WORKING PAPER | ISSUE 10/2024 | 29 APRIL 2024

# USING THE FINANCIAL SYSTEM TO ENFORCE EXPORT CONTROLS

BENJAMIN HILGENSTOCK, ELINA RIBAKOVA, ANNA VLASYUK, AND GUNTRAM WOLFF

Russian imports of battlefield goods that are subject to export controls, including from Western producers, 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 critical foreign components that it needs for its military industry. These imports 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 imports from the EU and other coalition countries that likely end up in Russia. The implementation and enforcement of export controls faces major challenges, which are multifaceted and centre around complex supply chains, lack of transparency in documentation and opaque financial structures. The issues are familiar from anti-money laundering (AML) and countering financing of terrorism (CFT) frameworks, where much progress has been made in the last two decades. A similar approach could help in rendering export controls effective. We propose: First, financial institutions could be tasked to play a role in the monitoring of the trade in export-controlled goods and the blocking of illicit transactions, building on their experience with due diligence in financial 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 are going to be part of the economic statecraft toolbox for the foreseeable future. The Russia case will test their effectiveness and credibility, or lack thereof.

Benjamin Hilgenstock is a Senior Economist at KSE Institute
Elina Ribakova (elina.ribakova@bruegel.org ) is a Non-resident Fellow at Bruegel
Anna Vlasyuk is a Project Manager at Office of the National Investment Council of Ukraine
Guntram Wolff (guntram.wolff@bruegel.org ) is a Senior Fellow at Bruegel

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

**Recommended citation:**
Hilgenstock, B., E. Ribakova, A. Vlasyuk and G. Wolff (2024) 'Using the financial system to enforce export controls', *Working Paper* 10/2024, Bruegel

## 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. The Coordinating Committee for Multilateral Export Controls (CoCom), which was established right after the Second World War and operated until 1994, played a central role in defining and implementing these export controls. 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 controls system – the Wassenaar Arrangement – that aims to limit the spread of specific weapons and dual-use goods. Russia is one of its 43 members[1].

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.

The EU adopted on 25 February 2022 wide-ranging export controls on dual-use goods as part of the union's second sanctions package[2]. On the previous day, the US Department of Commerce's Bureau of Industry and Security (BIS) amended its Export Administration Regulations (EAR) and extended the scope of the Foreign Direct Product Rule (FDPR) to apply strengthened export controls on Russia (and Belarus) and to ensure their extraterritorial application[3]. The UK also imposed restrictions on military and dual-use goods in February 2022[4].

Coalition countries have repeatedly tightened these restrictions and have also identified priorities for their enforcement – the so-called List of Common High Priority Items, often referred to as 'battlefield goods'[5]. These are prohibited dual-use and advanced technology products used in Russian military systems found on the battlefield in Ukraine[6], or critical to the development, production or use of those

---

[1] See information from the Arms Control Association, 'The Wassenaar Arrangement at a Glance', https://www.armscontrol.org/factsheets/wassenaar (accessed 12 April 2024).
[2] See the timeline of EU restrictive measures: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en (accessed 12 April 2024). See also the European Council's conclusions of 24 February 2022: https://www.consilium.europa.eu/en/meetings/european-council/2022/02/24/ (accessed 12 April 2024). See details on the package of individual and economic measures adopted on 25 February 2022: https://eur-lex.europa.eu/search.html?DB_COLL_OJ=oj-l&SUBDOM_INIT=ALL_ALL&DB_AUTHOR=council&DTS_SUBDOM=ALL_ALL&DTS_DOM=ALL&lang=en&type=advanced&date0=PD%3A25022022%7C25022022&qid=1647426657418 (accessed 12 April 2024).
[3] See BIS press release of 24 February 2023, 'Commerce Imposes Additional Export Restrictions in Response to Russia's Brutal War on Ukraine', https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3227-2023-02-24-bis-press-release-additional-russia-invasion-response-actions/file (accessed 12 April 2024).
[4] See the Russia (Sanctions) (EU Exit) (Amendment) (No. 3) Regulations 2022: https://www.legislation.gov.uk/uksi/2022/195/pdfs/uksi_20220195_en.pdf (accessed 12 April 2024).
[5] 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 UK and US. The list has been expanded twice to reflect new insights into critical inputs for the Russian military industry, among them non-electronic components (eg bearings) and machinery for local production of certain items (eg CNC tools).
[6] 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).

systems[7]. Microelectronics play a major role but the 50 Harmonised System (HS) codes on the list also include, among other things, communications and navigational equipment.

What sets the Russia-related export controls apart is not only their scope and the economic interconnectedness of their target. More importantly, to have an impact on the battlefield during an ongoing armed conflict, the imposed measures need to be implemented fast. The time horizon for ensuring the effectiveness of the measures is, thus, very different from the Iran and North Korea cases.

Export controls are here to stay beyond the specific circumstances of the Russia sanctions regime. 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)[8] clearly demonstrates that intent, together with (realised and planned) changes to outbound investment screening as a way to ensure that export-restricted items are not produced elsewhere to reach markets they are not supposed to reach. 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 sanctions[9] – and thus their effectiveness in constraining China – is equally on the line[10].

A well-established literature shows that the larger the coalition of countries enforcing sanctions, the more effective those sanctions are. A significant challenge in the context of Russia is exactly how many countries are willing to align with Western-led sanctions. China is the elephant in the room. It wants to avoid directly undermining Western sanctions and exposing itself to secondary US sanctions, especially in the financial sector. Yet, it has signalled at least partial alignment with Russia and is therefore probably not enforcing sanctions in certain areas. Section 2 provides empirical evidence on how sanctioned goods reach Russia via third markets.

On the whole, it is critical to investigate the impact of current restrictions against Russia and, if necessary, to find ways to improve them. We document Russia's continued ability to acquire goods that have been identified as enforcement priorities, and cite evidence that Russian weapons continue to incorporate significant amounts of Western technology that falls under export restrictions. We propose that financial institutions should play a larger role in increasing the effectiveness of export restrictions.

---

[7] 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).

[8] 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 favorite 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).

[9] '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.

[10] 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).

Moreover, we argue 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[11].

## 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. The extent of the problem is evident when looking at Russia's continued ability to import goods that the EU, US and other allies of Ukraine[12] have determined to be 'common high priority items' (aka 'battlefield goods'). This list comprises 50 six-digit Harmonised System (HS) product groups[13] deemed to be critical for Russia's military industry and largely consists of microelectronics and communications and navigational equipment.

