Testimony by Elina Ribakova

Senate Committee on Homeland Security and Governmental Affairs

Permanent Subcommittee on Investigations

"The U.S. Technology Fueling Russia's War in Ukraine: How and Why"

February 27, 2024

I. Summary of Testimony

Chair Blumenthal, Ranking Member Johnson, and distinguished Members of the Subcommittee: thank you for the opportunity to testify before the committee today. My name is Elina Ribakova, and I am the director of the International Affairs Program and vice president for foreign policy at the Kyiv School of Economics, a leading educational and research institution in Ukraine with over 700 students and 70 researchers. I am also a non-resident senior fellow at the Peterson Institute for International Economics and at Bruegel.

My testimony today is not on behalf of any organization and should be considered as reflecting my own views. The testimony draws on a large body of research that I have conducted – including with my colleagues at the Kyiv School of Economics – on economic statecraft, sanctions, and export controls. It also reflects my prior experience in the financial markets and at the International Monetary Fund. I am pleased to be testifying alongside colleagues from the Royal United Services Institute and Conflict Armament Research, whose work I respect profoundly.

<u>There are several key messages that I would like to convey in my testimony:</u>

- *One*, Despite Russia's efforts to diversify, its military still heavily relies on components from the U.S. and coalition countries, allowing for leverage through export controls.
- *Two*, we must do more as Russia continues to import significant amounts of what the U.S., European Union, and other allies have identified as high priority battlefield goods, including from producers headquartered in coalition countries.
- *Three*, more effective export controls will require improved corporate responsibility for supply chain control. It will also require strengthening the Bureau of Industry and Security (BIS), using financial sanctions, targeting third-country intermediaries, closing export controls loopholes, and improving multilateral cooperation.
- And *four*, addressing export controls circumvention is crucial, not just for halting Russia's aggression on Ukraine, but also for the credibility of our economic statecraft.[1] It is time to assess what works and what doesn't in export controls to effectively address the challenge posed by China's advances in strategic technologies.

[1] See "Economic sanctions risk losing their bite as a U.S. policy weapon" (2023), Elina Ribakova, FT.

Export controls[2] now stand at the forefront of U.S. economic statecraft.[3] They play a crucial role not only in undermining the ability of malign actors to bolster their military production but also in creating a strategic technology barrier to prevent these countries from gaining a military advantage in the future.[4] However, currently, we lack the institutional infrastructure needed to address these new geopolitical challenges.[5] The success of government policy hinges greatly on private sector involvement.[6] Decades ago, when implementing financial sanctions, and anti-money laundering and anti-terrorist financing measures, the U.S. government counted upon the financial sector to block malign actors from accessing U.S. financial systems. Today, the U.S. needs corporate assistance to prevent global malign actors from accessing U.S. strategic products and technologies.

We are at risk of undermining our sanctions and our enforcement agencies if the private sector globally learns that we cannot enforce new and increasingly comprehensive measures of economic statecraft. And, in fact, while export controls have had some effect on trade flows, Russia continues to import[7] large amounts of goods needed for military production. Since the imposition of restrictions, supply chains have adapted and many components, including a significant share from coalition-based producers, now reach Russia via intermediaries in third countries, including China, Turkey, and the UAE. Thus, export controls enforcement must be improved.

<u>My key policy recommendations for congressional consideration are as follows:</u>

- **First, it is critical to strengthen our own institutions.**[8] Export controls will remain a crucial component of economic statecraft in the foreseeable future. Therefore, U.S. government agencies should receive permanent – and increased – funding to enhance their capacity to develop, implement, enforce, and evaluate the effectiveness and assess costs of novel comprehensive export controls like those directed at countries such as Russia and China.
- **Second, we need to bolster corporate responsibility.** Improved enforcement of export controls ultimately requires buy-in from the private sector, particularly U.S. and coalition-based producers of goods needed for Russia's military industry. Effective control of supply chains must start at the point of production and with the initial sale of an item to a distributor. To incentivize corporations to establish compliance procedures, enforcement agencies must engage with the private sector, demonstrating a willingness and ability to

[2] Alongside measures such as inbound and outbound investment controls.

