] Including integrated circuits.
[27] The subset includes 14 codes in the area of semiconductors versus 37 codes used in the full analysis. Imports of those goods amounted to $692 million in the fourth quarter of 2022 – 75% of the total for all semiconductor categories ($947 million). For full-2022, the respective share was also 75% ($1.8 billion vs. $2.4 billion).

Figure 18: Imports of Semiconductors by Country of Origin



Source: KSE Institute

IV. Policy Recommendations: Increased Enforcement

We find that continued imports of critical components by Russia are manifestations of several separate issues of the export controls regimes: (1) Entities under coalition jurisdiction engage in **sanctions violations**; in other words, they undertake activities that are illegal. (2) Entities under coalition jurisdiction engage in **sanctions circumvention**; in other words, they undertake activities that are legal but opposed to the sanctions regimes' objectives. (3) Entities outside of coalition jurisdiction, i.e., **third-country actors**, contribute to sanctions violations and/or circumvention. These distinct phenomena require specific policy responses.

It is important to recognize that certain potential inputs for military production are still not covered by export controls. As a result, Russian imports of some critical components do not in all cases represent sanctions violations and/or circumvention.

Limiting Russia's access to inputs for its military production should be a top priority for Ukraine's partners; almost no other single issue is so directly linked to the objective of bringing Russia's war of aggression, including its attacks on civilians, to an end, and minimizing the risk of Russia's future aggression. Thus, we believe that the area of export controls is where the coalition should undertake decisive measures – and where it should focus its enforcement capabilities.

To improve enforcement:

Information exchange. In our view, the first step to more effective enforcement of military and dual-use goods export controls is better exchange of information. Detailed data on transactions is available in a timely manner, including for sensitive trade activities such as those with critical military or dual-use components. This includes data from customs services in sanctions coalition countries as well as data from third countries that can be acquired directly or through independent providers such as Export Genius. Authorities should set up systems through which information can be shared effectively – including by the academic/think tank community.

Joint investigations. In addition to the exchange of information, authorities in coalition countries should cooperate closely when it comes to investigations of sanctions violations or circumvention. Often, trade with critical components involves multiple actors in many

jurisdictions, which cannot be investigated by any single agency. Joint efforts in this area would also limit the extent to which nefarious actors can do "jurisdiction shopping". Especially in the European Union, where sanctions (and export controls) implementation remains the responsibility of member states, improvements are of critical importance.

Utilization of Anti-Money Laundering (AML) framework. Schemes to violate or circumvent sanctions, including export controls, are similar to those that are being used for money laundering or proliferation, including opaque ownership structures and frequent changes to structures and actors involved in activities. This also means, however, that the regulatory framework for the monitoring of these schemes is already in place to a substantial extent. Sanctions coalition authorities should vigorously enforce existing regulations and apply them to the area of export controls. In particular, the AML framework can be applied to track structures in third countries which are of critical importance for both production and exports to Russia of many inputs for military production. As we illustrated above, many of these goods do not ever physically touch sanctions coalition jurisdiction.

Financial sector measures. We believe that financial sector sanctions can play a critical role in the enforcement of other restrictions – from export controls to the G7/EU oil price caps – due to financial institutions' critical role in cross-border transactions. Limiting channels through which Russian entities can make payments for imports should be limited through additional sanctions on Russian banks. This would leave specific channels that can be monitored more effectively. Companies should also be required to provide information to banks if they are asking to process payments for shipments of goods that may be under export-controls.

<u>To address sanctions violations:</u>

Engagement with key companies. Authorities should engage with the companies whose products are being exported to Russia. Many large companies have extensive risk management and compliance structures which would allow them to minimize the risk of unknowing violations of export controls; what is likely missing at this point is a sense of urgency. From a public opinion perspective, companies should be very interested in avoiding having their products identified in Russian weaponry found on the battlefield or being used for attacks on Ukrainian civilians. As far as small-and-medium enterprises (SMEs) are concerned, these may actually lack the capacity to conduct the kind of due diligence necessary. Thus, authorities should consider providing technical assistance to enable them to track their products and limit the extent of involuntary export control violations.

Sharing of information with stakeholders. Clear guidance on sanctions is an important element of such an approach as well and will need to be reviewed at regular intervals, since circumvention networks adapt quickly to enforcement efforts. Companies would also benefit from establishment of a database through which they could access information about (potential) business partners, including company structures, ownership, coverage by sanctions and/or information about previous violations. These are critical inputs for any entity's risk assessments and need to be made available in a convenient and timely fashion.[28]

[28] To get banks' "Know-your-client" (KYC) attention, a list of third-country companies should also be indexed by FACTIVA – a major business intelligence platform owned by Dow Jones. It accumulates information from a wide scope of media sources, but not scientific publications. Once included, this information will appear every time a KYC or risk management procedure is conducted.

Demonstration of consequences. We find that many of the critical components that Russia continues to be able to acquire are produced in factories owned by Western companies but located in third countries. These firms do not appear to be undertaking sufficient due diligence as far as goods under export controls are concerned. Thus, we believe that implementing agencies need to demonstrate their commitment to preventing and/or prosecuting violations by undertaking investigations regarding high-profile players, including for production by their facilities in third countries.

