EU TECHNOLOGY-TRADE SANCTIONS ON RUSSIA

Obstacles to Enforcement and Future Enforcement Strategies

B4Ukraine

EXECUTIVE SUMMARY

- **Enforcement of European technology-trade sanctions on Russia is seriously underpowered.**

There have been over 2000 sanctions investigations reportedly announced by civil and criminal enforcement agencies in the European Union (EU), UK and Switzerland since the full-scale invasion of Ukraine in February 2022, but only a handful of successful prosecutions in each country. Across Europe as a whole, recent journalistic analysis found that there have only been 8 custodial sentences for Russia-related sanction crimes since 2022. In German states where figures are available, over two-thirds of cases have already been closed without any action. In the UK, which by April 2024 had launched over 250 investigations of sanctions violations (of all kinds), there have been just six fines for Russian trade sanctions violations – five of them for an average of just £73,000 (EUR 88,000) – and no criminal prosecutions at all.

- **Aspects of EU sanctions and export control law itself are challenges to enforcement of technology trade sanctions.**

While limited investigative and prosecutorial resources and capacity may be contributing to low levels of enforcement, discussions and public statements from investigators and prosecutors indicate obstacles in EU sanctions and export control law itself: particularly very high thresholds and requirements of knowledge to trigger export licensing requirements in some cases, and liability for violations of export controls in others. In the EU, knowledge thresholds are higher, and due-diligence requirements much lower, than in other allied jurisdictions, particularly the USA. In Switzerland, a key 'catch-all' which provides a knowledge-based backstop to prevent unlisted goods being exported for weapons production in embargoed destinations like Russia, does not exist in Swiss dual-use export controls at all.

- **EU exporters can and have avoided knowledge of the military end-use of their sensitive exports to Russia.** This report outlines anonymized cases investigated via open sources in which EU exporters:

  - Have shipped export-controlled machinery to third-party intermediaries in Turkey listed as non-controlled goods categories on export documentation, which were then shipped on – under controlled goods categories – to a company in Russia which is fully owned by the original EU exporter.
  - Have supplied satellite antennae and positioning modules to a Russian electronics distributor with which the EU exporter has collaborated for two decades, and with which it previously co-owned a Russian company. Despite the EU exporter being informed in 2019 that its products, exported to this Russian distributor for ostensible civilian use, had been recovered on multiple occasions from Russian military UAVs downed in Ukraine and during EU airspace incursions, the EU exporter continued to ship products to the Russian distributor for another two years.

- Have continued to supply specialized navigation components to a Russian distributor after it provided the EU exporter with lists of end-users that included Russia's leading producer of armed medium-range UAVs.

- Have supplied CNC machine tools to a leading procurer of machine tools for Russian military industry from after the imposition of an EU arms embargo in 2014 until July 2022 – despite that Russian partner company only contracting in publicly available procurement records to supply the EU exporter's machine tools to EU-sanctioned Russian weapons producers.

Though these activities may have involved unlawful acts, and merit further investigation, legal reviews suggest that in many cases these and other EU exporters could have avoided triggering knowledge-based reporting or licensing obligations under EU law – despite public information being readily available about their Russian customers' military procurement activity, and decades of close collaboration or even co-ownership with these Russian customers.

- **Three legislative changes to the EU's core technology trade control laws, and their counterparts in UK and Swiss law, could bring such activities within the scope of export controls and generate prosecutable liability for sanctions violations:**

- Exporter knowledge: Reduce the knowledge threshold that triggers export licensing requirements in the military end-use catch-all clause for embargoed destinations (Article 4 of Regulation 821/2021), from "is aware…are intended, in their entirety or part" to "is aware, or has reasonable cause to suspect…may be intended, in their entirety or part."