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 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 2022[14]. In fact, 2023 imports were only 2 percent lower than in the pre-full-scale invasion period (Figure 1). Items of greatest concern (Tier 1) *"due to their critical role in the production of advanced Russian precision-guided weapons systems, Russia's lack of domestic production, and limited global manufacturers"*[15] alone accounted for $2.3 billion or 18 percent of the total. Tier 2 products – *"additional electronic items for which Russia may have some domestic production capability but a preference to source from the United States and its partners and allies"* – made up another $2.4 billion (or 19 percent).

While there is some evidence that Russia is forced to pay significant markups for export-controlled goods acquired through third countries[16], meaning the decline in volume terms is more pronounced than what trade values indicate, the implementation and enforcement of restrictions appears to be facing major challenges.

---

[11] This builds on proposals that we initially made to improve energy sanctions enforcement and address the challenge of Russian shadow reserves abroad (Hilgenstock *et al*, 2023).

[12] Also includes Japan and the United Kingdom.

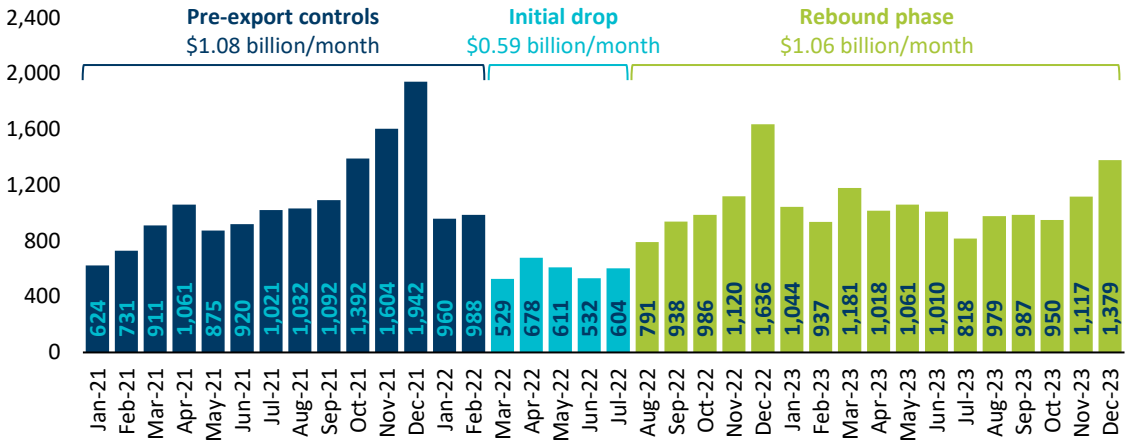
[13] The Harmonised Commodity Description and Coding System, (short, Harmonised System or HS) is a system to classify commodities, developed by the World Customs Organization (WCO). It identifies more than 5,000 groups of products by six-digit numerical codes, which are consistent across jurisdictions and used by more than 200 countries. According to the WCO, more than 98 percent of international merchandise trade is captured by HS codes. See the WCO website: https://www.wcoomd.org/en/topics/nomenclature/overview/what-is-the-harmonized-system.aspx (accessed 12 April 2024). While the system also contains aggregate categories (on the four- or two-digit level), six-digit codes allow to identify specific goods that are of particular importance for the Russian military industry and should be subject to export controls.

14 Racz *et al* (2023) provided evidence that export restrictions in 2022 effectively limited some military production in Russia.

[15] See the BIS's version of the Common High Priority Items List: https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items (accessed 12 April 2024). These include electronic integrated circuits.

[16] For an analysis of price changes for goods from two key producers, Analog Devices and Texas Instruments, see Box 1 in Bilousova *et al* (2023). See also Chupilkin *et al* (2024).

**Figure 1: Russian imports of battlefield goods, $ millions**




Source: KSE Institute.

Russia can thus acquire critical inputs that its economy and military industry require by using producers in China and other countries that have stepped in and 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. But equally worrying is the fact that Western technology still finds its way into Russian arms. A substantial share of Russia's battlefield goods[17] imports – 40.3 percent in 2023 – is produced on behalf of companies headquartered in coalition countries[18]. And evidence from the battlefield shows that Western components still dominate as far as actual weapons production is concerned: 95 percent of all foreign parts identified were sourced from producers in coalition countries, with 72 percent accounted for by US-based companies alone[19]. This could mean that Russia is not able to easily replace Western components with substitutes from, for instance, China. However, it could also mean that Russia has not been required to substitute Western products in weapons because access to such imports remains in place despite export controls.

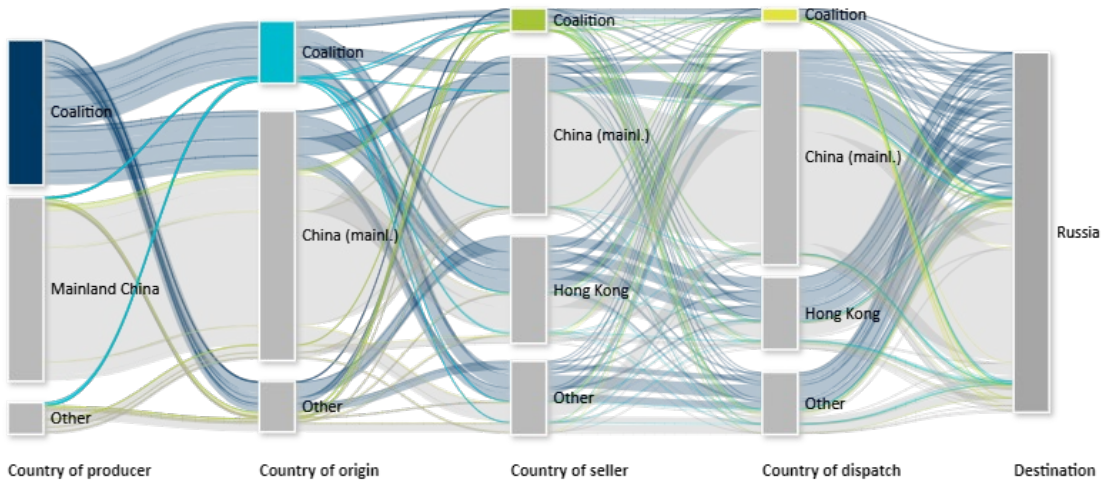
In most cases, albeit not exclusively, these goods are manufactured in third countries and reach Russia via intermediaries located in places including mainland China, Hong Kong, Turkey and the United Arab Emirates (Figure 2). As direct shipments from sanctions coalition countries dropped markedly – accounting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

Circumvention is not limited to the aforementioned jurisdictions. We also observe worrying trends for countries of the Eurasian Economic Union (EEU)– namely Armenia, Kazakhstan and the Kyrgyz

[17] Goods identified by the EU, Japan, UK and US as enforcement priorities (ie 'Common High Priority Items').
[18] 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.
[19] 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).