Documentary evidence requirements. As in other areas of the sanctions complex, we believe that enhanced documentary requirements are key as well. They should also be accompanied by clear assignments of responsibilities for the approval of transactions within companies.[29]

To address sanctions circumvention:

Dual-use goods lists alignment. It is critical that authorities across the sanctions coalition align their export control regimes to close existing loopholes. The same goods should be classified as "dual use" in all countries, and criteria for licensed approval should be standardized. In addition, it is critical that authorities define dual-use goods based on Harmonized System (HS) codes; otherwise, the monitoring of transactions will be significantly more challenging.

Broader export controls. In several areas, export controls target very specific goods while similar products remain excluded; as a result, the sanctions regime may miss substitutes for controlled goods. For instance, of the 385 codes that we use for our definition of "critical components," only 170 are included in the EU's list of dual-use goods.[30] This could also allow sellers and buyers to misclassify the content of shipments on customs declarations – betting that no thorough physical inspection of the goods will be undertaken. The issue is further complicated by the fact that substantial advance knowledge is necessary to be able to identify specific equipment types and distinguish export controlled and non-export-controlled goods. Exemptions for specific uses, e.g., imports by Rosatom, also represent a problem. As long as critical components are approved for export to Russia for any reason, they will end up being diverted and used for the war effort, rendering any controls ineffective.

To address third-country actors:

Threat of secondary sanctions. The United States has previously used so-called secondary sanctions to target third-country actors that engage with sanctioned entities. The key for this kind of extraterritorial application of sanctions is the threat to cut off entities from access to the US dollar and the US financial system. While such measures are controversial and should, thus, be employed in a selective fashion, they can be extraordinarily effective in addressing third-country loopholes. In many cases, entities in third countries do not want to run afoul of the Office of Foreign Assets Control (OFAC) and face the aforementioned penalties. Thus, targeted threats of secondary sanctions may be sufficient to entice cooperation in key areas.

New legal instrument in the EU. The European Union is fundamentally opposed to the extraterritorial application of sanctions and, in fact, prohibits EU-based companies from following such restrictions through the "blocking statute". However, the EU should create a new legal basis for the imposition of restrictions on third-country entities, which act as

[29] For export controls, authorities could require end user agreements from all exporters, including companies under coalition jurisdiction that produce their products in and export them from third countries. While the legal enforceability of such agreements can be problematic, this would entice companies to undertake proper due diligence before engaging in any trade with military/dual-use goods.
[30] For the EU list, see here.

intermediaries and contribute to sanctions violations by EU actors.[31] The EU is also considering imposing export bans, i.e., to restrict the sale, supply, transfer, or export of certain technologies and goods to third countries that are used by Russia as intermediaries.

Robust monitoring of schemes. We recognize that the relative ease (and low cost) with which new entities (i.e., shell companies) can be set up in third countries represents a major challenge. Authorities, thus, need to constantly monitor developments utilizing all available data sources to identify how schemes adjust to restrictions – and revise the sanctions regime accordingly.

Provision of technical assistance. It should not be underestimated that some third-country entities may face substantial capacity constraints when it comes to the monitoring of shipments to Russia in the context of the export controls regime. In particular, small and medium-sized enterprises (SMEs) may not be able to conduct the kind of due diligence that would lead to the identification of problematic transactions. Sanctions coalition authorities should consider providing technical assistance to these actors to reduce the number of cases in which these counteract the objective of export controls unknowingly or unintentionally.

[31] Official press report: https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2661

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.

Anne Clunan, Associate Professor of National Security Affairs, Naval Postgraduate School; Faculty Affiliate, Center for International Security and Cooperation (CISAC), Stanford University. *The views here are my own, and not those of the U.S. Navy, Department of Defense, or Government.*

Tatyana Deryugina, Associate Professor of Finance, University of Illinois.

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.

Denis Gutenko, Ukrainian Emerging Leaders Program Fellow, Stanford University, and Former Head of the State Fiscal Service of Ukraine.

James Hodson, Director and Chief Executive Officer, AI for Good Foundation; Co-organizer of the Economists for Ukraine group.

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

Bronte Kass, Program Manager, Freeman Spogli Institute for International Studies (FSI), Stanford University; Assistant Coordinator, International Working Group on Russian Sanctions.

Dr. Craig Kennedy, Center Associate, Davis Center for Russian and Eurasian Studies, Harvard University, and Former Vice Chairman, Bank of America Merrill Lynch.

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.

Olesksandr Novikov, National Agency on Corruption Prevention, Ukraine.

Steven Pifer, Affiliate, Center for International Security and Cooperation, Stanford University.

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

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.

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

Jeffrey A. Sonnenfeld, Senior Associate Dean for Leadership Studies and Lester Crown Professor of Leadership Practice, Yale School of Management.

Dr. Kathryn Stoner, Mosbacher Director and Senior Fellow, Center for Democracy Development and Rule of Law (CDDRL), and Professor, Freeman Spogli Institute for International Studies (FSI), Stanford University.