- Due-diligence: Introduce mandatory due-diligence requirements on exporters of all goods listed in the EU Dual-Use List, Annex VII of Regulation 833/2021 and Annex XXIII of Regulation 833/2021. Harmonise these due-diligence requirements with those in Supplement No. 3 to Part 732 of the US Export Administration Regulations, to include a list of key documentation/information that all exporters must obtain from customers, and a list of red-flag checks that exporters must check. As with the US Export Administration Regulations, inability to 'clear' these red-flag checks should trigger a notification/licensing requirement to Member State export licensing authorities.

- Trade control coverage of key sectors: Also apply these mandatory due-diligence requirements to exporters of all goods in certain key sectors useful for military production, including machine tools and related components and consumables of all kinds, so that suspicious transactions in these sectors trigger the notification/export licensing requirements in the EU's military-end-use catch-all clause.

- As shown by the examples in this paper, these three changes would bring EU technology trade controls in line with countries outside the EU. Nor are they entirely new within the EU: versions of them were proposed by the European Commission in 2016. With EU exports to Russian military industry now a key European security threat, it is past time to revisit these reforms.

INTRODUCTION: MANY INVESTIGATIONS, FEW PROSECUTIONS

The European Union's military-technology trade ('tech-trade') sanctions on Russia cover an unprecedented scope of goods and technology. They have introduced innovative sanctions design techniques: from the use of harmonized customs codes in place of technical definitions of controlled goods;[1] to expanded and elaborated definitions of sanctions circumvention.[2]

Criminal or even administrative enforcement, by contrast, remains comparatively rare. Since 2022 prosecutors have initiated large numbers of investigations with relatively few prosecutions, either attempted or successful. According to a law firm which tracks sanctions enforcement activity, across the EU, UK and Switzerland over 2000 sanctions investigations (of all kinds and for all destinations) had been publicly announced as of April 2024, including nearly 750 in Finland.[3] This is almost certainly a significant underestimate, given the large number of investigations that are never announced. In Germany – the source of a significant proportion of the European-made machine tools and other sanctioned industrial goods that Russian customs data has shown is being supplied to Russia's military industry and wider economy[4] – journalists' state-level information requests revealed over 1,400 investigations by regional prosecutors for potential violations of Russia or Belarus sanctions (of all kinds) as of July 2024: including 406 investigations in Hesse state alone (whose capital, Frankfurt, is a major European air and road logistics hub).[5] The vast majority of these investigations, however, had already been closed without action: though comprehensive figures are not available, state-level figures are illustrative, with Mainz (Rhineland-Palatinate) prosecutors, for example, closing 50 of their 79 cases, and those in Stuttgart (Baden-Württemberg) closing 44 out of 52 cases.[6]

In the UK, which shares much of its trade sanctions law with the European Union, there had reportedly been over 250 investigations of sanctions violations (of all kinds) by April 2024.[7] Yet as of November 2024 UK authorities have issued just six fines for Russian trade sanctions violations since February 2022 – five of them for an average of just £73,000 (EUR 88,000)[8] – and have undertaken no criminal prosecutions at all.[9]

A recent journalistic analysis by Investigate Europe identified just 11 custodial sentences for Russia-related sanctions crimes since 2017, eight of which had been imposed since 2022.[10]

Lack of resources or gaps in the law?

Standing outside these necessarily confidential investigations, the reasons for their large-scale discontinuation or failure are not always clear. Resources and capacity may certainly have played a part. Trade sanctions are often the poor cousin to financial sanctions: in most countries they lack dedicated national intelligence-gathering or enforcement bodies, relying instead on existing investigation units within customs authorities or export control units, which may not have the experience or resources to enforce sanctions circumvention taking place outside their territorial jurisdiction, via third countries or intermediaries.