[3] Kevin J. Kurland, "Improving Export Controls Enforcement", Hearing, January 23, 2024.

[4] See comments by Matthew Axelrod, Assistant Secretary for Export Enforcement, at the Munich Security Conference.

[5] See "Forging a positive vision of economic statecraft" (2024), Daleep Singh, Atlantic Council.

[6] See "The New Economic Security State: How De-risking Will Remake Geopolitics" (2023), Henry Farrell and Abraham Newman, Foreign Affairs.

[7] See "Challenges of Export Controls Enforcement: How Russia Continues to Import Components for Its Military Production" (2023), Olena Bilousova et al., International Working Group on Russian Sanctions and KSE Institute.

[8] See congressional testimony by Emily Kilcrease, CNAS.

investigate trade involving controlled goods and impose meaningful fines for export control violations.[9]

- **Third, we should leverage the role of our financial industry in global trade.** Export controls enforcement faces similar challenges to anti-money laundering and countering financing of terrorism: often highly fungible goods, complex chains of custody, opaque ownership structures, frequent institutional changes, and reliance on less-strict jurisdictions for the set-up of circumvention schemes. Due to the regulatory framework that has been established over the past two decades in these areas, financial institutions have already built the internal compliance architecture to detect such schemes and could contribute to tracing the trade in export-controlled goods.
- ***Four*, remaining loopholes in the export controls regime need to be closed.** Significant inconsistencies impede effective enforcement and facilitate circumvention. Harmonizing restrictions across coalition jurisdictions, alongside establishing clear licensing and derogation procedures would help mitigate this problem. Strengthening implementation and enforcement of U.S. Foreign Direct Product Rule regimes is vital, given many goods are produced in third countries.[10]
- ***Five*, we also need to address third-country circumvention networks.** Coalition authorities must address the involvement of intermediaries, particularly in China, Turkey, and the UAE, in the circumvention of export controls. They can achieve this by imposing sanctions on entities that facilitate violations. While networks will always adjust to such restrictions, it would significantly increase the cost of operating them. In fact, we already see Russia having to pay large markups.
- **And, *six*, improved multilateral cooperation will be key going forward.** As technology sanctions will remain a critical element of the economic statecraft toolbox, we should step up cooperation between jurisdictions – up to entering into a new multilateral export controls treaty, similar to the Cold War CoCom and replacing the existing Wassenaar Arrangement.[11] Moreover, the U.S. should also encourage its allies[12] to enact legal and institutional reforms facilitating an effective multilateral strategy to undermine the military capacities of malign actors such as Russia, China, North Korea, and Iran.

Let me conclude by stressing that while export controls have had some effect in limiting Russia's military capacity, we must intensify our efforts. Preserving the credibility of our economic statecraft is crucial to sending a clear message to malign actors worldwide that their actions will result in severe consequences. I am deeply grateful for the opportunity to address these critical issues and look forward to your questions.

---

[9] See “Enforcing U.S. Economic Sanctions: Why Whale Hunting Works” (2020), Bryan Early and Keith Preble, The Washington Quarterly.

[10] See congressional testimony by Kevin Wolf.

[11] See “Technology Controls Can Strangle Russia—Just Like the Soviet Union (2022), Maria Shagina, Foreign Policy,