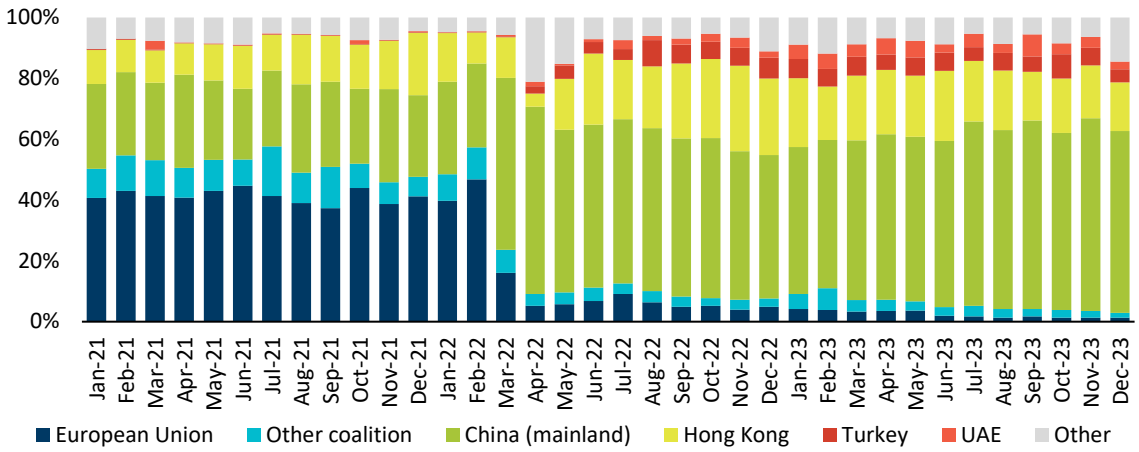
Republic – whose trade with Russia is not fully reflected in the data underlying Figures 1-3. Exports from the coalition, in particular the EU, to these three countries and Georgia have risen sharply, coinciding with the imposition of export controls on Russia (Figure 4)[20].

**Figure 2: Flows of battlefield goods to Russia in 2023**[21]




Source: KSE Institute. Notes: 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.

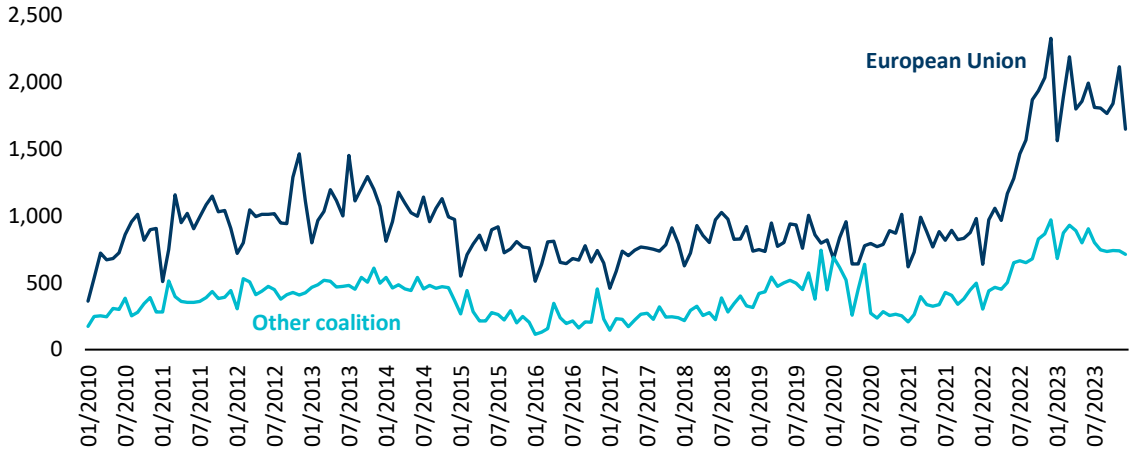
**Figure 3: Russian imports of battlefield goods by location of shipment, in %**




Source: KSE Institute.

[20] We do not find similar dynamics for other countries bordering Russia or having close economic relations with Russia, including Tajikistan, Turkmenistan, and Uzbekistan.
[21] Figure only includes transactions for which the full chain of custody could be determined (80 percent of the total value).

**Figure 4: Exports to Armenia, Georgia, Kazakhstan and the Kyrgyz Republic, $ millions**




Source: International Monetary Fund. Notes: Other coalition: Australia, Canada, Japan, New Zealand, Norway, Singapore, South Korea, Switzerland, United Kingdom and United States.

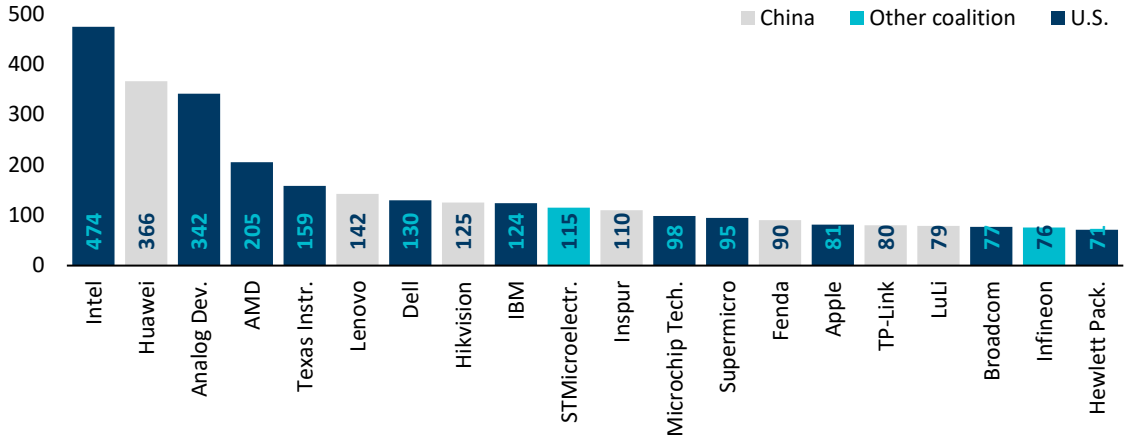
These trade dynamics, and the evidence from the battlefield, show that Russia has not been able to substitute certain high-technology Western goods and that export controls therefore remain a powerful tool of economic statecraft. However, it is also clear that enforcement needs improvements urgently, 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 exist to ensure the legality of financial transactions. However, the effectiveness of relying on the private sector is increasingly under threat as the economic statecraft toolbox expands to comprehensive technology sanctions. Gaps in the legal framework make it difficult to trace export control-related transactions, and regulations do not require the same level of diligence that banks have become accustomed to in areas such as anti-money laundering.