Pavlo Verkhniatskyi, Managing Partner, Director, COSA.

Vladyslav Vlasiuk, Assistant Coordinator, International Working Group on Russian Sanctions.

Agiya Zagrebelska, National Agency on Corruption Prevention, Ukraine.

V. Appendix

Appendix 1: Summary of Equipment and Foreign Components

	Armored vehicles & artillery	Drones	Electronic warfare equipment	Helicopters	Missiles	Small electronic devices	**Total**
Microchips	48	18	19	14	145	92	**336**
(Micro-)processors	11	46	6	14	30	39	**146**
Transistors	5	18	5	1	5	14	**48**
Memory devices	4	7		17	14	5	**47**
Voltage regulators	1	23		8	2	4	**38**
Capacitors	3	1	8		3	19	**34**
Transceivers		10		3	5	10	**28**
DC-to-DC converters	6	9		1	6	5	**27**
Analog-digital converters	2	5	1	3	4	9	**24**
FPGAs	1	2	1	7	7	5	**23**
Drivers/receivers	1	14		6		2	**23**
Amplifiers	2	7		1		9	**19**
Relays	3	1	2		1	7	**14**
Video codecs				12			**12**
Other	32	86	16	40	16	48	**238**
Total	**119**	**247**	**58**	**127**	**238**	**268**	**1,057**

Appendix 2: Foreign Companies Identified in Russian Weapons

Company	**Headquarters**	**Items**	**Company**	**Headquarters**	**Items**
Analog Devices	United States	186	MaxLinear	United States	1
Texas Instruments	United States	145	Voltage Multipliers	United States	1
Microchip Technology	United States	96	Token Electronics	China	1
Intel Corporation	United States	63	Michelin	France	1
AMD	United States	62	Ramtron International	United States	1
Infineon Technologies	Germany	60	DFRobot Electronics	United States	1
STMicroelectronics	Switzerland	28	Cornell Dubilier	United States	1
Renesas Electronics	Japan	23	SECURON	United Kingdom	1
Vishay Intertechnologies	United States	23	TTM Technologies	United States	1
NXP Semiconductor	Netherlands	21	Hextronik	United States	1
Yageo	Taiwan	19	Deyuan Technology	China	1
Onsemi	United States	18	Lantronix	United States	1
Micron Technologies	United States	16	Hongfa	China	1
Murata Manufacturing	Japan	11	Delta Electronics	Taiwan	1
Kyocera	Japan	9	Real Support Electr.	China	1
Traco Electronic	Switzerland	9	Axis	Sweden	1
TE Connectivity	Switzerland	8	Kodenshi Corporation	South Korea	1
Merrimac Industries	United States	6	Controp	Israel	1
Anderson Electronics	United States	6	Silicon Laboratories	United States	1
SMC Corporation	Japan	6	Semicon	South Korea	1
Nexperia	Netherlands	5	Guangdong Kexin Ind.	China	1
Holt Integrated Circuits	United States	5	Inchange Semiconductor	China	1
XP-Power	Singapore	5	Nippon Instruments	Japan	1
U-blox	Switzerland	5	Hirose Electric	Japan	1
Samsung Electronics	South Korea	4	Souriau	France	1
Marvell Semiconductor	United States	4	Poccio Electronics	China	1
Thales	France	4	Telpod	Poland	1
Motorola	United States	4	Future Tech. Dev. Int.	United Kingdom	1