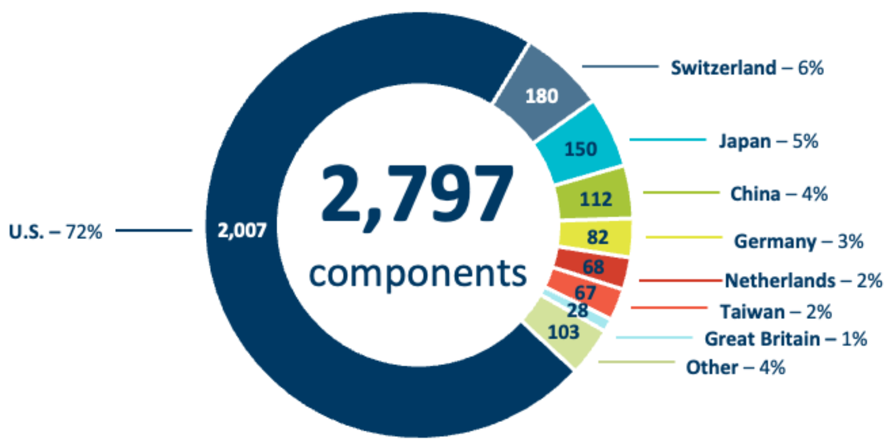
[12] See “For Effective Controls, Build Coalitions” (2020), Martin Chorzempa, CNAS.

II. Evidence: What Works and How We Can Strengthen Export Controls

With Russia's brutal full-scale invasion now in its third year, 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.

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 would 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 (Figure 1).[13]

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



Source: NACP, UA War Infographics, KSE Institute

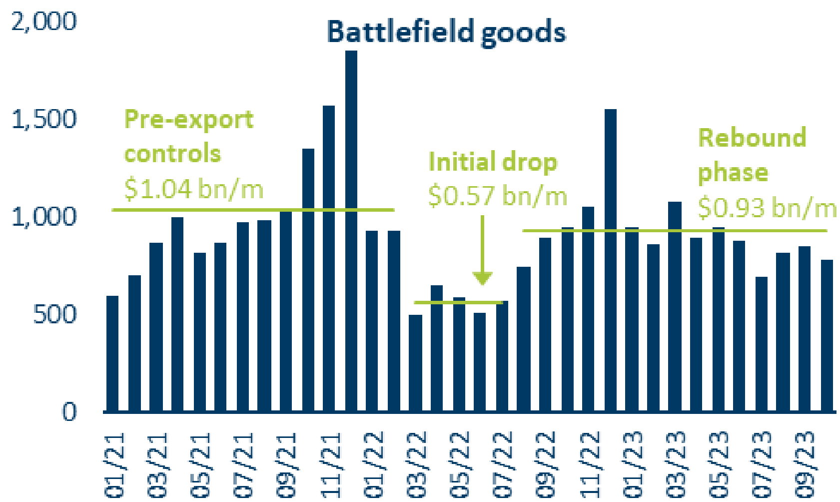
Russia's dependence on foreign components for its military production persists, with a striking 95% of foreign parts found in Russian weapons sourced from coalition countries, notably 72% from U.S.-based companies alone. This stark reality highlights Russia's ongoing struggle to find viable substitutes within the Russian domestic market or its allies, with Chinese components comprising only 4% of all identified items.

The United States and coalition countries have identified a list of 45 six-digit Harmonized System (HS) codes deemed crucial for export controls enforcement, known as "common high-priority items" or "battlefield goods." Initial observations show a tangible impact of export controls on Russia's importation of these priority items in mid-2022. However, Russia has managed to adapt

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

its supply chains, resulting in only a marginal 10% decrease in monthly average imports of battlefield goods throughout 2023 compared to the period preceding the full-scale invasion in 2022 (Figure 2).

Figure 2: Russian imports of battlefield goods, in $ million



Source: KSE Institute

It appears that many companies from coalition countries continue to supply billions of dollars' worth of critical goods to third countries, from where these goods eventually make their way to Russia. However, effective enforcement of export restrictions hinges on the private sector's cooperation. The $8.8 billion in Russian high-priority goods imports recorded from January to October 2023 consisted of over 800,000 individual transactions, a volume that overwhelms coalition authorities' investigative resources. Crucially, the aim is to halt any illicit transactions early enough to prevent these goods from reaching Russia and its military industry.

