

Enforcing export controls learning from and using the financial system

Benjamin Hilgenstock¹ | Elina Ribakova^{1,2,3} | Anna Vlasyuk¹ | Guntram Wolff^{3,4}

¹KSE Institute (Kyiv School of Economics), Kyiv, Ukraine

²Peterson Institute for International Economics, Washington, DC, USA

³Bruegel, Brussels, Belgium

⁴Université Libre de Bruxelles, Bruxelles, Belgium

Correspondence

Guntram Wolff, Solvay Brussels School/ECARES, Université Libre de Bruxelles, Belgium.

Email: guntram.wolff@ulb.be

Abstract

Russian imports of battlefield goods subject to export controls have surged since mid-2022 and reached levels close to those prior to Russia's full-scale invasion of Ukraine. Russia thus continues to be able to acquire foreign components critical for its military industry. These imports largely occur via mainland China, Hong Kong, Turkey and the United Arab Emirates, while other countries including Armenia, Georgia, Kazakhstan and the Kyrgyz Republic have also seen massive increases in tech imports that likely end up in Russia. The enforcement of export controls faces multifaceted challenges centred around complex supply chains, lack of transparency and opaque financial structures, issues familiar from anti-money laundering (AML) and countering financing of terrorism (CFT) frameworks. We propose using a similar framework in export control enforcement: *First*, financial institutions need to play a role in monitoring trade in export-controlled goods and blocking illicit transactions. *Second*, non-financial companies could learn from banks' efforts in the AML/CFT sphere to implement proper due-diligence procedures and to ensure export controls compliance. Public-sector investigations and appropriate fines are critical to increase the incentives for firms to act. Technology sanctions will remain part of the economic statecraft toolbox. The Russia case will test their effectiveness and credibility.

1 | EXPORT CONTROLS: A NEW FRONTIER IN ECONOMIC STATECRAFT

Export controls played an important role in the Cold War when Western allies attempted to restrict the Soviet Union's access to critical technology. More recently, restrictions have been imposed on countries including Iran and North Korea to impede their nuclear and missile programmes. In addition, there is a multilateral voluntary export control system—the Wassenaar Arrangement—that aims to limit the spread of specific weapons and dual-use goods.

The current sanctions regime against Russia has, however, changed the scope of export controls fundamentally. Unlike in Soviet times, Russia was well integrated into the global economy when its full-scale invasion of Ukraine started in February 2022. It had access to and used modern Western technology. Only since February 2022 have far-reaching export control

measures been imposed in a coordinated fashion by the European Union, United Kingdom, United States and other partners.

Coalition countries have repeatedly tightened these restrictions and have also identified priorities for their enforcement—the so-called common high priority (CHP) items, often referred to as 'battlefield goods'.¹ These are prohibited dual-use and advanced technology products used in Russian military systems found on the battlefield in Ukraine,² or critical to the development, production or use of those systems.³ Microelectronics play a major role but the 50 harmonised system (HS) codes on the list also include, among other things, communications and navigational equipment.

Export controls are here to stay. In particular, the United States is determined to limit access to technology for its principal geopolitical rival, China. The expansion of the US Foreign Direct Product Rule (FDPR)⁴ clearly demonstrates that intent as do changes to outbound investment screening to prevent that restricted

products are produced elsewhere and reach sanctioned markets. The effectiveness of export controls is thus not only critical in whether they constrain effectively Russia's military industry and its war on Ukraine. Rather, the credibility of technology sanctions⁵—and thus their potential effectiveness in constraining China—is equally on the line.⁶

Sanctions become less effective the fewer countries implement them. An extensive literature documents how sanctions can get undermined. Drezner (2003) shows how cooperation breaks down at the stage of sanction enforcement. The threat of secondary sanctions can have some effectiveness on compliance with secondary sanctions. However, this is limited by the willingness of competing powers to compensate for possible losses on secondary sanctions. For example, Trehubova (2023) documents how China uses foreign aid to systematically help countries avoid US' Office of Foreign Assets Control (OFAC) sanctions. In Central Asia, for example, China and Russia can both offer significant economic alternatives, being close and economically sizeable trading partners. We would therefore expect that sanction enforcement is less effective in this region. An important paper by Kupatadze and Marat (2023) indeed finds significant trade irregularities in Central Asia as Russia manages to re-route trade supplies. Kazakhstan is an interesting case. On the one hand, it has Russia as a major trading partner. At the same time, it also has close trading relationships with the European Union. Stognei and Ivanova (2023) document how Kazakhstan is stepping up monitoring of re-exports to Russia in a diplomatic effort to avoid countersanctions.

Section 2 provides empirical evidence documenting that substantial amounts of sanctioned goods reach Russia via third markets. To address the fact that Russia continues to be able to acquire battlefield goods and incorporate significant amounts of export-controlled

Western technology into its weapons, we propose that financial institutions should play a larger role in increasing the effectiveness of export restrictions and that Western firms producing sanctioned dual-use goods should face greater obligations to monitor and restrict their distribution networks in order to ensure compliance with export restrictions.⁷ Finally, Heathershaw et al (2021) document the post-Soviet influence on political decision making in the West, for example in the UK, a fact that surely can have some influence also on sanctions enforcement.

2 | THE RUSSIA CASE: CHALLENGES OF EXPORT CONTROL IMPLEMENTATION

Given the complexity of the post-February 2022 export controls regime, and the lack of experience, especially in Europe, with the implementation of such comprehensive measures, it is unsurprising that substantial challenges have emerged.

According to an analysis of transaction-level trade data by the Kyiv School of Economics (Bilousova et al., 2024), Russia acquired \$12.5 billion of such battlefield goods in 2023. This means that imports have almost fully rebounded in value terms from the drop they went through in the immediate aftermath of the imposition of export controls in spring 2022⁸ (Figure 1). While there is some evidence that Russia is forced to pay significant mark-ups for export-controlled goods acquired through third countries,⁹ meaning the decline in volume terms is more pronounced than what trade values indicate, the implementation and enforcement of restrictions appear to be facing major challenges.