As far as export controls are concerned, 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 something is 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[22].

[22] 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).

**Figure 5: Russian imports of battlefield goods in 2023 by producer, $ millions**




Source: KSE Institute.

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 simply do not possess the resources needed to 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 smart phones, 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 in 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 might be 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 in itself is not a reason to start an 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? How to ensure 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.

In the following, we make proposals on: (1) how the financial system can be better used to detect such transactions (see section 3.1), and (2) what can be learned from existing practices, eg in anti-money laundering and anti-terrorist financing, for enforcement (section 3.2).

## 3 The financial system's role in improving export controls

To improve 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 could be tasked to play a key role in the monitoring of trade in export-controlled goods and in impeding illicit transactions.** Export controls enforcement faces similar challenges to anti-money laundering and countering 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[23]. Because of 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. 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 – and the experience and resources to use it. We explain below in more detail how this can be done but, intuitively, the continued dominance of banks from coalition countries within the global financial system should enable them to trace the corresponding financial transactions to many physical shipments of export-controlled goods.

***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.** Their involvement is critical for improved implementation and enforcement, as it can significantly reduce the number of problematic trades. As detecting and preventing suspicious transactions involving export-controlled goods is a legitimately difficult task considering the complexity of supply chains, companies should build on banks' experience with 'know your client' (KYC) standards and related due-diligence procedures to ensure that risks of illegality from financial flows, even from known clients, is reduced. In this context, the incentive structure is vital. After all, banks established their compliance infrastructures because of a very straightforward risk calculation: the potential financial penalties simply outweigh the costs. But to get to this point, authorities had to demonstrate an ability and willingness to investigate violations and impose significant fines[24]. In the case of non-financial companies, this is simply not the case yet as they are not regulated in the same way. It needs to be clearly established that there is a high cost to non-compliance, and the probability of detection has to increase substantially for companies' behaviour to change[25].

### 3.1 Using financial institutions to monitor trade flows and stop violations

Financial institutions, particularly those incorporated in coalition countries, should play a greater role in the monitoring and, if needed, interruption of transactions related to export-controlled goods. Any

[23] 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).
[24] See, for example, Osman Husain, '12 Biggest Anti-Money Laundering (AML) Fines, $500 Million and Above', https://www.enzuzo.com/blog/biggest-aml-fines (accessed 12 April 2024).
[25] For examples of export controls-related enforcement action and challenges, see Boxes 3-6 in Bilousova *et al* (2024).

trade is inevitably reflected in a corresponding financial transaction. Because of the widespread involvement of coalition-based producers, an initial link to the US 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 and, thus, the items never physically touch the territory of any sanctions-imposing country, 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 and is therefore traceable. There is a second argument for banks' playing a critical role: they have accumulated considerable experience with, and have built-up institutional resources, for the tracing of financial transactions in the AML/CFT sphere, which they can use for monitoring financial transactions related to goods under export controls.

#### *3.1.1 Leveraging banks' critical role in the trade in export-controlled goods*

The fact that large, multinational companies appear to be the initial sellers of a significant share of the trade in controlled goods – independent of where the items are manufactured – means that financial institutions from coalition jurisdictions are involved in the transactions, either as the seller's bank or via correspondent accounts due to the trade's execution in US dollar. The US government has sent a clear signal to financial institutions that it acknowledges their critical role. Specifically, President Biden issued in 2023 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"*[26]. 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 US. Such measures – so-called secondary or extraterritorial sanctions – could have a dramatic effect on any targeted, internationally-operating financial institution.

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; (ii) access to critical information specifically related to the trade in export-controlled goods; and (iii) clear guidance to the financial industry to move towards a more risk-based approach.

[26] 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).

### *3.1.2 Revising regulatory frameworks to support compliance*

The interrelation between money laundering and sanctions evasion has been repeatedly highlighted by various authorities[27], and some of the most significant enforcement actions by the Office of Foreign Assets Controls (OFAC) in recent years relate to sanctions evasion schemes that could have been prevented with proper application of AML procedures[28]. In some instances, financial institutions have been found to willingly help sanctioned entities avoid restrictions and AML requirements[29]. For instance, Turkish state-owned Halkbank is now on trial in the United States for *"launder*[ing] *billions of dollars of Iranian oil and gas proceeds through the global and U.S. financial system"*[30].

The anti-money laundering (AML) and countering financing of terrorism (CFT) frameworks can be instrumental in better enforcement of sanctions – and, specifically, export controls. In fact, the frameworks aim to improve transparency of the identity, beneficial ownership, institutional setup and

---

[27] 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%20Evasion%20FINAL%20508.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.

[28] 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).

[29] For instance, from 2004 to 2015, Bahrain's Future Bank assisted the Iranian regime in concealing $7 billion in trade transfers by forging documents and using 'wire-stripping', ie removing or changing the identifying information of a bank transfer. See Souad Mekhennet and Joby Warrick, 'Billion-dollar sanctions-busting scheme aided Iran, documents show', *Washington Post*, 3 April 2018, https://www.washingtonpost.com/world/national-security/billion-dollar-sanctions-busting-scheme-aided-iran-documents-show/2018/04/03/37be988a-3356-11e8-94fa-32d48460b955_story.html (accessed 12 April 2024). Similarly, in 2010, Barclays was fined for using wire-stripping to conceal $500 million in financial transactions with Iran. See the U.S. Department of Justice press release of 18 August 2010, 'Barclays Bank PLC Agrees to Forfeit $298 Million in Connection with Violations of the International Emergency Economic Powers Act and the Trading with the Enemy Act', https://www.justice.gov/opa/pr/barclays-bank-plc-agrees-forfeit-298-million-connection-violations-international-emergency (accessed 12 April 2024).