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 the battlefield goods imported by Russia continues to be produced in China and other countries 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 also demonstrates that export controls face substantial enforcement challenges. One of these challenges is that many of the items in question never physically touch the jurisdiction of export controls-imposing countries – they are produced offshore and then make their way to Russia via certain transshipment jurisdictions. Monitoring of transactions and interruption of shipments is, thus, a complex task.

III. Policy Recommendations: Strengthening the Export Controls Regime

We urge policy makers to take action to ensure that export controls stay ahead of Russian efforts to circumvent them. Our measures need to address the distinct challenges at various stages of the supply chain with tailored solutions. They should aim to (i) close policy gaps in the existing export 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.

Closing Export Controls Policy Gaps

We need 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 Rules 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.

1. **Align, expand, and simplify export controls.** Export controls need to be harmonized across coalition jurisdictions. The current focus on specific products leaves similar goods unregulated, allowing considerable room for circumvention schemes. Governments should also regularly review the list of export-controlled items[14]—based on evidence from investigations of and new findings regarding foreign inputs to the Russian military industry.[15,16] 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.[17] Thus, sanctions aiming to constrain military capacity need to also target non-military entities. 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

---

[14] "CNC Machinery 2.0. Updated research on the strategic role of CNC machines in curtailing Russia's military capacity", Economic Security Council of Ukraine (ESCU), November 2023.

[15] 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.

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

[17] 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.

all coalition jurisdictions or not sanctioned at all.[18] Exceptions from export controls should be considerably revised to prevent sales being redirected to the war effort. In the U.S., entity lists should also capture third-country subsidiaries of companies.[19] 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 Rules.** It is crucial that export control provisions address the large share of Russian imports of export-controlled goods produced on behalf of companies headquartered in coalition countries but manufactured and shipped from other locations. Currently, most countries lack explicit policies in this regard and/or improvements are needed. 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[20] 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 lack data for cross-checking voluntary corporate reporting to monitor FDPR compliance or conduct effective on-site 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.[21]

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.[22] Moreover, for items with satellite-related or military content going to, among other places, China and Russia, the threshold is 0%. We recommend considering a 0% De-Minimis level for all shipments to Russia, being mindful of the costs of the potential increased due diligence burden and possible switch away from the U.S. components.[23] This would also send a strong message that Russia is considered as belonging to 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

---

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

[19] The entity list's approach to subsidiaries should be at least 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.

[20] Russia and Belarus-related FDPR was issued within the first 24 hours of Russia's full-scale invasion of Ukraine

[21] See "Effectiveness of the FDPR," Emily Kilcrease, Thomas Krueger, and Elina Ribakova, CNAS (forthcoming). The U.S. has waived the FDPR as far as the EU is concerned for dual-use items and certain advanced technology items. Commission Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014, Item 53, please see here.

[22] See here.

[23] Excessive export controls to protect U.S. national security and innovation could compel firms to move overseas | PIIE

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").[24] Improvements are also needed in the United States. We also propose that the EU remove certain grounds for 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.[25]

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 with vastly more complex 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 inadequate for effective enforcement**, posing a significant challenge to agencies responsible for implementing the existing Russia export controls regime. The sheer volume of individual transactions, exceeding 800,000 for the battlefield goods subset shipped to Russia in January-October 2023 alone, overwhelms the capacity for comprehensive investigations necessary to identify circumvention schemes and penalize violators. As export controls become a permanent fixture in economic statecraft, urgent public sector capacity building is essential to ensure their effectiveness and credibility in the medium to long term. While enforcement structures for export controls already exist in the U.S., unlike in other jurisdictions, these agencies lack the financial and human resources to address challenges arising from the broader scope of modern-day export controls.[26] It is also necessary to convince our allies to move beyond the "Wassenaar world" of relatively

[24] 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.

[25] 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.

[26] See "Want to Help Ukraine? Fund This U.S. Government Agency," Emily Benson, Foreign Policy.

clear differentiations between military and non-military goods to a world where dual use is much more pervasive than it used to be.