Russia can acquire critical inputs that its economy and military industry require by using producers in China and other countries that have stepped in and

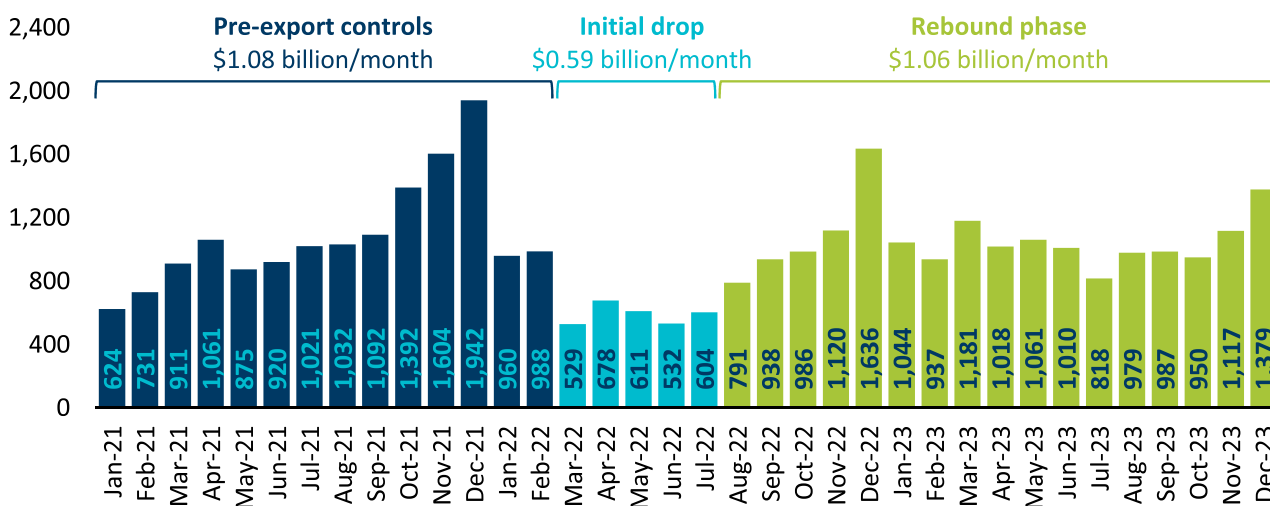


FIGURE 1 Russian imports of battlefield goods, \$ millions. Source: KSE Institute based on customs and trade data.

replaced suppliers from coalition countries. This development has not come as a surprise and inevitably plagues any sanctions regime not implemented on a global level. Moreover, *Western* technology still finds its way into Russian arms. A substantial share of Russia's battlefield goods¹⁰ imports—40.3% in 2023—is produced by or on behalf of companies headquartered in coalition countries.¹¹ Evidence from the battlefield shows that Western components still dominate as far as actual weapons production is concerned: 95% of all foreign parts identified in Russian weapons were sourced from producers in coalition countries, with 72% accounted for by US-based companies alone.¹²

In most cases, albeit not exclusively, these goods are manufactured in third countries and reach Russia via intermediaries located in mainland China, Hong Kong, Turkey, the United Arab Emirates and other places (Figure 2). As direct shipments from sanctions coalition countries dropped markedly—accounting for only 5.7% of the total value of battlefield goods imports in 2023 (vs. 50.9% in 2021)—Russia succeeded in adapting supply chains quickly (Figure 3). Shipments from mainland China made up 56.3% (vs. 27.2% in 2021), from Hong Kong 19.3% (vs. 14.4%), Turkey 5.7% (vs. 0.2%) and the UAE 4.2% (vs. 0.4%).

Circumvention is not limited to the aforementioned jurisdictions. We also observe worrying

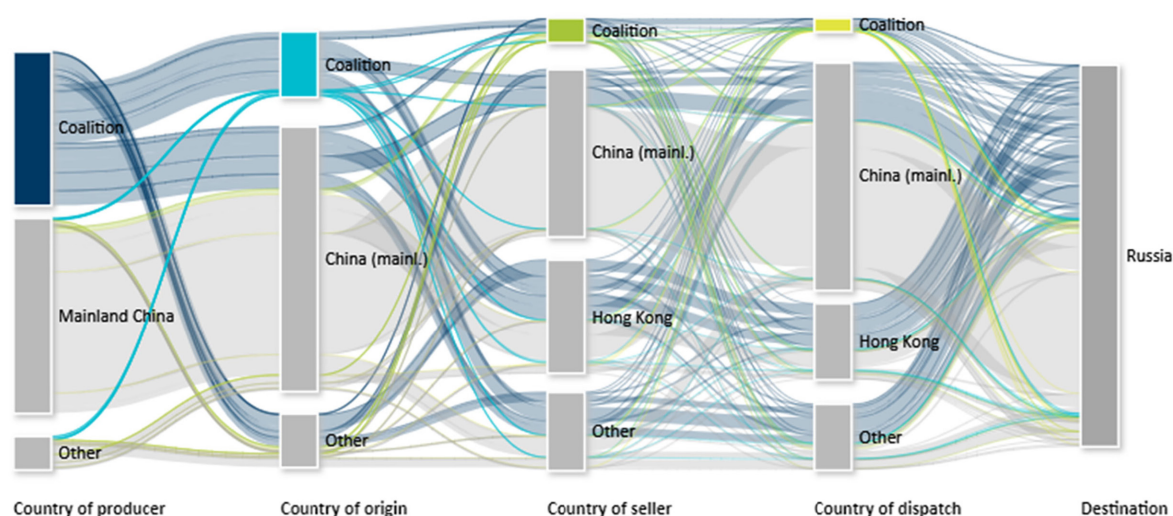


FIGURE 2 Flows of battlefield goods to Russia in 2023. Figure only includes transactions for which the full chain of custody could be determined (80% of the total value). Country of producer=location of company ultimately responsible for the good; country of origin=location of manufacturing; Country of seller=location of final seller to Russia; country of dispatch=location from which final shipment to Russia was made. *Source:* KSE Institute based on customs and trade data.