[30] Halkbank's alleged criminal conduct included facilitation of an estimated $20 billion of money transfers through the international financial system. Among other things, the bank used front companies in Iran, Turkey, and the United Arab Emirates for certain transactions, and facilitated transactions fraudulently designed to appear to be purchases of food and medicine and, thus, fall under 'humanitarian exceptions' to the sanctions regime. See US Department of Justice press release of 15 October 2019, 'Turkish Bank Charged in Manhattan Federal Court for Its Participation in a Multibillion-Dollar Iranian Sanctions Evasion Scheme', https://www.justice.gov/opa/pr/turkish-bank-charged-manhattan-federal-court-its-participation-multibillion-dollar-iranian (accessed 12 April 2024). Major financial institutions that processed billions in Halkbank transactions through correspondent relations — namely, Bank of America, Citibank, Deutsche Bank, HSBC, JP Morgan Chase, Standard Chartered, UBS, and Wells Fargo — were identified in case materials as *"victim banks"*. See Senator Ron Wyden press release of 25 October 2019, 'Wyden Launches Investigation Into Halkbank Scandal', https://www.finance.senate.gov/ranking-members-news/wyden-launches-investigation-into-halkbank-scandal (accessed 12 April 2024). See also Supreme Court of the United States, No. 21-1450, Turkiye Halk Bankasi A.S., aka Halkbank, Petitioner vs. United States, https://www.supremecourt.gov/opinions/22pdf/21-1450_5468.pdf (accessed 12 April 2024).

business activities of counterparties. This is exactly what is needed for banks and non-financial companies as they undertake the kind of due diligence that we propose. Companies' efforts have to go beyond a 'simple' screening of business partners. Instead, a comprehensive mapping of supply chains and identification of potential 'red flags'[31] is required. 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. In Annex 1, we discuss such issues in three key jurisdictions: the EU, United States and United Kingdom.

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 percent threshold for ownership/control to identify assets as the property of sanctioned individuals or entities[32]. In contrast, Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing contains a much broader definition, stipulating that *"'beneficial owner' means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted"*[33]. Moreover, the directive states that ownership through a trust falls within its scope, which

---

[31] A critical step toward better sanctions enforcement would also be the blacklisting of Russia by the Financial Sanctions Task Force (FATF). So far, the organisation has only suspended the country's membership (in February 2023) and expressed concerns over Russia's arms trade with jurisdictions sanctioned by the United Nations. See the 'FATF Statement on the Russian Federation' of 24 February 2023, https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html (accessed 12 April 2024). The FATF blacklist identifies countries or jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and financing of proliferation and inclusion on the list triggers enhanced due diligence and, in the most serious cases, FATF member countries are called upon to apply counter-measures to protect the international financial system from risk emanating from a certain country or jurisdiction. See the FATF '"Black and grey" lists': https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html (accessed 12 April 2024). Currently, only three countries are blacklisted by FATF: Iran, Myanmar, and North Korea. We argue that Russia poses such an imminent risk and its blacklisting is long overdue to restrict its ability to circumvent sanctions. For more details on recent efforts to weaken AML/CFT regulations, see 'Госдума приняла закон о выводе религиозных организаций из-под "антиотмывочных" норм', *Tass*, 18 April 2023, https://tass.ru/ekonomika/17550173 (accessed 12 April 2024). For Russia's rapprochement with two with two jurisdictions sanctioned by the United Nations and identified as state sponsors of terrorism by the U.S. (Iran and North Korea) see, for instance Maziar Motamedi, 'What's behind Iran and Russia's efforts to link banking systems?', *Al Jazeera*, 8 February 2023, https://www.aljazeera.com/news/2023/2/8/whats-behind-iran-and-russias-efforts-to-link-banking-systems (accessed 12 April 2024). See also United Nations Security Council Report S/2021/211, 'Final report of the Panel of Experts submitted pursuant to resolution 2515 (2020)', https://documents.un.org/doc/undoc/gen/n21/034/37/pdf/n2103437.pdf?token=pju9bfVo0irmipjfXK&fe=true (accessed 12 April 2024).

[32] 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).

[33] See Directive (EU) 2015/849: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849 (accessed 12 April 2024). In the case of corporate entities, *"[a] shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control."* Moreover, the directive states that ownership through a trust is falling within its scope—which is not the case for sanctions legislation. It provides guidance on identifying trust ownership and permits for member states to set even lower threshold for the purpose of identifying ownership.

is not the case for sanctions legislation. It provides guidance on identifying trust ownership and allows EU countries to set even lower thresholds for the purpose of identifying ownership.

### *3.1.3 Expanding access to critical information for export controls enforcement*

When it comes to the specific issue of export controls 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 controls implementation requires spotting specific illicit transactions. In some cases, banks may have access to this information, in other cases, they do not at this point. For instance, there is an important distinction between an involvement in trade finance and the 'simple' execution of cross-border transactions. In the case of the former, trade finance agreements contain a wealth of information, including on entities and the specific goods, allowing banks to determine if export-controlled items are traded and/or red flags appear for any of the entities involved. In the case of the latter, banks do not have information on the specific goods that are part of a transaction. They can only do a basic screening of the transfer's recipient.

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 determine 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. A related issue is that export controls, insofar as they are based on dual-use goods lists, have only recently begun to include specific numerical trade codes (Harmonised System or HS codes) as well – a critical step to enable better implementation.

### *3.1.4 Providing clear guidance and moving towards a risk-based system*

The current financial sanctions regime is far from a risk-based approach. 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. Instead, this leads to the fulfilment of formal legal requirements without too much consideration given to national security considerations. Ultimately, this is the result of a lack of coordination between government agencies engaged in sanctions enforcement (eg OFAC and FinCEN) and financial industry supervisors. 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, eg suspicious activity reports (SARs), which satisfy supervisory authorities but do not help to identify illicit transactions involving export-controlled goods[34]. While financial institutions have their own reasons for objecting to them, onerous regulatory requirements are not only

[34] 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.

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.

Clear guidance is particularly important when it comes to small- and medium-sized institutions, which do not have the same resources for compliance efforts but actually play a major role with regard to trade finance. To enable them to implement export controls-related due-diligence procedures, it is necessary to do more than simply define additional regulatory requirements. Instead, authorities need to work with the industry, including trade organisations, to develop systems that work for different players in the financial sector, from global banks to smaller institutions. Again, the focus has to be on creating an effective system that delivers results rather than simply increasing the regulatory burden. Ultimately, leveraging the role of banks to improve export controls enforcement will require government agencies and the private sector to cooperate closely.