Germany, for example, established a new federal sanctions enforcement body in January 2023, the Zentralstelle für Sanktionsdurchsetzung (ZfS), in response to the new sanctions on Russia: but the ZfS only has a mandate to investigate and enforce individual asset freezes, not trade sanctions.[11] The UK announced in December 2023 that in early 2024 it would set up a new Office of Trade Sanctions Implementation (OFTI) to coordinate civil enforcement of trade sanctions as a counterpart to the existing Office of Financial Sanctions Implementation (OFSI),[12] but the laws establishing OFTI's powers only came into force in October 2024,[13] and as of November 2024 the responsible minister could not give detailed answers to questions regarding the new body's staffing or budget.[14] Even in the US, where dual-use export controls have a dedicated enforcement unit within the Bureau of Industry and Security (BIS), a December 2024 Congressional investigation reported that due to budget constraints BIS' investigation unit has not upgraded its IT systems since 2006, conducts most of its analysis in data pasted into Microsoft Excel, and lacks the ability to search its own export licences or the full text of documents within its investigation database.[15] It has only 11 staff to conduct diversion end-use checks (although most countries lack powers and personnel to make such checks at all),[16] who in 2022 and 2023 conducted only five diversion end-use checks in Armenia, a country which BIS itself had in June 2022 publicly identified as a diversion hub; and none in Georgia, another such publicly-identified hub[17] – despite aggregated exports from the four largest US semiconductor companies to Armenia and Georgia having more than doubled from 2021 to 2022.[18]

Enforcement resource constraints are therefore significant, and ongoing. But while such constraints may explain a limited number of investigations, they cannot fully explain why such a high proportion of the investigations that do take place appear to be ultimately fruitless.

We cannot look inside the closed box of unsuccessful enforcement investigations. However, this paper draws upon two years of open-source investigations into EU natural and legal persons which since 2022 have supplied restricted products to sanctioned Russian military-industrial entities or their proximate Russian suppliers; leading to submissions to prosecutors and export control authorities in Germany, the UK, the USA and other European countries. These investigations generated sufficient initial evidence, according to independent legal reviews, to merit formal law enforcement investigation. The results of each investigation were reviewed by external lawyers specializing in sanctions and export controls in EU member states, Switzerland and the UK, to determine evidential sufficiency and gaps on the basis of sanctions legislation in each jurisdiction.

The experience of these investigations, their legal review, and their subsequent submission to enforcement authorities, suggests that three interlinked aspects common to Russia tech-trade sanctions legislation in the EU, UK and Switzerland may be hindering prosecutions, by making it difficult to prove that sanctions violators had the required levels of knowledge and intent. Informal discussion with prosecutors and law enforcement investigators, though anecdotal, appear to confirm these obstacles.[19]

In Germany, Stuttgart's public prosecutors stated this publicly in July 2024, explaining to journalists that a high number of investigations were fruitless because "the accused often lacked intent because they were **"under the misconception about the scope of the Russia embargo" or because in some cases only minor guilt can be established. A typical case is that an employee of a company illegally sells goods to Russia but does not derive any financial benefit from it. This means that there is no motive for the crime. In such cases, a company fine for organizational deficiencies could be considered."**[20]

Of course, mental elements of crimes are an important part of preventing unjust prosecutions of unwitting individuals. Open-source investigation, moreover, can never replicate the powers of prosecutorial or civil enforcement bodies to obtain non-public information and communications, which are usually necessary to meet legal/evidential requirements regarding knowledge and intent. Nonetheless legal reviews of the investigations detailed below have shown that some aspects of tech-trade sanctions legislation, even with its dramatic expansion since 2022, may make law enforcement evidence-gathering or prosecution difficult even where there is open-source evidence – as in several of our cases – of contact, cooperation, or even personnel or ownership links, between the EU exporter and sanctioned Russian importers or end-users. In these cases, therefore, EU exporters appear to have had ample opportunities to determine the prohibited end-uses or end-users of their products, were they required to do so. Gaps in EU law allowed them not to do so.