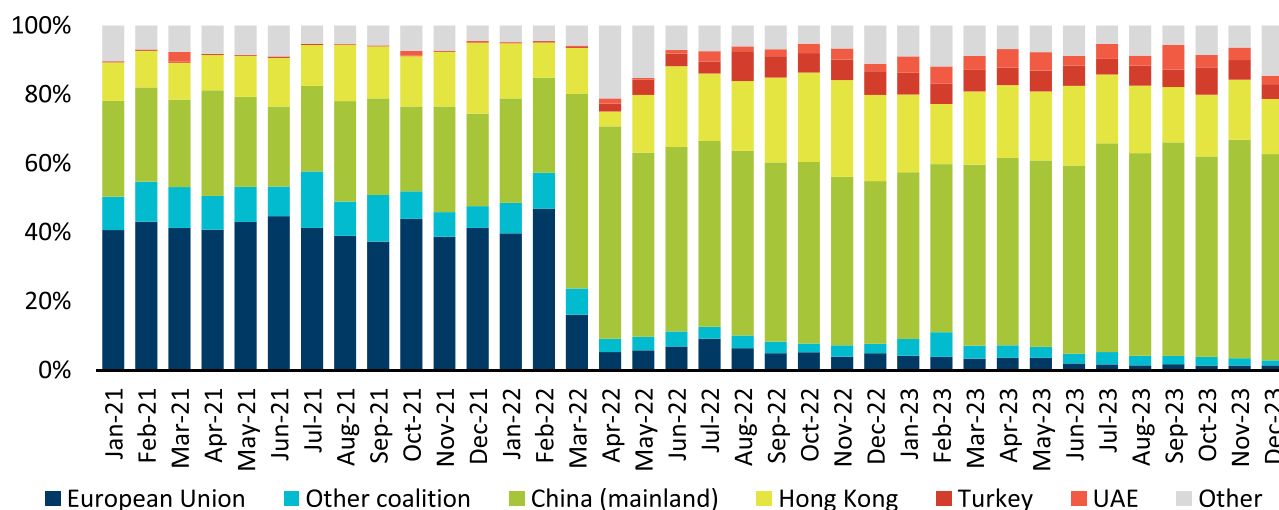


FIGURE 3 Russian imports of battlefield goods by location of shipment, in %. *Source:* KSE Institute based on customs and trade data.

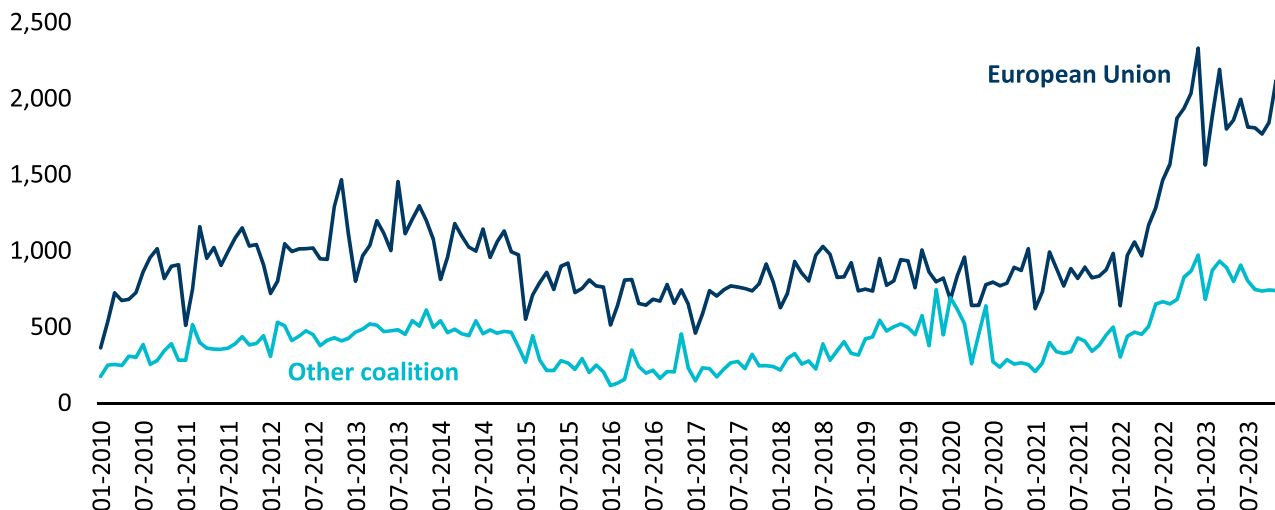


FIGURE 4 Exports to Armenia, Georgia, Kazakhstan and the Kyrgyz Republic, \$ millions. Other coalitions: Australia, Canada, Japan, New Zealand, Norway, Singapore, South Korea, Switzerland, United Kingdom and United States. *Source:* International Monetary Fund.

trends for countries of the Eurasian Economic Union (EEU)—namely Armenia, Kazakhstan and the Kyrgyz Republic—whose trade with Russia is not fully reflected in the data underlying Figures 1–3. Exports from the coalition, in particular the EU, to these three countries and Georgia have risen sharply, coinciding with the imposition of export controls on Russia (Figure 4).¹³

These trade dynamics, and the evidence from the battlefield, show that Russia has not been able to substitute certain high-technology Western goods and that export controls therefore remain a powerful tool of economic statecraft. However, it is also clear that enforcement needs improvements urgently because critical technology still reaches Russia.

The private sector plays a critical role in sanctions enforcement. Authorities have long relied on businesses to undertake the actual implementation of sanctions. In the financial industry, a set of elaborate compliance procedures exists to ensure the legality of financial transactions. Gaps in the legal framework make it more difficult to trace export control-related transactions, and regulations do not require the same level of diligence for technology firms that banks have become accustomed to in areas such as anti-money laundering.