### 3.2 Empowering the corporate sector by applying lessons from the financial system

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 percent in value terms in 2023. As these goods are overwhelmingly manufactured in third countries (61 percent) and shipped to Russia from there (93 percent), 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. In practice, this 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.

It is important to recognise that the implementation of financial sanctions and export controls differs considerably. The former are defined by governments and largely enforced by private-sector compliance regimes, with investigations and legal proceedings providing important incentives. The latter rely much more on audits and traditional law-enforcement techniques. Ultimately, what we propose is to move more towards compliance procedures, in this case by non-financial companies.

#### *3.2.1 Understanding complex supply chains and holding distributors accountable*

The most important element of such due-diligence efforts is 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. Russia's continued ability to import components for its military industry shows that whatever the companies are already doing is not sufficient. In addition, companies need to be obliged legally to take action should it become clear that a business partner is violating contractual arrangements (eg end-user agreements) intended to ensure that controlled goods do not reach certain jurisdictions. Any trade with such entities would need to end immediately if the violation occurred deliberately or was the result of a distributor's inadequate due-diligence checks on its own business partners. Large

multinational companies, such as those responsible for the production of an overwhelming share of export-controlled goods, have access to a distribution network consisting of partners that do not violate sanctions and/or fail to implement compliance procedures. This also means that they do not have to trade with intermediaries whose ownerships and/or business practices are not fully known to them and where risks of abuse exist. Holding business partners accountable for their actions would ensure that good-faith participants throughout the supply and distribution chain conduct proper due diligence.

### *3.2.2 Creating incentives for due diligence and building institutional capacities*

As far as non-financial companies are concerned, 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 – eg 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. For banks, the outcome has clearly become increased compliance efforts, as many institutions have faced substantial monetary penalties in recent years and law enforcement and supervision have become stricter. But the situation is different for non-financial companies as export controls enforcement has a much less-extensive track record and governments have significantly less experience with it. 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 that will introduce criminal offences and penalties for the violation of EU sanctions, including in the trading of sanctioned goods and conducting transactions with states or entities under EU sanctions, as well as providing financial services or performing financial activities, which are prohibited or restricted. Importantly, inciting, aiding and abetting these offenses will also be punishable as a crime and legal persons (eg companies) can be held liable for offences committed by certain individuals within the organisation[35].

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[36]. All coalition jurisdictions should align their laws to ensure that sanctions violations constitute crimes when committed with serious negligence, ie enforcement agencies can penalise or prosecute legal or natural persons who violate sanctions if they knew or *should have known* that their actions could result in such an outcome. The EU, in its twelfth sanctions package, established a legal requirement for companies to include *"no*

[35] See the European Council press release of 12 December 2023, 'Council and Parliament reach political agreement to criminalize 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).

[36] The aforementioned agreement's language on this topic might not go far enough as trade with war material would only constitute a criminal offense when committed intentionally or with *serious* negligence. The European Parliament has been pushing for stricter provisions that do not require *serious* negligence.

*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 and, if properly implemented, can also have a significant deterrent effect on non-EU entities[37]. Many coalition countries have issued guidance to the private sector on trade in export-controlled goods, including the United States[38] – 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 US, 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 when it comes to trade activities that physically take place outside of their jurisdictions and, thus, do not involve those agencies that often have the necessary personnel and resources: customs services. The UK recently announced the establishment of a new entity for trade sanctions implementation: OTSI[39]. The EU should follow suit and create unified enforcement structures as soon as possible.

### *3.2.3 Enabling non-financial companies to conduct proper due diligence*

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.

On a related note, the improvements to AML/CFT frameworks discussed above will be as important for non-financial companies' efforts as for those of banks, if regulations are aligned for the two types of entities. 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. While the ECJ judgement discussed in Annex 1 appears to provide access to EU registries to financial institutions with AML obligations – and should, therefore,

---

[37] 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).

[38] 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).

[39] 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).

also apply to non-banks falling under similar legal requirements – it will be critical to establish clear procedures to ensure that information can be acquired in a timely manner by any party conducting business that may result in their export-controlled products reaching a sanctioned jurisdiction or entity.

**4 Conclusions: towards effective and credible export controls**

Russia-related 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 and address the challenges that allow Russia to continue to import critical inputs for its military industry. 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. Outside it, 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. These are priorities to make export controls work more effectively.

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. While this topic is outside the scope of our paper, it is very important that strong diplomatic efforts are directed towards countries including Turkey, Armenia, Georgia and countries in central Asia, to support Western-led efforts and help trace illicit exports of dual-use goods.

Better enforcement is undoubtedly going to be burdensome on both public authorities and companies. Obviously, 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. We argue that it is still on the whole

very much advisable to step up enforcement efforts. First, Russia's war effort critically depends on technology access, and Ukrainian and broader European security is at stake. While 40 percent 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 percent. 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, which are needed to defend Ukrainians against missiles and drones that Russia is able to produce at increasing rates due to insufficient export controls enforcement.

**References**


Bilousova, O., B. Hilgenstock, E. Ribakova, N. Shapoval, A. Vlaysuk and V. Vlasiuk (2024) *Challenges of Export Controls Enforcement: How Russia Continues to Import Components for Its Military Production*, KSE Institute, available at https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf

Chupilkin, M., B. Javorcik, A. Peeva and A. Plekhanov (2024) *Decision to leave: Economic sanctions and intermediated trade*, European Bank for Reconstruction and Development, forthcoming

Fraiha Granjo, A. and M. Martini (2021) *Access denied? Availability and accessibility of beneficial ownership data in the European Union*, Transparency International, available at https://images.transparencycdn.org/images/2021-Report-Access-denied-Availability-and-accessibility-of-beneficial-ownership-data-in-the-European-Union.pdf

Heathershaw, J., A. Cooley, T. Mayne, C. Michel, T. Prelec … R. Soares de Oliveira (2021) 'The UK's kleptocracy problem: How servicing post-Soviet elites weakens the rule of law', *Research Paper*, Chatham House, available at https://www.chathamhouse.org/2021/12/uks-kleptocracy-problem