TT Electronics	United Kingdom	4	TCB WORTH	China	1
Littelfuse	United States	4	Kioxia	Taiwan	1
Alliance Memory	United States	4	Z-Communications	United States	1
Scientific Components	United States	3	Epson	Japan	1
IC Haus GmbH	Germany	3	Wolfspeed	China	1
Macronix International	Taiwan	3	ADLINK	Taiwan	1
Bourns	United States	3	iFlight	China	1
Sumida Corporation	Japan	3	3D Plus	United States	1
VBSsemi	China	3	Scorpion Power System	China	1
Macom	United States	3	NVE Corporation	United States	1
Hitano Enterprise	Taiwan	3	Ligitek Photovoltaic	Taiwan	1
Broadcom Corporation	United States	3	Integrated Circuit Syst.	United States	1
Harting	Germany	3	Productwell	China	1
Sony	Japan	3	HEICO	United States	1
Vicor	United States	3	Molex Electronics	United States	1
Silex Technology	United States	3	Nanya Technology Corp.	Taiwan	1
Philips	Netherlands	3	Mercury	United States	1
Mornsun	China	3	M-TRON	United States	1
IDEC Corporation	France	2	Eaton Electronics	United States	1
Toshiba	Japan	2	Dyna Logic	South Korea	1
Semtech Corporation	United States	2	CML Microsystems	United Kingdom	1
CTS Corporation	United States	2	Futaba Corporation	Taiwan	1
Wurth Elektronik	Germany	2	Golledge Electronics	United Kingdom	1
TDK Corporation	Japan	2	Kuwes Industry Corp.	Taiwan	1
Qorvo	United States	2	Timoney Technology	Ireland	1
Fujitsu	Japan	2	Advanced Digital	United States	1
New Jersey Semicond.	United States	2	Shenzhen Joy Battery	China	1
Amphenol	United States	2	Cortina Systems	United States	1
UN Semiconductor	China	2	Transcend	Taiwan	1
HALO Electronics	United States	2	Greenliant	United States	1
Winbond	Taiwan	2	Sonitron	Belgium	1
Hitec RCD	South Korea	2	DM&P Electronics	Taiwan	1
NGK	Japan	2	CANON	Japan	1
Hemisphere GNSS	United States	2	Lattice Semiconductor	United States	1
Anaren	United States	2	ОКБ “Фотон”	Uzbekistan	1
Bolymin	Taiwan	2	Finntek	Taiwan	1
OMRON	Japan	2	System Logic Semicond.	South Korea	1
Plasan	Israel	2	Brushless Fan	China	1
Panasonic	Japan	2	Talisman	Canada	1
SIMCom Wireless Sol.	China	2	Ebm-papst	Germany	1
Coilcraft	United States	2	Unisonic Technologies	United States	1
MCL Electr. Materials	China	2	Mitsubishi Electric	Japan	1
Taiwan Semiconductor	Taiwan	2	Weigao Group	China	1
Peak Electronics	Germany	2	QuartzCom	Switzerland	1
Integrated Silicon Sol.	United States	2	Gumstix	United States	1
Saito	Japan	2	Hitachi	Japan	1
Transcom	Taiwan	1	LG Corporation	South Korea	1
Phoenix Contact	Germany	1	Swatch Group	Switzerland	1
Ampleon	Philippines	1	Planar Systems	United States	1
Alinx Electronic Tech.	China	1	Unidentified		12

Appendix 3: HS Codes of Critical Components

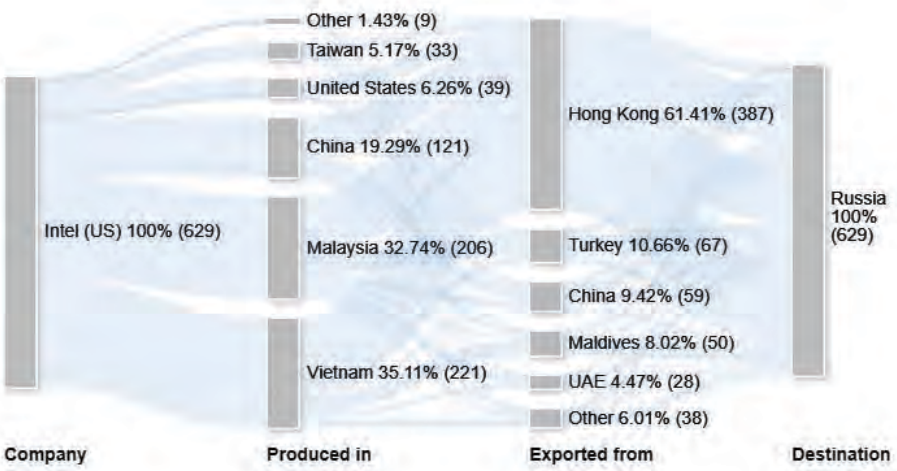
Table includes **385** 10-digit HS codes which make up the universe of "critical components". Bold codes (**223**) are those in the subset of goods for which Q1 2023 data is available.

Automotive Components and Equipment				
Engines and their parts	Electric motors and generators	Ignition and starting equipment	Motor vehicle parts and accessories	Vessels
8409990009	8501101001	**8511100009**	8708309109	8907100000
8411123009	**8501101009**	**8511300008**	8708309909	
8411910001	**8501109100**	**8511400008**	8708409909	
8411910002	**8501109300**	**8511500008**	8708509909	
8411910008	**8501109900**	**8511800008**	8708709909	
8411990019	**8501200009**	**8511900009**	8708913509	
8412212002	**8501310000**		8708939009	
8412212009	8501320008		8708949909	
8412218008	**8501402004**			
8412298109	**8501402009**			
8412298909	**8501408009**			
8412310009	**8501510001**			
8412808009	**8501510009**			
8412904008	**8501522001**			
8412908009	**8501522009**			
	8501523000			
	8501620000			
Communication equipment				
Telecommunications equipment	Radio equipment and its components			
8517140000	8522904000	8523519900	8525899109	**8529106500**
8517610008	8523210000	8523529001	8525899900	8529106901
8517620003	8523291505	8523529009	8526100001	**8529106909**
8517620009	8523291509	8523591000	8526100009	**8529108000**
8517699000	8523293102	8523599101	**8526912000**	**8529109500**
8517711100	8523293908	8523599109	**8526918000**	8529901027
8517711500	8523419000	8523809101	**8526920008**	8529902002
8517711900	**8523492500**	8523809300	8527139900	8529902008
8517790009	8523493900	**8523809900**	8527190000	**8529904900**
	8523494500	8525500000	**8527212009**	8529906502
	8523495100	8525600009	8527911900	8529906508
	8523495900	8525811900	8527913500	8529909200
	8523511000	8525813000	8527919900	8529909600
	8523519101	8525819100	8527990000	
	8523519109	8525891900	**8529101100**	
	8523519300	8525893000	**8529103900**	
Computer components and modules				
8471300000	**8471606000**	**8471705000**	**8471900000**	**8473308000**
8471410000	**8471607000**	**8471707000**	**8473299000**	**8473502000**
8471490000	**8471702000**	**8471709800**	**8473302002**	
8471500000	**8471703000**	**8471800000**	**8473302008**	
Drones and aircraft components				
8807200000	8807300000	8807900009		
Electrical and electronic equipment and components				
Electrical transformers, converters, and magnets				
8504102000	**8504318001**	8504403008	**8504502000**	**8505110000**
8504108000	**8504318007**	8504403009	**8504509500**	**8505191000**
8504210000	**8504320002**	**8504405500**	8504900600	**8505199000**
8504229000	**8504320009**	8504408300	**8504901100**	**8505200000**
8504230009	**8504330009**	8504408500	8504901700	**8505902009**