Giving a specific example of re-routed supply chains is useful to illustrate the issue at hand. Investigations have shown how China has become the leading supplier of specific industrial equipment—Computer Numerical Control ‘CNC’ machines—to Russia as Ukraine’s allies stepped up export controls on such items. This involves China functioning as a re-export hub for equipment originally produced in sanctions coalition countries but also involves the production in China of such equipment by companies from the coalition. Distribution network control by the producers, thus, has clearly been shown to be insufficient to stem export controls evasion.¹⁴ As we will argue,

the incentives for companies to take greater control of distribution networks need to improve.

Beyond this specific example, systematic data show that many goods from coalition countries reach Russia. The fact that many companies from coalition countries continue to supply billions of dollars in critical goods to third countries, from where they find their way to Russia, means that export controls are not working as intended (Figure 5). More broadly, the credibility of sanctions regimes and enforcement agencies is at risk of being undermined if the private sector learns that new and increasingly comprehensive measures of economic statecraft cannot be policed.¹⁵

Effective enforcement of export restrictions cannot be done without the private sector doing its part (Bilousova et al., 2024). The \$12.5 billion in Russian high-priority goods imports in 2023 was made up of more than one million individual transactions. Coalition authorities cannot investigate all these cases individually. Importantly, the objective is to stop any illicit transaction early enough, so that the good does not reach Russia and its military industry.

For companies, it is inherently difficult to establish the end destination for dual-use goods, in particular when they are relatively widely used mass products. Take standard computers and smartphones, for instance. A company might deliver a product to a country like Turkey, where its subsidiary sells it to various companies registered in Turkey. But how far does the company need to go in checking where its business partners deliver the product? At what stage does such a delivery constitute a breach of an export restriction? For the company, there is currently little incentive to investigate further downstream distribution, as long as the direct buyer itself is not subject to the export restriction. The company might notice an increase in sales to a specific country, but that is not a reason to start an

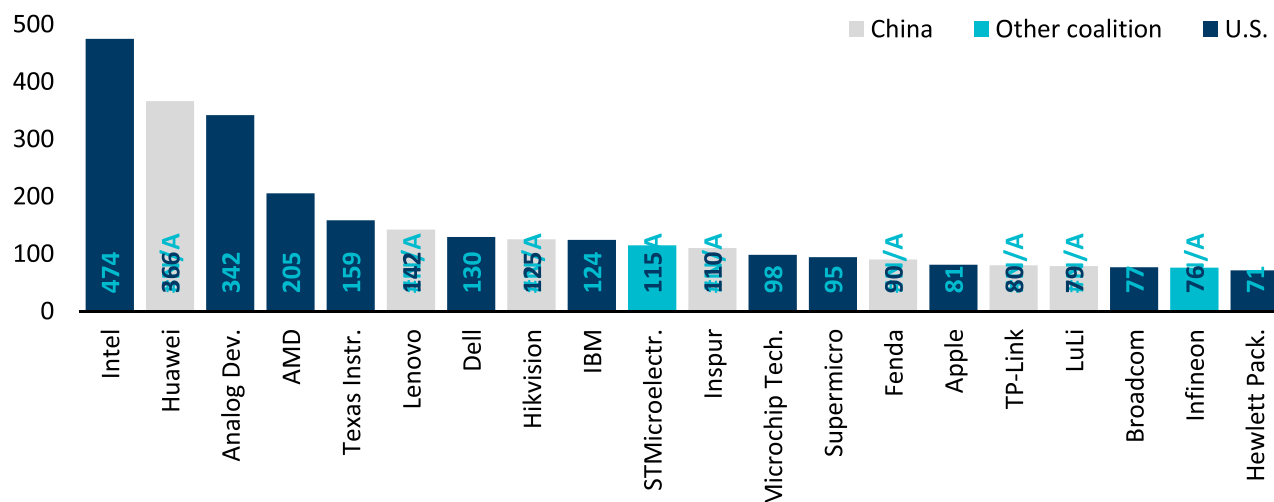


FIGURE 5 Russian imports of battlefield goods in 2023 by producer, \$ millions. Source: KSE Institute based on customs and trade data.

investigation into compliance with export restrictions. Tracing distribution networks is particularly difficult if the item in question is small and can be shipped in simple packages (as is the case for semiconductors and other electronics).

The main question is, thus, how to design mechanisms that ensure that export controls are effective and that the private sector prevents dual-use technologies from reaching Russia? In principle, companies will pay more attention to the topic when: (i) the ex-post probability of detection of an illicit delivery is greater, (ii) the reputational and financial fine if such a delivery is detected is greater and (iii) a fine is imposed more quickly, as late enforcement could be beyond the scope of the management that is taking decisions to reap the rewards of continued trade.

3 | THE FINANCIAL SYSTEM'S ROLE IN IMPROVING EXPORT CONTROLS

To improve the implementation and enforcement of the export controls regime against Russia, and to safeguard the credibility of technology sanctions, we propose to leverage the financial system's critical role in international trade and to draw on its considerable experience with due diligence efforts related to financial transactions.

First, financial institutions should be tasked to play a key role in the monitoring of trade in export-controlled goods and in impeding illicit transactions. Any trade is inevitably reflected in a corresponding financial transaction. Because of the widespread involvement of coalition-based producers, an initial link to the United States and European financial systems should exist for many of the transactions in

question. Even if a large share of the goods under export restrictions is produced abroad, the fact that the company is incorporated in a coalition country means that a financial transaction will ultimately need to involve a Western-registered financial firm.

Export controls enforcement faces similar challenges to anti-money laundering and countering the financing of terrorism (AML/CFT): complex chains of custody, opaque ownership structures, frequent institutional changes, reliance on less-strict jurisdictions for the set-up of circumvention schemes, and often highly fungible goods.¹⁶ Because of the regulatory framework that has been established over the past two decades in these areas, financial institutions have already built an internal compliance architecture to detect such schemes. While some modifications to the legal framework and internal procedures may be required to apply existing AML/CFT regulations to the sanctions sphere, banks, fundamentally, have access to much of the information needed to trace the trade in export-controlled goods.