Crucially, the three legal obstacles discussed below – **the necessarily partial coverage of controlled goods lists, knowledge thresholds, and limited due-diligence requirements** – interact. As shown in the cases discussed below, this interaction makes it possible for EU exporters – unlike those in the USA – to actively avoid acquiring the knowledge necessary to be liable for violating sanctions even while continuing to supply strategically-significant goods to military-industrial suppliers and distributors in Russia.

Our investigations also indicate prosecutorial strategies that may help address these legal obstacles. Without legislative change, however, prosecutors will continue to be hampered. Crucially, these gaps are not new: from 2016 to 2021 the European Commission attempted to amend knowledge thresholds and due-diligence requirements in the EU's dual-use trade controls. These changes were resisted by coalitions of EU member states concerned about constraints to their technology export industries. In the new international security environment of the 2020s, with state military threats on Europe's borders, and the EU potentially unable to rely upon some traditional allies to counter such threats, these reform efforts deserve another chance.

THREE INTERLINKED LEGAL OBSTACLES

1. NECESSARILY INCOMPLETE LISTS OF CONTROLLED GOODS/TECHNOLOGY

The lists of goods prohibited for export to Russia are unlikely ever to cover all the kinds of products and materials used in Russian military production. First, the long-standing Dual-Use control list[21] has never been a comprehensive list of goods that could be used for either military or civilian production, as its name might suggest: it has always been intended as a highly specialized list of goods and materials whose legitimate trade merited the inevitable disruption of trade controls because of their specific utility in producing weapons of mass destruction and other advanced military technologies. To this specialized list, EU tech-trade sanctions on Russia have since February 2022 added two much broader lists of "goods and technology which might contribute to Russia's military and technological enhancement, or the development of the defence and security sector"[22] and "goods which could contribute in particular to the enhancement of Russian industrial capacities".[23]

These additional lists are wide, but are also unlikely to control all goods procured by Russia's military industry: both because many basic goods are used for all kinds of industrial production, including military production; and because both lists use customs category codes to define controlled goods, and many goods can fit into several different customs category codes, not all of are or can be included in the lists, in the absence of a comprehensive trade embargo. (The use of harmonised customs codes in export control lists is an innovation of the post-2022 Russia sanctions, and is useful for exporters; but customs codes are designed primarily for statistical analysis, not for export control, and do not define goods according to detailed technical definitions).

For instance:

In August 2022, an Italian manufacturer of 5-axis CNC machining centres exported machine tools parts and components directly to a Russian supplier to the aerospace and defence industry. This Russian supplier has had multiple contracts in Russia to supply European machine tools to state-owned producers of fighter jets, military electronics and naval navigation systems; and was itself listed in March 2022 on the EU's trade sanctions list (Annex IV of Regulation 833/2014). One of these shipments from Italy included goods categorised in shipping documentation under six customs codes, only one of which was then a customs code listed on EU sanctions lists (8466 92, a code covering parts and components for machine tools for working hard non-metallic materials).[24] Two of the codes used in the shipment were only listed on EU sanctions lists after this shipment took place (8537 10 and 8528 59).[25] Finally, two codes used in the shipment (8421 99 and 8418 69) have never been listed as goods prohibited for export to Russia. In practice, since they were all shipped together, it is likely that all the items in this shipment were parts or accessories of the same set of machine tools. Nonetheless the majority of the machine-tool parts in this shipment could, according to the exporter's own customs classification, be freely exported to a sanctioned supplier of machine tools to Russia's military industry.

Open-source investigations have uncovered cases where items' customs codes have changed during multi-stage shipments to Russia in ways which raise suspicions of manipulation to avoid declaring customs codes that appear on sanctions lists. For instance:

A leading international manufacturer of measurements systems for machine tools had, prior to the February 2022 full-scale invasion of Ukraine, sent numerous shipments of goods from its EU subsidiary to a subsidiary it owned in Russia, which was responsible for supplying its products to the Russian market. During 2022, these direct shipments to its Russian subsidiary ceased. In late March 2023, however, one of this manufacturer's EU subsidiaries made a large shipment of goods to an ostensibly unrelated machine tool broker in Turkey. The goods were declared on shipping documentation under generic customs codes for measuring instruments and software, not specific to machine tools. In early April 2023, the Turkish machine tool broker sent a similar shipment of goods to the international manufacturer's own subsidiary in Russia, listed as being manufactured by the international manufacturer which had shipped them to Turkey in March 2023, and now declared under customs codes specifically covering components for machine tools that had been included in the EU's trade sanctions on Russia on 17 December 2022.[26]

In the Italian case described above, however, the ability of the exporter to list items that are likely components for the same set of machine tools under a range of different customs codes, many not appearing on sanctions lists, may not necessarily be nefarious. It may simply be a function of the fact that any one item may legitimately be listed under several different customs codes: as components of a particular machine; as an item with functions covered by different customs codes (e.g. a pump, a computer, a control screen); as an item made of a particular material (e.g. cast articles of iron or steel); and so on.

It may also seem surprising that an EU exporter, as in this Italian case, could export goods of any kind to a Russian military-industrial company listed in EU trade sanctions and not violate those sanctions; but in fact the vast majority of Russian military-industrial companies listed in EU trade sanctions are only on a list of companies ('Annex IV' of Regulation 833/2014) with a relatively narrow sanctioning effect. For these companies, EU authorities must operate a presumption of denial if they receive applications for export licences of goods on the EU's (narrow) dual-use list where there are "reasonable grounds to believe" that the ultimate end-user is one of these listed 'Annex IV' companies.[27] The EU has recently begun to move some of these 'Annex IV' Russian military-industrial companies to a different sanctions list ('Annex I' of Regulation 269/2014), for entities to which EU persons may not make any 'economic resources available', which might include providing goods that those entities can subsequently use to generate funds or resources.[28] Nonetheless most Russian military-industrial companies placed on the EU's trade sanctions list since 2022 remain 'Annex IV' companies, and are the not in fact comprehensively sanctioned: they can still receive goods from EU exporters if those goods are not on the Dual-Use list, or other trade sanctions goods lists.

2. HIGH KNOWLEDGE THRESHOLDS IN CATCH-ALL CLAUSES

The malleability of customs codes and goods definitions – whether nefarious or not – and the absence of a comprehensive EU trade embargo on Russia, mean that tech-trade sanctions' control lists will never cover all the goods that might be used by Russia's military industry. This is almost inevitable in a system based on lists of goods and materials. Export controls have long recognized this problem, and many jurisdictions including the European Union therefore include 'catch-all clauses' in their export controls.

The main catch-all clause relevant to Russia's military technology trade is the 'military end-use' catch-all clause contained within the EU's Dual Use Regulation (821/2021). This requires exporters to apply for an export licence (presumably to be refused) for any ordinarily uncontrolled goods at all that the exporter knows or has been told by the competent government authorities is destined for incorporation into a military-list item (a weapons system) in an EU-embargoed country, including Russia; or for use with production equipment or unfinished goods for producing a military-list item in an EU-embargoed country.[29]

The catch-all clause, however, is substantially reliant upon exporters self-reporting. Not only is the likelihood of detection low if they do not, but an exporter only needs to notify the authorities and apply for a licence if they know with certainty that the item is destined for such an end-use in Russia. It is not enough that the exporters suspect a possible Russian military production end-use, or that their shipment meets diversion red flags; the licensing requirement only applies if the exporter **"is aware"** that the goods **"are intended"** for such end-use.[30] This is a significantly higher threshold than comparable catch-all provisions in US export control law (Table 1). In 2021 the EU introduced a provision for member states on a unilateral basis to lower this threshold to **"grounds for suspecting"**,[31] but research for this note has not been able to identify any EU member state which has so far adopted this lower threshold.