2. **Capacity building should also encompass technological solutions.** While undoubtedly a complex endeavor, it may be technologically feasible to establish systems for tracking goods throughout the supply chain. These efforts should initially focus on larger items but could eventually extend to small-scale components like semiconductors and other microelectronics.[27] Mandatory implementation of tamperproof identifiers such as serial numbers should also be included, as recent cases have shown these identifiers being erased in weapons found on Ukrainian territory. Additionally, systems could be devised to remotely disable items if they somehow reach Russia. This would address a key challenge of export controls enforcement: taking action before the goods reach their intended destination.

Bolstering Corporate Responsibility

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 are critical for the success of the entire export controls regime. Cleaning up distribution networks is certainly a resource-intensive task for corporations. Governments will need to create proper incentives by demonstrating the ability[28] 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.

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 civil/administrative monetary penalties in the case of export controls violations.[29] 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.

    a. Given the multi-jurisdictional nature of the trade in export-controlled goods, coalition authorities should closely collaborate on investigations. Transparency is crucial and

---

[27]See "Secure, Governable Chips, Using On-Chip Mechanisms to Manage National Security Risks from AI & Advanced Computing", Onni Aarne, Tim Fist and Caleb Withers, CNAS.

[28] Further analysis is warranted regarding where currently corporate liability begins and ends. If needed, the government needs to be granted legal powers to enforce export controls.

[29] See "Viral Governance: How Unilateral U.S. Sanctions Changed the Rules of Financial Capitalism", Grégoire Mallard and Jin Sun, American Journal of Sociology Volume 128, Number 1.

information on ongoing inquiries,[30] 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 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 administrative proceedings related to sanctions violations—should include significantly higher amounts). 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.[31] Further to substantial penalties in the context of civil and administrative procedures, we propose that all coalition jurisdictions criminalize sanctions violations and urge governments to consider prosecution for aiding and abetting war crimes in certain cases.

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.[32] 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 civil/administrative 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).

---

[30] U.S. sets the example here: as of June 2, 2022, charging letters sent by BIS to companies suspected of export control violations can be made public prior to the final administrative disposition of such cases, https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3010-russia-corrections/file

[31] 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 the annul, suspend, modify, or revoke a previously granted export authorization.

[32] For example, the plea settlement and imposition of penalties in the Chinese ZTE Technologies case 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 was deprived of export privileges in 2018 – only after repeated violations in the form of failure to abide by terms of settlement agreements had been discovered.

2. **Apply lessons from the financial industry regarding "know-your-customer" 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 Customer" (KYC) and understanding their customers' customers.[33] 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 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 the latest technologies (e.g., artificial intelligence) in identifying "red flags" and Russia's procurement practices with the objective of reducing compliance costs.[34]

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 and develop ways to share more information more quickly, e.g. via industry bodies. 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

[33] In a novel move, the BIS is now applying KYC for cloud computing.

[34] 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, particularly where the tracing of structures and activities in third countries is 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.

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 efforts turn out to be systemic in nature—and the aforementioned measures insufficient to address existing challenges—broader trade restrictions are needed 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 have to entail extraterritorial application of sanctions or secondary sanctions.
2. **Restrict exports to countries with systemic problems.** Measures could include export quotas, export bans, denial of market access, and expanded in-use checks.
3. **Engaging both the public and private sectors in third countries.** Initiatives could entail sharing information, such as the provision of third-country trade data to coalition countries, enhancing administrative capacities within third-country customs services, and providing technical assistance to private sector entities in those countries.

Improving Multilateral Cooperation

The complexity of global supply chains and the breadth of modern-day export controls necessitate improved cooperation across jurisdictions. Without such collaboration, gaps in the sanctions regime—and its enforcement—will persist, allowing circumvention on a scale that undermines the effectiveness and credibility of restrictions. We believe that enhanced information exchange is key to improving the system, particularly given that the ultimate goal of export controls is to prevent shipments of dual-use goods to Russia before they happen. Moreover, if technology sanctions are indeed the new frontier in economic statecraft, more enduring structures may be required, such as multilateral export controls treaties.