The US government has sent a clear signal to financial institutions that it acknowledges banks' critical role. Specifically, President Biden issued an Executive Order that provides the US Treasury Department's Office of Foreign Assets Control (OFAC) with new powers to target foreign financial institutions that *'conduct or facilitate significant transactions or provide any service involving Russia's military-industrial base'*.¹⁷ In case of non-compliance, banks may face comprehensive restrictions, including prohibitions on opening and/or maintaining correspondent accounts or payable-through accounts in the United States, and blocking of property in the United States.

While a conducive incentive structure has been established by regulators and enforcement agencies in recent years through legal requirements, investigations

of violations and imposition of significant fines—and banks themselves have set up compliance departments and instituted compliance cultures—three things are needed to properly leverage the financial system's role in international trade:

- (i) Changes to the existing regulatory framework in areas such as AML and CFT to eliminate loopholes. The interrelation between money laundering and sanctions evasion has been repeatedly highlighted by various authorities,¹⁸ and some of the most significant enforcement actions by OFAC in recent years relate to sanctions evasion schemes that could have been prevented with a proper application of AML procedures.¹⁹ However, a closer look at the existing AML/CFT regime reveals critical weaknesses in the form of regulatory and supervisory fragmentation as well as loopholes which impede transparency see Freiha Granjo and Martini (2021). Banks would benefit from the application of the AML/CFT frameworks with stricter ownership and control tests in the context of sanctions. Currently, EU and US sanctions legislation and regulations rely on a 50% threshold for ownership/control to identify assets as the property of sanctioned individuals or entities.²⁰
- (ii) Access to critical information specifically related to the trade in export-controlled goods. When it comes to the specific issue of export control enforcement, a major challenge is that banks may not have the information needed to screen for potentially problematic deals. After all, financial institutions have set up their compliance systems to identify counterparties that may be problematic, while export control implementation requires spotting specific illicit transactions. Changes to the legal framework are needed to put financial institutions in a position to properly play the role that we are proposing. Mandatory disclosure is needed of information on cross-border transactions, including when executed via the SWIFT (Society for Worldwide Financial Telecommunications) financial messaging system. For instance, a description of goods and/or services is currently optional in the case of letters of credit in trade. This is a significant challenge for banks: While they have the legal right to request additional information from the parties involved in a transaction, the inability to determine whether goods are export-controlled makes it difficult to conclude in which cases this should be done. Given the large number of cross-border transfers that banks carry out daily, this is a major practical limitation.
- (iii) Clear guidance to the financial industry to move towards a more risk-based approach. The current financial sanctions regime is far from that. Financial institutions face such a wide range

of regulatory requirements—from AML/CFT to sanctions—that they are often not able to properly prioritise tasks. For banks to be able to help enforce export controls, they have to be provided with specific guidance that not only clearly outlines regulatory requirements but also defines priorities. Sanctions will not become more effective if banks are simply forced to fill out additional paperwork, which satisfies supervisory authorities but does not help to identify illicit transactions involving export-controlled goods.²¹ While financial institutions have their own reasons for objecting to them, onerous regulatory requirements are not only a problem in terms of the cost of compliance, they can actually significantly reduce the overall effectiveness of the industry's involvement in AML, CFT and sanctions implementation.

Second, non-financial companies can learn from banks' efforts in the AML/CFT sphere to implement proper due diligence procedures and ensure compliance with export controls. The involvement of non-financial companies is crucial for better implementation and enforcement of sanctions and export controls. Companies from sanctioning countries continue to account for a substantial share of the high-priority battlefield items that reach Russia—40% in value terms in 2023. As these goods are overwhelmingly manufactured in third countries (61%) and shipped to Russia from there (93%), thus, likely never physically passing through coalition jurisdictions, compliance efforts must start with the sellers that are incorporated in sanctioning countries. After the initial sales, it becomes increasingly challenging, if not impossible, to monitor supply chains and to impede transactions.

For due-diligence efforts to succeed it is critical to properly understand who one is conducting business with. In the financial industry, this is known as 'know your client' (KYC) and has been expanded over time to also involve a partners' subsequent business relationships. Export-control regimes would be much more effective if non-financial companies were required to do this as well. It means that companies need to implement procedures to identify trusted intermediaries that they can rely on for the distribution of their goods without running the risk of subsequent on-shipments of the products to Russia. And they have to take decisive steps to rework supply chains should violations take place within this network. While this is not an easy task, proper due diligence with regard to export-controlled goods is not more complex than similar efforts instituted in recent decades for the monitoring of financial transactions.

The most important challenge for effective export controls enforcement is the inadequate incentive structure. Ultimately, companies undertake very straightforward calculations weighing the costs of compliance—for

example, loss of business or resources invested in due-diligence procedures—the risk of discovery in the case of violations of laws and regulations, and the size of the penalties incurred. Many financial institutions have faced substantial monetary penalties in recent years as law enforcement and supervision have become stricter. But the situation is different for non-financial companies. It will be critical for enforcement agencies to demonstrate an ability and willingness to investigate sanctions violations and impose significant fines. Unless and until coalition governments send clear signals to the private sector, businesses' calculations on risks and rewards are unlikely to change.

Two changes to the legal framework can play an important role to change companies' risk assessments: criminalisation of sanctions violations and detailed negligence provisions. On the first point, the Council and the European Parliament at the end of 2023 reached agreement on a law.²² Negligence provisions such as those currently under discussion in the EU can also make a difference as they define clearly which steps individuals and companies must undertake in order to fall under safe-harbour provisions that protect them from civil or criminal liability.²³ All coalition jurisdictions should align their laws to ensure that sanctions violations constitute crimes when committed with serious negligence, that is, if companies knew or *should have known* that their actions could undercut export restrictions of battlefield goods. The EU, in its twelfth sanctions package, established a legal requirement for companies to include 'no re-export to Russia' clauses in their contracts. This clearly defines the due diligence required from EU-based companies in their dealings with export-controlled goods.²⁴ Many coalition countries have issued guidance to the private sector on trade in export-controlled goods, including the United States²⁵—a welcome development but not sufficient in our view. Rather, these procedures should become mandatory requirements.