The other Russia-specific tech-trade control lists incorporate no such catch-all clause. Exporters of listed goods themselves – whether goods on the Dual-Use list or the other Russia-specific lists – have no liability under EU law if **"they did not know, and had no reasonable cause to suspect, that their actions would infringe the measures set out in this Regulation."**[32] Efforts to circumvent EU tech-trade sanctions, meanwhile, are only an offence if the exporter has both knowledge and intention that their efforts will circumvent the sanctions, though in June 2024 the European Commission explicitly added to the legislation the standard established in jurisprudence of the European Court of Justice that this threshold encompasses **"participating in [circumvention] activities without deliberately seeking that object or effect but being aware that the participation may have that object or effect and accepting that possibility".**[33]

Table 1: Knowledge/intention thresholds for Russia tech-trade sanctions violations in EU and USA

Activity	Knowledge/intention threshold (EU)	Knowledge/intention threshold (USA)
Export of listed prohibited goods to Russia, directly or indirectly	**"know"** or have **"reasonable cause to suspect**, that their actions would infringe the measures set out in this Regulation"[34]	"You may not sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR and exported, reexported, or transferred (in-country) or to be exported, reexported, or transferred (in-country) with knowledge that a violation of the Export Administration Regulations, the Export Control Reform Act of 2018, or any order, license, license exception, or other authorization issued thereunder has occurred, is about to occur, or is intended to occur in connection with the item." [Emphasis added][35] "Knowledge of a circumstance...includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also **an awareness of a high probability of its existence or future occurrence.** Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts".[36]

Table 1: Knowledge/intention thresholds for Russia tech-trade sanctions violations in EU and USA

Activity	Knowledge/intention threshold (EU)	Knowledge/intention threshold (USA)
Export of unlisted goods for military production end-use in Russia	"Where an exporter **is aware** that dual-use items which he proposes to export, not listed in Annex I, **are intended**, in their entirety or in part" for "a military end-use if the purchasing country or country of destination is subject to an arms embargo"[37]	"if, at the time of the export, reexport, or transfer (in-country), **you have "knowledge,"** as defined in § 772.1 of the EAR **that the item is intended, entirely or in part, for a 'military end use,'** as defined in paragraph (f) of this section, **in Belarus or Russia, or a Belarusian or Russian 'military end user'"**[38] "Knowledge of a circumstance...includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also **an awareness of a high probability of its existence or future occurrence.** Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts".[39]
Circumvention of Russia trade sanctions	"participate, **knowingly and intentionally**, in activities the object or effect of which is to circumvent prohibitions in this Regulation, including by participating in such activities **without deliberately seeking that object or effect but being aware that the participation may have that object or effect and accepting that possibility."**[40]	N/A (§ 736.2 covers all kinds of acts promoting the export, re-export or other transfer of a controlled good, direct and indirect)

Table 1 indicates that the knowledge threshold for triggering licence requirements for unlisted goods destined for military end-use – the backstop for all the EU's list-based tech-trade sanctions – is the highest of these three knowledge thresholds in EU law. EU exporters have exported critical items to Russian importers which have been destined for military production end-use, and have had extensive opportunities to discover such end-use, without ostensibly reaching the 'is aware' threshold:

A manufacturer in an EU member state – a subsidiary of a major US defence and aerospace manufacturer – manufactures a key navigation component used in guided weapons and UAVs. The component is not listed on the EU Dual Use list, and therefore does not ordinarily require a licence for export from the EU country in which the manufacturer is located.

Since at least 2016 (after the imposition of an EU arms embargo on Russia in 2014) this exporter's navigation component has been recovered from Russian military surveillance UAVs downed in occupied Donbas, and from a Russian military surveillance UAV shot down during an incursion into another EU member state.