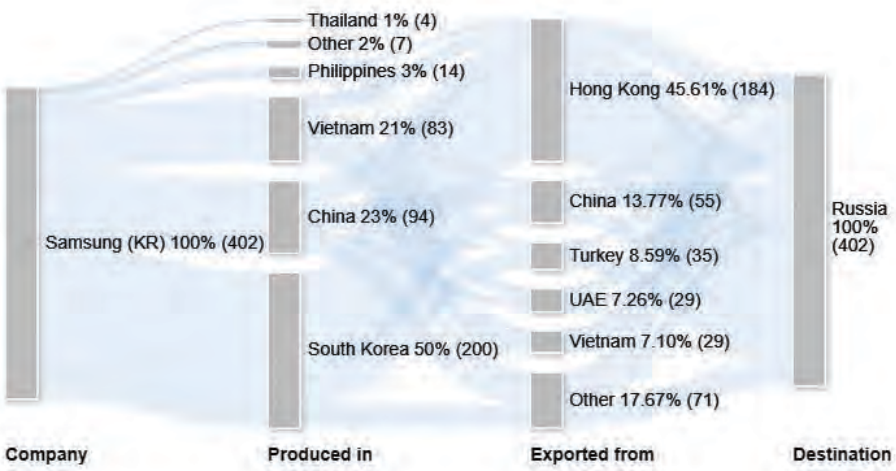
8504312109	**8504340000**	8504408700	8504909200	
8504312909	8504403004	8504409100	8504909800	
Electrical components and equipment				
8532100000	**8533409000**	8536201007	8536508008	**8537101000**
8532210000	**8533900000**	8536209007	8536611000	**8537109100**
8532220000	8534001100	8536302000	8536619000	8537109800
8532230000	**8534001900**	8536304000	**8536691000**	8537209200
8532240000	**8534009000**	8536308000	**8536693000**	8537209800
8532250000	**8535100000**	**8536411000**	8536699002	**8538100000**
8532290000	**8535210000**	**8536419000**	**8536699008**	8538901200
8532300000	**8535290000**	**8536490000**	8536700001	8538909200
8533100000	8535302000	8536500400	8536700002	8538909901
8533210000	**8535400000**	8536500600	**8536700003**	8538909908
8533290000	8535900008	**8536501109**	8536700004	8540710009
8533310000	**8536101000**	**8536501509**	**8536900100**	8540890000
8533390000	**8536105000**	8536501904	**8536901000**	
8533401000	**8536109000**	8536501906	**8536908500**	
Batteries				
8506101100	**8543900000**	8544300003	**8544429007**	**8544499101**
8506101801	8506109809	**8544300007**	**8544429009**	**8544499108**
8506101809	**8506501000**	**8506600000**	**8544492000**	**8544499309**
8506109100	**8506503000**	**8507202000**	**8507302009**	**8544499509**
8543200000	8506509000	**8507208001**	**8507500000**	**8544601000**
8543400000	**8544119000**	**8507208008**	**8507600000**	**8544609009**
8543703008	**8544200000**	**8544421000**	8507800009	8544700000
8543708000	8544300002	8544429003	**8544499101**	
Semiconductors and electronic circuits				
8541100009	8541410007	**8541600000**	8542323900	8542391000
8541210000	8541410008	**8541900000**	**8542324500**	**8542399010**
8541290000	8541410009	8542311001	8542325500	**8542399090**
8541300009	8541420000	**8542311009**	8542326100	8542900000
8541410001	8541430000	**8542319010**	8542326900	**8486909008**
8541410002	8541490000	8542319090	8542327500	
8541410004	8541510000	8542321000	**8542329000**	
8541410006	8541590000	8542323100	**8542339000**	
Military navigation and sensor systems				
Optical equipment	Navigation equipment	Avionics, thermal heaters, sensors		Automatic control instruments
9002110000	**9014100000**	**9025192000**	9030310000	**9032102000**
9002190000	9014202009	**9025198009**	9030320009	**9032108100**
9002200000	9014208001	**9025804000**	**9030331000**	**9032108900**
9002900009	**9014208009**	**9025808000**	**9030339900**	9032200000
9005100000	**9014800000**	9025900003	9030390009	**9032810000**
9013200000	9014900000	**9025900008**	**9030400000**	**9032890000**
9013800000	**9015101000**	**9026108900**	9030820000	**9032900000**
9013900000	**9015401000**	**9029203809**	**9030899009**	
	9015900000	**9029900009**	**9030908500**	
Other				
3926300000	**8482101009**	**8482990000**	**8483402308**	**8483508000**
3926400000	8482109001	**8483109500**	**8483402500**	**8483608000**
3926909200	**8482109008**	**8483200000**	**8483402900**	**8483908909**
3926909706	**8482200009**	**8483303209**	**8483403009**	**9020000000**
3926909707	**8482400009**	**8483308007**	**8483405900**	**9023008000**
3926909709	**8482500009**	**8483402100**	**8483502000**	