Part of creating incentives is also the building-up of adequate institutional resources across coalition jurisdictions. Even in the United States, where authorities have somewhat more experience with export controls, the agency in question—the US Department of Commerce's Bureau of Industry and Security (BIS)—does not have the personnel for the enforcement of comprehensive measures like those in the Russia case. In the European Union, the institutional challenges are even bigger. Currently, member states remain responsible for the enforcement of sanctions, including those adopted at EU level, which inevitably leads to fragmentation in their implementation. Many EU countries also do not have sufficiently empowered and resourced agencies. The United Kingdom recently announced the establishment of a new entity for trade sanctions implementation: OTSI.²⁶ The EU should follow suit and create unified enforcement structures as soon as possible.

In addition to the aforementioned incentive structure and clear guidance related to legal obligations, non-financial companies need to be given sufficient access to information. Otherwise, they will not be able to implement effective compliance procedures and/or the costs of such efforts will be unreasonably high. After all, the objective of what we propose is to allow for any legal trade with export-controlled goods to take place without onerous requirements. In terms of access to critical information, banks have more comprehensive rights under existing regulations, including their ability to approach counterparties in financial transactions to request additional data. Specifically, transparency with regard to business partners throughout the supply chain can only be achieved for non-financial companies if they are provided with the same access to, for instance, beneficial ownership registries, as financial institutions enjoy.

4 | CONCLUSIONS: TOWARDS EFFECTIVE AND CREDIBLE EXPORT CONTROLS

Export controls can only be effective if enforced properly. We have documented that many battlefield products that are banned under the existing sanctions regime still reach Russia. A significant part of these goods stems from companies headquartered in sanctioning countries, with the goods moving via third countries and with several intermediaries involved. Foreign components in Russian weapons are still basically sourced from Western companies, suggesting that substitution is not easily achieved.

To ensure effective export controls, enforcement needs to step up. The challenges are multifaceted and centre around complex supply chains, lack of transparency in documentation and opaque financial structures. Enforcement of export controls, thus, faces similar issues to those well-known—and substantively addressed—issues in anti-money laundering and the countering of terrorist finance.

The financial system's critical role in international trade should be leveraged. In trade finance, it would be straightforward for financial institutions to monitor the purpose of a financial transaction. For other financial services, however, changes to the regulatory framework are needed to eliminate loopholes, improve access to critical information related to the trade with export-controlled goods and provide clear guidance to the financial industry to move towards a more risk-based approach.

Finally, lessons can be learned from the considerable experience of banks with due-diligence efforts and applied to non-financial companies. Firms need to have clear incentives to trace transactions involving

export-controlled goods and control their supply chains effectively. Knowing your customers is a crucial first step that needs to become mandatory for all companies dealing with battlefield goods. But incentives also need to be set so that this costly monitoring is undertaken. In finance, it took considerable fines for financial institutions to set up substantial compliance departments. Increasing fines and the likelihood for detection, while also providing support to companies to enable proper due diligence, are crucial. Including clauses in government subsidy agreements with Western firms related to compliance with export controls could further incentivise firms to step up efforts. Sanctions enforcement will be further strengthened by widening the coalition of participating countries.

Better enforcement is undoubtedly going to be burdensome on both public authorities and companies. There are trade-offs to enforcement and the cost of implementation is non-zero. Moreover, properly designing the governance of enforcement and ensuring optimal government supervision of companies without creating unnecessary bureaucracy is crucial. Stepping up enforcement efforts is still very much advisable. First, Russia's war effort critically depends on technology access, and Ukrainian and broader European security is at stake. While 40% of battlefield goods under sanctions come from companies in coalition countries, the percentage of their products in the actual weapons is significantly higher, at above 95%. Second, the effectiveness of sanctions against Russia will also be considered as a test case for any future conflicts, meaning that Western credibility is at stake. Third, the longer the war lasts, the greater will be the general costs for the economy. For the public sector, high upfront costs of greater Ukraine support and better sanctions enforcement may be a price worth paying, compared to a drawn-out conflict that undermines economic sentiment and dynamic entrepreneurship. In addition, the West is providing Ukraine with costly and scarce air-defence capabilities needed to defend Ukrainians against missiles and drones that Russia is able to produce at increasing rates due to insufficient export controls enforcement.

ACKNOWLEDGEMENTS

The authors thank Olena Bilousova, Emily Kilcrease, Clay Lowery, Nataliia Shapoval, Nicolas Véron and Bruegel research seminar participants for their contributions and comments.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ENDNOTES