Hilgenstock, B., E. Ribakova and G. Wolff (2023) 'Toughening Financial Sanctions on Russia: Enforcing Energy Sanctions and Reducing Shadow Reserves Effectively', *DGAP Policy Brief* 10, German Council Foreign Relations, available at https://dgap.org/en/research/publications/toughening-financial-sanctions-russia

Rácz, A., O. Spillner and G. Wolff (2023) 'Russia's War Economy', *DGAP Policy Brief* 3, German Council Foreign Relations

**Annex 1: AML/CFT regulations in major jurisdictions and main weaknesses**

European Union: Between 1991 and 2021, the European Union published six anti-money laundering and terrorist financing directives, which aim to improve the transparency of transactions[40]. The most-relevant provisions include requirements for EU countries to create registries to trace the ownership of companies and certain assets. Specifically, the fourth EU AML directive, which entered into force in 2015, requires EU countries to establish publicly-available registers of the beneficial ownership of companies and other entities such as trusts located in their jurisdictions – known as transparency registers – by January 2020. In 2021, the European Commission set up the Beneficial Ownership Registers Interconnection System to link the national registers through a joint interface[41]. EU AML directives also require member states to set up similar systems for ownership or control of bank accounts and safe deposit boxes, as well as ownership of real estate.

While the institutional and regulatory setup can be leveraged to improve export controls enforcement as described, it is important to also outline some of the shortcomings that allow for AML/CFT offenses and sanctions circumvention. First, transparency registers are still not fully operational in all EU countries[42]. There are serious doubts about access to the information by companies with AML obligations because of a 2022 decision by the EU Court of Justice (ECJ) which ruled that such access would constitute a violation of privacy and personal data protection under the EU Charter of Fundamental Rights[43]. If necessary, legislative amendments will be required to reconcile data-privacy concerns with the need to prevent money laundering and circumvention of export restrictions. Furthermore, transparency registers only cover beneficial ownership amounting to at least 25 percent of shareholding. Clearly, there are mechanisms to dilute shareholding and formally remain under the 25 percent threshold, while retaining factual ownership of the entity in question. Here, stricter monitoring systems might be needed to detect such dilution. Moreover, it is not clear to what extent

[40] See Directive 91/308/EEC of 10 June 1991: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31991L0308 (accessed 12 April 2024). See Directive 2001/97/EC of 4 December 2001: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0097 (accessed 12 April 2024). See Directive 2005/60/EC of 26 October 2005: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0060 (accessed 12 April 2024). See Directive (EU) 2015/849 of 20 May 2015: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849 (accessed 12 April 2024). See Directive (EU) 2018/843 of 30 May 2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843 (accessed 12 April 2024). See Directive (EU) 2018/1673 of 23 October 2018: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1673 (accessed 12 April 2024).

[41] See Commission Implementing Regulation (EU) 2021/369 of 1 March 2021: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0369 (accessed 12 April 2024).

[42] In May 2021, a study by Transparency International found that one year after the deadline, nine countries had failed to establish public registers while others imposed geographic access restrictions in breach of EU AML directives (Fraiha Granjo and Martini, 2021).

[43] See ECJ Judgement Joined Cases C-37/20 and C-601/20: https://curia.europa.eu/juris/document/document.jsf?docid=268059&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=9481 (accessed 12 April 2024). As a result of the ruling, several European countries immediately closed public access to their registries, including Austria, Germany, Ireland, Luxembourg, and the Netherlands. Importantly, the ECJ stated that journalists and civil society organizations that investigate or campaign on crude and corruption, as well as financial institutions with AML obligations had a legitimate interest in access to the registrations. However, we believe that the ruling weakens the EU's stance on AML and sanctions enforcement. It is not clear how an evaluation of legitimate interest will take place in practice and whether ordinary business parties who may transact with entities from sanctioned jurisdictions will be able to access the registries.

national authorities verify the accuracy and completeness of information submitted, or how often it is updated, requiring also probably an upgrade in public-sector monitoring.

In addition, there are loopholes regarding the recording of companies active in the EU but domiciled elsewhere. While in the US, disclosure for all companies active in the US is obligatory, EU requirements only apply to entities that are incorporated in a member state. Similarly, in the trust register, member states need to record trusts from third countries but only if they have bought real estate or started a new business activity in the EU since March 2020, and the real estate registry only covers legal rather than beneficial ownership and there is currently no unified registry or proposal to establish one. Finally, member states' bank-account registries do not record other financial assets such as securities or crypto currency, and no interconnection on the EU level has been implemented. Stricter requirements on the recording of companies active in the EU appears necessary and warranted – not only as regards export controls but also when it comes to geoeconomic risks from third countries.

Recognising these weaknesses, the European Commission, in 2021, presented a new package of proposals to harmonize AML/CFT rules across the union with a focus on better information exchange, and to establish a new EU authority to address money laundering[44]. In light of enforcement challenges related to Russia sanctions, it is critical that these proposals are advanced quickly. In particular, beneficial ownership registries play an indispensable practical role in the enforcement of sanctions[45].

United States: On 1 January 2021, the US Congress passed the Corporate Transparency Act (CTA), part of the Anti-Money Laundering Act of 2020, which stipulates reporting requirements on the beneficial owners of most entities that are incorporated and/or operating within the United States. This legislation supplements previously existing requirements to file ownership-disclosure forms. Beneficial ownership reports are to be submitted to the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), and FinCEN started to accept beneficial ownership reports on 1 January 2024. In September 2022, FinCEN issues a final rule on the implementation of the CTA's beneficial ownership reporting requirements, specifying the entities that fall under the mandate[46]. The US also stipulates several other reporting requirements applicable to financial institutions and other entities[47]. The ownership threshold for the reporting requirement is the same as in the EU (and UK): 25 percent. On 21 December 2023, FinCEN issued its final Access Rule, whereby financial institutions can