IV. Conclusion

Export controls are now a critical tool of the U.S. economic statecraft. Following Russia's invasion of Ukraine, a coalition of nations, including the U.S., EU, UK, Japan, and South Korea, implemented unprecedented export controls, aiming to deprive Russia of critical resources for its military industry. These measures mark a significant test of 21st-century technology sanctions and economic statecraft, with broader implications beyond the immediate challenge. Potential malign actors worldwide are watching whether the U.S. and its allies will succeed.

While export controls had an immediate impact on Russia’s military production, policy needs to be continuously adjusted and strengthened. Enforcement faces challenges due to global supply chain complexities, major economies like China's facilitation of sanctions evasion and avoidance by Russia, and limited experience and resources among coalition countries.

In this testimony, I highlighted the role of producers from coalition countries whose products end up in Russian weapons due to insufficient compliance efforts. However, I believe that improved cooperation between authorities and the private sector can bolster the effectiveness and credibility of U.S. economic statecraft. Urgent actions are needed to strengthen enforcement institutions, incentivize private sector compliance, target circumvention schemes, and enhance multilateral cooperation in export controls to uphold the rules-based international order.

V. Additional Analysis

The following reports are used in preparing this testimony and are listed here for the convenience of the Committee in its future work.

Yermak-McFaul International Group on Russian Sanctions, KSE Institute (Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, Anna Vlasyuk and Vladyslav Vlasiuk), *“Challenges of Export Controls Enforcement: How Russia Continues to Import Components for Its Military Productions”*, January 2024, https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf

Elina Ribakova, *“Economic sanctions risk losing their bite as a U.S. policy weapon”,* FT, November 7, 2023, https://www.ft.com/content/b54201be-f307-4171-bb99-b356537b1898

Yermak-McFaul International Group on Russian Sanctions, KSE Institute (Olena Bilousova, Nataliia Shapoval, and Vladyslav Vlasiuk), “*Strengthening Sanctions on Foreign Components in Russian Military Drones”,* August 23, 2023, https://kse.ua/wp-content/uploads/2023/08/230828%20Drones%20for%20KSE%20site.pdf?_t=1693243181

Co-authored with Benjamin Hilgenstock, Elina Ribakova and Guntram B. Wolff, *“Toughening Financial Sanctions on Russia”,* Intereconomics, Volume 58, 2023 · Number 4 · pp. 201–208 · JEL: B17, F5, July-August 2023, https://www.intereconomics.eu/contents/year/2023/number/4/article/toughening-financial-sanctions-on-russia.html

Yermak-McFaul International Group on Russian Sanctions, KSE Institute (Olena Bilousova, Oleksii Gribanovskiy, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, and Vladyslav Vlasiuk), “*Russia’s Military Capacity and the Role of Imported Components”*, June 2023, https://kse.ua/wp-content/uploads/2023/06/Russian-import-of-critical-components.pdf

Peterson Institute for International Economics, Elina Ribakova, April 2023, *“Sanctions against Russia will worsen its already poor economic prospects”*, https://www.piie.com/blogs/realtime-economics/sanctions-against-russia-will-worsen-its-already-poor-economic-prospects

Free Russia Foundation (Sebastian Bienkowski, Pavel Elizarov, Maria Kausman, Natalya Lunde, Maxim Mironov, Elina Ribakova, Maria Telegina, Elizaveta Volkova, and Kathryn McConaughy with contributions by Samuel Bendett, Kevin DelliColli, Oleg Itskhoki and Sergey Aleksashenko), *“Effectiveness of U.S. Sanctions Targeting Russian Companies and Individuals”,* January 2023, |https://www.4freerussia.org/wp-content/uploads/sites/3/2023/01/frf-sanctions-web.pdf