- ¹ See the EU's version of the list: https://finance.ec.europa.eu/publications/list-common-high-priority-items_en (accessed 12 April 2024). The same items have been identified by authorities in Japan, the United Kingdom and the United States. The list has been expanded twice to reflect new insights into critical inputs for the Russian military industry, among them non-electronic components (e.g. bearings) and machinery for local production of certain items (e.g. CNC tools).
- ² See the National Agency on Corruption Prevention's database on foreign components in Russian weapons: <https://sanctions.nazk.gov.ua/en/military-components/> (accessed 20 March 2024).
- ³ See the National Agency on Corruption Prevention's database on foreign equipment used for military production: <https://sanctions.nazk.gov.ua/en/military-tools/> (accessed 20 March 2024).
- ⁴ The Foreign Direct Product Rule (FDPR; 15 CFR § 734.9) establishes the extraterritorial effect of US export controls. In essence, it states that Export Administration Regulations (EAR) — ie export controls — apply not only to products manufactured in the US, but that “foreign-produced items located outside of the United States are subject to the EAR when they are a ‘direct product’ of specified ‘technology’ or ‘software,’ or are produced by a complete plant or ‘major component’ of a plant that itself is a ‘direct product’ of specified ‘technology’ or ‘software.’” See the US Code of Federal Regulations: <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.9> (accessed 12 April 2024). For more on the FDPR, please also see ‘The history and limits of America's favourite new economic weapon’, *Economist*, 8 February 2023, <https://www.economist.com/united-states/2023/02/08/the-history-and-limits-of-americas-favourite-new-economic-weapon> (accessed 12 April, 2024) and Jane Lee and Stephen Nellis, ‘Explainer: What is ‘FDPR’ and why is the U.S. using it to cripple China's tech sector?’, *Bloomberg*, 8 October 2022, <https://www.reuters.com/technology/what-is-fdpr-why-is-us-using-it-cripple-chinas-tech-sector-2022-10-07/> (accessed 12 April 2024).
- ⁵ ‘Technology sanctions’ is a somewhat broader term than ‘export controls’ and may include measures beyond restrictions on sales to a certain country or entity, for instance prohibition of investments of transfer of intellectual property.
- ⁶ See, for instance, testimony by Daleep Singh, Clay Lowery, and Kevin Wolf before the Senate Committee on Banking, Housing, and Urban Affairs in February 2023: <https://www.banking.senate.gov/hearings/advancing-national-security-and-foreign-policy-through-sanctions-export-controls-and-other-economic-tools> (accessed 12 April 2024).
- ⁷ The use of the financial system was proposed to improve energy sanctions enforcement and address the challenge of Russian shadow reserves abroad (Hilgenstock et al., 2023).
- ⁸ Rácz et al. (2023) provided evidence that export restrictions in 2022 effectively limited some military production in Russia.
- ⁹ For an analysis of price changes for goods from two key producers, Analog Devices and Texas Instruments, see Box 1 in Bilousova et al. (2024). See also Chupilkin et al. (2024).
- ¹⁰ Goods identified by the EU, Japan, UK and US as enforcement priorities (ie ‘Common High Priority Items’).
- ¹¹ The following jurisdictions have imposed export controls on Russia and are part of what we define as the ‘export controls coalition’ for the purpose of this analysis: Australia, Canada, European Union, Japan, New Zealand, Norway, South Korea, Switzerland, Singapore, Taiwan, United Kingdom and the United States.
- ¹² See the National Agency on Corruption Prevention's database on foreign components in Russian weapons: <https://sanctions.nazk.gov.ua/en/military-components/> (accessed 12 March 2024).

- ¹³ We do not find similar dynamics for other countries bordering Russia or having close economic relations with Russia, including Tajikistan, Turkmenistan, and Uzbekistan.
- ¹⁴ <https://reb.org.ua/en/reporting/zapasni-variant-dlya-agresora-novii-zvit-reb-pro-rol-kitayu-u-zberezeni-dostupu-rosiyi-do-kriti-cno-vazlivogo-promislovogo-obladnannya-v2qm62>.
- ¹⁵ See Elina Ribakova, 'Economic sanctions risk losing their bite as a US policy weapon', *Financial Times*, 7 November 2023, <https://www.ft.com/content/b54201be-f307-4171-bb99-b356537b1898> (accessed 12 April 2024). See also testimony by Elina Ribakova before the United States Senate: <https://www.hsgac.senate.gov/subcommittees/investigations/hearings/the-u-s-technology-fueling-russias-war-in-ukraine-how-and-why/> (accessed 12 April 2024).
- ¹⁶ See 'Clamping down on Russia's sanctions evasion', *Financial Times*, 18 May 2023, <https://www.ft.com/content/5ecbc9f0-ee9e-46db-8a67-91f2fdf985d3> (accessed 12 April 2024).
- ¹⁷ See 'Executive Order on Taking Additional Steps With Respect to the Russian Federation's Harmful Activities': <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/12/22/executive-order-on-taking-additional-steps-with-respect-to-the-russian-federations-harmful-activities/> (accessed 12 April 2024). See also 'Statement from Secretary Yellen on President Biden's Executive Order Taking Additional Steps With Respect to Russia's Harmful Activities': <https://home.treasury.gov/news/press-releases/jy2011> (accessed 12 April 2024). Furthermore, see OFAC's sanctions advisory 'Guidance to Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base': <https://ofac.treasury.gov/media/932436/download?inline> (accessed 12 April 2024).
- ¹⁸ For instance, the UK House of Commons Committee issued a report 'The cost of complacency: illicit finance and the war in Ukraine', which details how Russian oligarchs and kleptocrats use legal loopholes in AML and sanctions regulations and provides related policy recommendations: <https://committees.parliament.uk/publications/22862/documents/167820/default/> (accessed 12 April 2024). Furthermore, in March 2022, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an alert identifying certain "red flag indicators" for financial institutions to detect sanctions evasion attempts. See the FinCEN alert of 7 March 2022, 'FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts', <https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evolution%20FINAL%200508.pdf> (accessed 12 April 2024). The alert also reminds financial institutions of their reporting obligations under the Bank Secrecy Act as well as due diligence obligations and other procedures that are part of the AML regime.
- ¹⁹ For example, in March 2023, OFAC sanctioned 39 entities "constituting a significant 'shadow banking' network, one of several multi-jurisdictional illicit finance systems which grant sanctioned Iranian entities (...) access to the international financial system and obfuscate their trade with foreign customers." See OFAC's press release of 9 March 2023, 'Treasury Targets Sanctions Evasion Network Moving Billions for Iranian Regime', <https://home.treasury.gov/news/press-releases/jy1330> (accessed 12 April 2024).
- ²⁰ Specifically, the Update of the EU Best Practices for the effective implementation of restrictive measures states that "[t]he criterion to be taken into account when assessing whether a legal person or entity is owned by another person or entity is the possession of more than 50% of the proprietary rights of an entity or having majority interest in it. If this criterion is satisfied, it is considered that the legal person or entity is owned by another person or entity." See the Council of Europe publication: <https://data.consilium.europa.eu/doc/document/ST-8519-2018-INIT/en/pdf> (accessed 12 April 2024).
- ²¹ The US government appears to consider adding a special code to suspicious activity reports (SAR) through which financial institutions would be able to denote possible export control violations and, thus, guide raise red flags for BIS investigations.
- ²² See the European Council press release of 12 December 2023, 'Council and Parliament reach political agreement to criminalise violation of EU sanctions', <https://www.consilium.europa.eu/en/press/press-releases/2023/12/12/council-and-parliament-reach-political-agreement-to-criminalise-violation-of-eu-sanctions/> (accessed 12 April 2024).
- ²³ The aforementioned agreement's language on this topic might not go far enough as trade with war material would only constitute a criminal offence when committed intentionally or with *serious* negligence. The European Parliament has been pushing for stricter provisions that do not require *serious* negligence.
- ²⁴ See FAQs to the 'no re-export to Russia' clause by the European Commission: https://finance.ec.europa.eu/document/download/7f54341b-2bf1-4142-b5d4-b1b09c93d03e_en?filename=faqs-sanctions-russia-no-re-export_en.pdf (accessed 12 April 2024).
- ²⁵ See the US Department of State business advisory of 23 February 2023, 'Risks and Considerations for Doing Business in the Russian Federation and Russia-Occupied Territories of Ukraine', <https://www.state.gov/russia-business-advisory/> (accessed 12 April 2024).
- ²⁶ See the Office of Trade Sanctions Implementation press release of 11 December 2023, 'New unit to crack down on firms dodging Russian sanctions', <https://www.gov.uk/government/news/new-unit-to-crack-down-on-firms-dodging-russian-sanctions> (accessed 12 April 2024).