Appendix 4: Trade Flow Illustrations for Major Companies

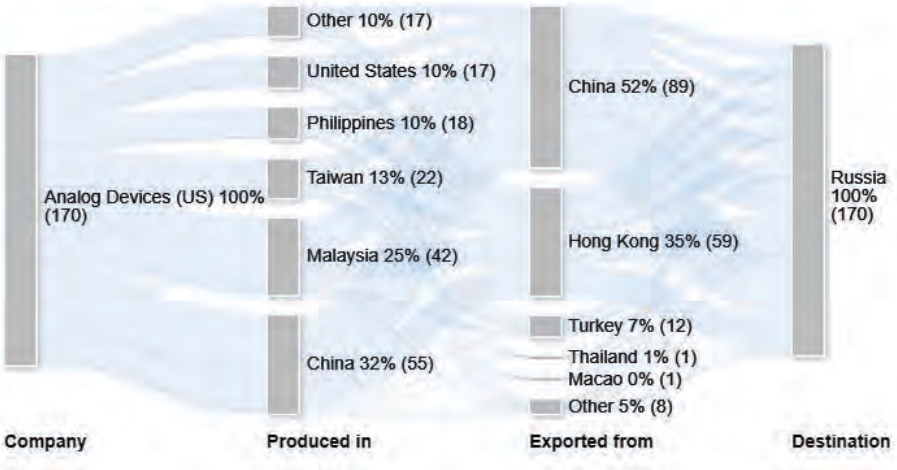
Intel Corporation



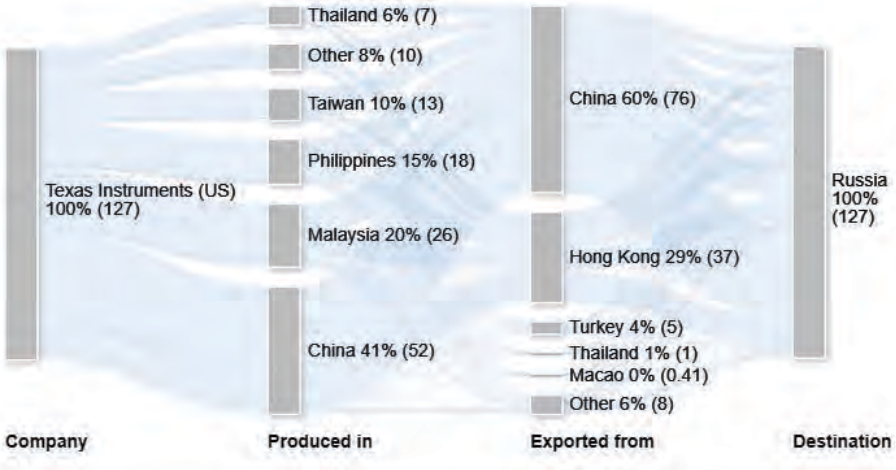
Samsung



Analog Devices

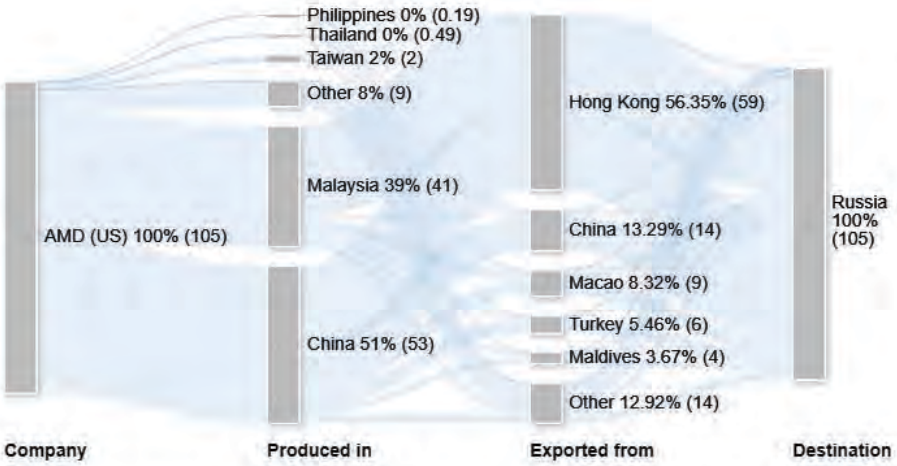


Texas Instruments

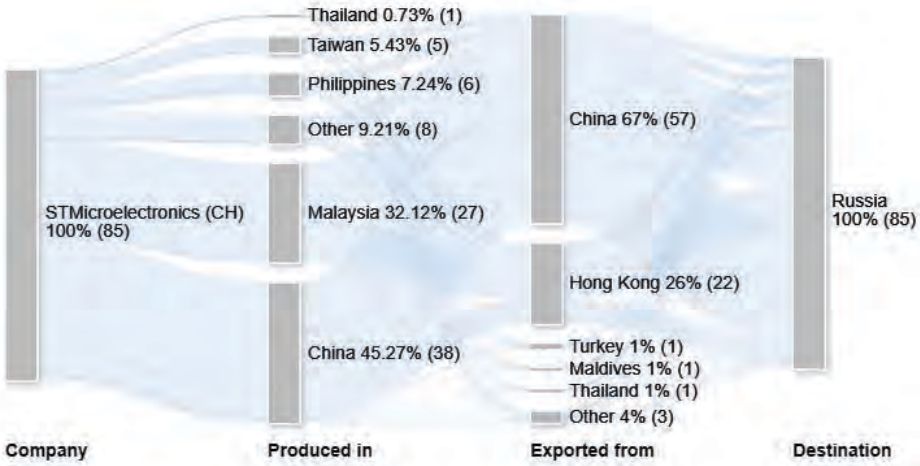


KSE | Institute