[44] See the European Parliament Briefing: EU Legislation in Progress of 20 March 2024, 'Anti-money-laundering authority (AMLA): Countering money laundering and the financing of terrorism', https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733645 (accessed 12 April 2024).
[45] Notably, the Russian Elites, Proxies, and Oligarchs (REPO) Task Force, established by the governments of Australia, Canada, France, Germany, Italy, the United Kingdom, and the United States, as well as the European Commission in March 2022, emphasized that it relied on beneficial ownership registers to identify sanctioned individuals who are beneficiaries of shell companies. See the European Commission press release of 29 June 2022, 'Russian Elites, Proxies, and Oligarchs Task Force Joint Statement', https://ec.europa.eu/commission/presscorner/detail/en/statement_22_4232 (accessed 12 April 2024).
[46] See FinCEN final rule of 30 September 2023, 'Beneficial Ownership Information Reporting Requirements', https://www.federalregister.gov/documents/2022/09/30/2022-21020/beneficial-ownership-information-reporting-requirements (accessed 12 April 2024).
[47] Including Suspicious Activity Reports (SAR), Currency Transaction Reports (CTR), Reports of Cash Payments Over $10,000 Received in a Trade or Business, Reports of Foreign Bank and Financial Accounts (FBAR), Report of International Transportation of Currency of Monetary Instruments (CMIR), Registrations of Money Service Business (RMSB), and Designations of Exempt Persons (DOEP).

request beneficial ownership information with the customer's permission in order to implement FinCEN's 2016 customer due-diligence rule and to comply with *"any legal requirement or prohibition designed to counter money laundering or the financing of terrorism, or to safeguard the national security of the United States, to comply with which it is reasonably necessary for a financial institution to obtain or verify beneficial ownership information of a legal entity customer"*[48].

United Kingdom: The most pressing issue in the UK context is corporate transparency – or rather the lack of it – in British Overseas Territories and Crown Dependencies. The UK has had several bilateral agreements with these jurisdictions on the sharing of beneficial ownership information since 2017. In addition, the Sanctions and Anti Money-Laundering Act 2018 required public registers to be established in Overseas Territories by 31 December 2020, but the deadline was later postponed to the end of 2023. Similarly, Crown Dependencies were to launch such registers at the same time. This, however, did not fully materialise[49]. For the time being, beneficial ownership information from British Overseas Territories and Crown Dependencies is only available to UK government agencies and by request, for which law enforcement relies on the bilateral Exchange of Notes[50, 51]. The government has planned since 2017 to launch a public beneficial ownership registry for UK property. In March 2022, in

[48] See FinCEN final rule of 22 December 2023, 'Beneficial Ownership Information Access and Safeguards', https://www.federalregister.gov/documents/2023/12/22/2023-27973/beneficial-ownership-information-access-and-safeguards (accessed 12 April 2024).

[49] On December 13, 2023, the governments of Guernsey, the Isle of Man and Jersey issued a joint statement whereby they withdrew the commitment to provide public access to beneficial ownership registers, justifying this decision by pointing to the 2022 ECJ ruling. See the 'Joint commitment by Guernsey, the Isle of Man and Jersey: Registers of beneficial ownership of companies' of 13 December 2023: https://www.gov.je/News/2023/pages/jointcommitmentbyguernseytheisleofmanandjerseyregistersofbeneficialownershipofcompanies.aspx (accessed 12 April 2024). At the same time, the Crown Dependencies stated their plans to open access to the registries for financial services business and certain other businesses who are required to conduct customer due diligence under AML/CFT/CPF regime by the end of 2024. According to a U.K. Parliament Report on the issue, published on December 4, 2023, the negotiations with British Overseas Territories were still ongoing. See the House of Commons Research Briefing of 4 December 2023, 'Public registers of beneficial ownership in the Overseas Territories and Crown Dependencies', https://commonslibrary.parliament.uk/research-briefings/cdp-2023-0220/ (accessed 12 April 2024). However, on December 8, 2023, the Government of the British Virgin Islands issued a statement attesting its intent to abide by the 2022 ECJ decision, even though *"the Virgin Islands does not fall within the ambit of the ECJ"*. See the Government of the Virgin Islands press release of 8 December 2023, 'Government of Virgin Islands Position on Publicly Accessible Registers of Beneficial Ownership', https://bvi.gov.vg/media-centre/government-virgin-islands-position-publicly-accessible-registers-beneficial-ownership (accessed 12 April 204). Further, according to the statement, "the Virgin Island will continue technical work and cooperation with partners to launch publicly available registers but will balance this commitment with human rights concerns. Presently, Gibraltar is the only Territory or Dependency that has publicly available register.

[50] Exchange of Notes (EON) for Information Sharing is an arrangement between the United Kingdom and Crown Dependencies as well as six Overseas Territories with significant financial services sectors (Anguilla, Bermuda, British Virgin Islands, Cayman Islands, Gibraltar, and Turks and Caicos Islands), whereby the latter provide U.K. law enforcement agencies with company beneficial ownership information upon request.

[51] According to the Home Office's 2019 review of the Exchange of Notes scheme, law enforcement agencies had found the agreement *"extremely useful;"* however, it was *"too soon to quantify the full outcome in terms of successful investigations."* See the Home Office's 'Statutory review of the implementation of the exchange of notes on beneficial ownership between the United Kingdom, Crown Dependencies and Overseas Territories' of 27 June 2019, https://www.gov.uk/government/publications/statutory-review-of-the-exchange-of-notes-arrangements/statutory-review-of-the-implementation-of-the-exchange-of-notes-on-beneficial-ownership-between-the-united-kingdom-crown-dependencies-and-overseas-te (accessed 12 April 2024).

response to Russia's full-scale invasion of Ukraine, it also introduced legislation establishing a register of overseas entities owning UK property, and the register was activated in August 2022.

Another important element of the UK's AML regime is Unexplained Wealth Orders (UWOs), which were introduced by the Criminal Finances Act 2017. UWOs can be used to demand information from an individual, trust or company on legal ownership and the source of funds used to obtain assets. The purpose of UWOs is to enable UK authorities to examine the financial activities of those whose assets appear to exceed what could be acquired from their legitimate incomes. Importantly, the burden of proof in UWO proceedings is on the defendant. UWOs do not automatically trigger asset forfeiture but enable investigations into suspicious assets even if no obvious violation has been committed within the jurisdiction of UK law-enforcement agencies. Furthermore, Account Freezing Orders (AFOs) allow such bodies to freeze bank accounts if they can demonstrate reasonable grounds to suspect that money in an account has been obtained through unlawful conduct or is intended for unlawful use[52].

[52] AFOs have led to several successful forfeitures of funds held by relatives or nominees of sanctioned individuals or politically exposed persons (PEPs), including the niece of Syrian president Bashar al-Assad and the son of a former Moldovan prime minister (Heathershaw *et al*, 2021).


Bruegel, Rue de la Charité 33, B-1210 Brussels
(+32) 2 227 4210
info@bruegel.org
**www.bruegel.org**