REFERENCES

- Bilousova, O., Hilgenstock, B., Ribakova, E., Shapoval, N., Vlasyuk, A. & Vlasuk, V. (2024) *Challenges of export controls enforcement: how Russia continues to import components for its military production*. Kyiv, Ukraine: KSE Institute. Available from: <https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf>
- Chupilkin, M., Javorcik, B., Peeva, A. & Plekhanov, A. (2024) *Decision to leave: economic sanctions and intermediated trade*. London: European Bank for Reconstruction and Development, forthcoming.
- Drezner, D.W. (2003) Bargaining, enforcement, and multilateral sanctions: when is cooperation counterproductive? *International Organization*, 54(1), 73–102. Available from: <https://doi.org/10.1162/002081800551127>
- Fraiha Granjo, A. & Martini, M. (2021) Access denied? Availability and accessibility of beneficial ownership data in the European Union, Transparency International. Available from: <https://images.transparencycdn.org/images/2021-Report-Access-denied-Availability-and-accessibility-of-beneficial-ownership-data-in-the-European-Union.pdf>
- Heathershaw, J., Cooley, A., Mayne, T., Michel, C., Prelec, T., Sharman, J. et al. (2021) *The UK's kleptocracy problem: how servicing post-soviet elites weakens the rule of law*. Research Paper, Chatham House. Available from: <https://www.chathamhouse.org/2021/12/uks-kleptocracy-problem>
- Hilgenstock, B., Ribakova, E. & Wolff, G. (2023) Toughening financial sanctions on Russia: enforcing energy sanctions and reducing shadow reserves effectively. *Intereconomics: Review of European Economic Policy*, 58, 201–208. Available from: <https://doi.org/10.2478/ie-2023-0042>
- Kupatadze, A. & Marat, E. (2023) *Under the radar: how Russia outmanoeuvres western sanctions with help from its neighbours*. Research Paper No. 18, University of Birmingham.

- Rácz, A., Spillner, O. & Wolff, G. (2023) *Russia's war economy*. DGAP Policy Brief 3, German Council Foreign Relations.
- Stognei, A. & Ivanova, P. (2023) Kazakhstan to step up monitoring of goods re-exported to Russia, Financial Times. Available from: <https://www.ft.com/content/b4e8c02a-adb5-4148-9b15-c0cf2845fa0f>
- Trehubova, A. (2023) *The impact of Chinese foreign aid on OFAC sanctions effectiveness: non-conditionality, non-interference, and the reality of Chinese foreign policy*. Master thesis, Stockholm University. Available from: <https://www.diva-portal.org/smash/get/diva2:1762792/FULLTEXT01.pdf>

Guntram Wolff is a Senior Fellow at Bruegel and Professor of Economics at the Université Libre de Bruxelles. Previously, he was Director and CEO of the German Council on Foreign Relations and Director of Bruegel. He focuses on European economy, climate policy, economic statecraft, macroeconomics and defence economics.

AUTHOR BIOGRAPHIES

Benjamin Hilgenstock is a Senior Economist at KSE Institute (Kyiv School of Economics) focusing on international sanctions on Russia, including in the areas of energy, trade and finance. He was previously an Economist at the Institute of International Finance and an analyst with the International Monetary Fund's Research Department.

Elina Ribakova is a Non-resident Fellow at the Peterson Institute for International Economics and at Bruegel as well as the Director of the International Affairs Program and Vice President for foreign policy at the Kyiv School of Economics. Her research focuses on global markets, economic statecraft and economic sovereignty.

Anna Vlasiuk is a Legal Research Fellow at KSE Institute (Kyiv School of Economics), focusing on legal aspects of sanctions as well as the issue of possible confiscation of Russian sovereign assets. Previously she worked at the National Investment Council under the President of Ukraine and in international investment arbitration.

How to cite this article: Hilgenstock, B., Ribakova, E., Vlasyuk, A. & Wolff, G. (2024) Enforcing export controls learning from and using the financial system. *Global Policy*, 00, 1–10. Available from: <https://doi.org/10.1111/1758-5899.13463>