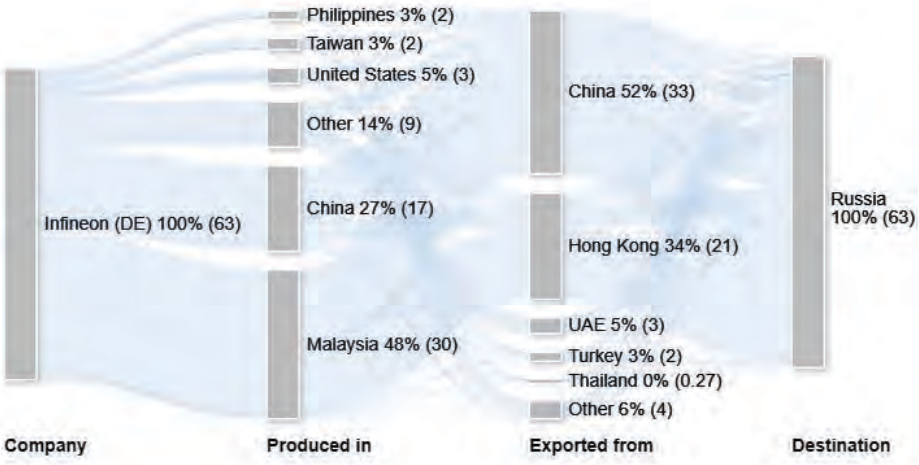
AMD



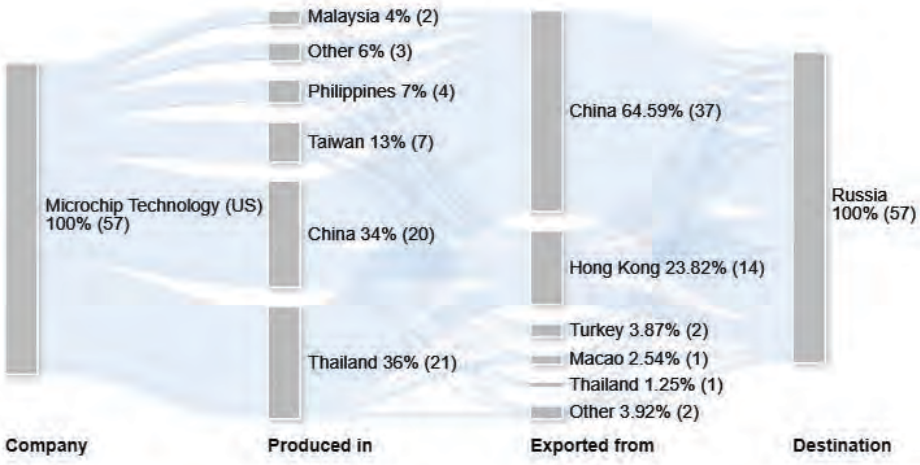
STMicroelectronics



Infineon Technologies

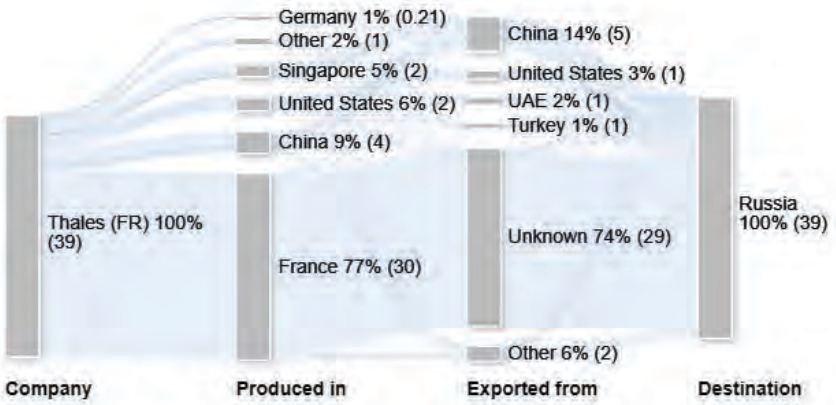


Microchip Technology

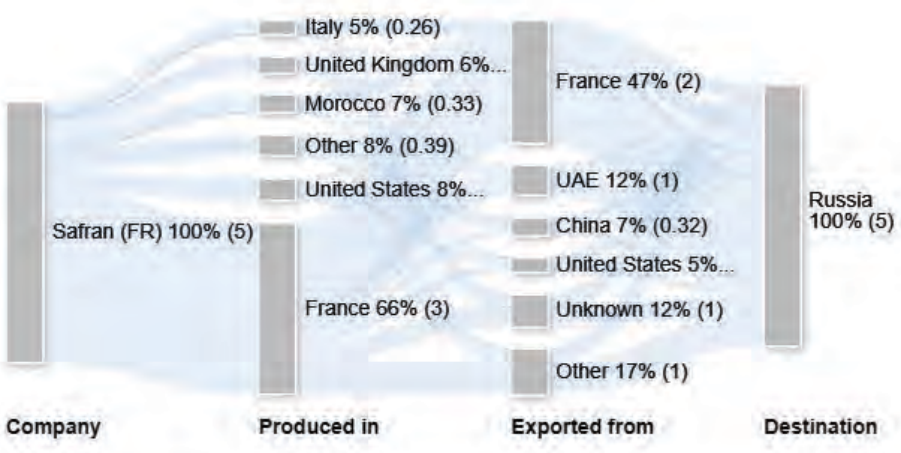


KSE | Institute

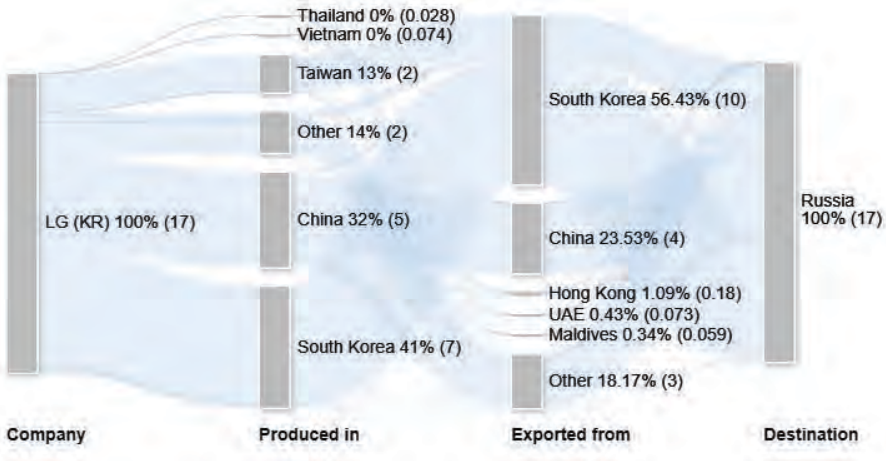
Thales**



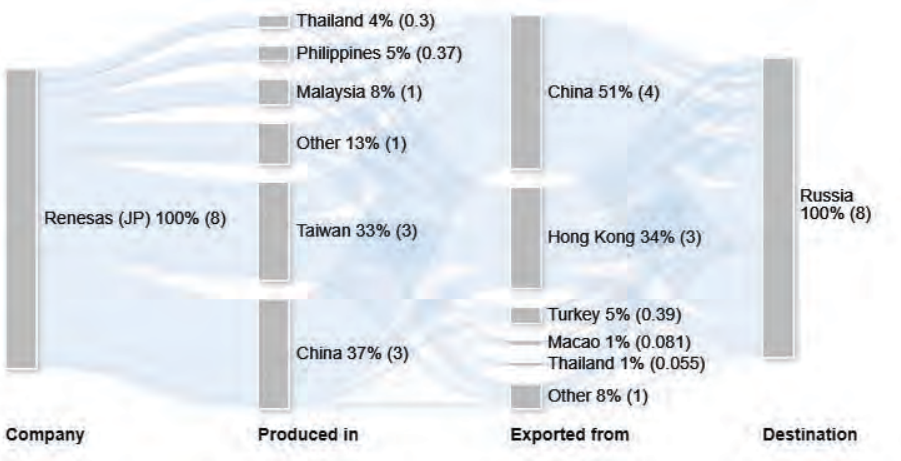
Safran**



LG Corporation



Renesas Electronics



Source: KSE Institute

** Charts shows Russian imports of critical components; percentages show distribution on each level and numbers in parentheses denote trade values in $ million in March-December 2022*

*** Data for location of export missing in some/many cases*