Each component costs several hundred Euros, and is sufficiently specialised that the manufacturer receives periodic lists of end-users from the third-party distributors in other countries to which the manufacturer exports its products. In 2019, researchers provided evidence to the company that its products had been identified in Russian military surveillance UAVs downed in Ukraine. The manufacturer checked its records and determined that the item had been exported to a Russian electronics distributor in 2012 which had stated that it was procuring the items for use by other Russian companies in "educational" applications. Searches of publicly available databases would have indicated that this Russian electronics distributor was a longstanding contractor to the Russian Ministry of Defence, according to Russian public procurement records; and was sanctioned by the USA in 2016 for alleged involvement in state-backed cyber operations.

Regardless of the information it had received in 2019 about the ostensible diversion to military end-uses of its product by this Russian electronics distributor, the EU manufacturer continued to export dozens of the same navigation components to the same Russian electronics distributor during 2020 and 2021, according to shipment-level customs records. According to information provided by the manufacturer and subsequently published, the Russian electronics distributor continued during this time to receive lists of the intended end-users of these components in Russia. The lists included a Russian UAV manufacturer of both military and civilian UAVs, whose flagship product is Russia's first medium-altitude long-endurance armed UAV (I.e. Russia's equivalent of the US 'Predator' UAV). Though it is not known whether these armed UAVs also contain navigation components from the EU manufacturer, it is clear that the EU manufacturer either did not conduct basic internet searches which would have indicated that some of the end-users openly disclosed by its distributor were Russian military manufacturers, nor the US government's allegations underlying US sanctions on the manufacturer's direct Russian customer; or it disregarded

such information. Significantly, however, the information that the manufacturer received from the researchers in 2019, and could have obtained from basic internet searches about its customer and proposed end-users, did not constitute firm proof that subsequent exports to Russia were destined for incorporation into military items, however suggestive was (or would have been) the information that the manufacturer received (or could have obtained). The distributor was not sanctioned in the EU, was not sanctioned for providing products to weapons manufacturers, and provided lists of end-users which produced both military and civilian products. It is arguable that the EU manufacturer could therefore continue to export its products

– to a US-sanctioned electronics distributor in an EU-embargoed country (Russia)

– whose purchases had previously ended up in Russian military surveillance UAVs used in combat in Ukraine and in incursions into EU member state airspaces,

– and with disclosed end-users which included the leading Russian manufacturer of armed UAVs.

without necessarily reaching the knowledge threshold in the EU's Dual Use Regulation that would require it to apply for an export licence to its home government for exporting unlisted goods. It is not clear from existing jurisprudence whether it would have met the "reasonable cause to believe" test in post-2022 prohibitions on exporting listed goods to Russia.

Direct exports to Russia from the EU manufacturer continued until February 2022.

A similar pattern of diversion notification and absent due-diligence, evading knowledge thresholds in EU export control catch-alls, is evident in European exports to a different Russian electronics distributor of GLONASS-compatible satellite positioning modules. These modules, made by a Swiss manufacturer in Switzerland and East Asia, have been found by researchers and governments in Russian military surveillance UAVs since 2016; and, since 2022, in Russian/Iranian armed UAVs used in Ukraine, in military radio sets, and in the electronic warfare modules that enable Russian guided weapons systems like Iskander-series ballistic missiles to reach their targets.

The Swiss-made satellite positioning modules found in Russian military UAVs prior to 2022 were initially exported to a German electronics distributor which had itself helped to establish (and subsequently sold its stake in) a Russian electronics distributor which since 2011 has had at least thirty published supply contracts with state-owned Russian military manufacturers, and a military unit owned controlled by a Russian intelligence service, according to the Russian state register of federal entities. The German distributor in turn exported the Swiss-made modules to this Russian partner distributor (which it had previously co-owned).

In 2019, researchers informed both the Swiss manufacturer and the German distributor that the positioning modules exported to Russia for ostensibly civilian end-use had been recovered from Russian military UAVs downed in Ukraine and an EU member state. After receiving this information, the Swiss manufacturer continued to export its products to the Russian electronics distributor until February 2022: both directly, and via the German distributor.

At the time of these 2020-22 exports, these positioning modules were not listed on the EU or Swiss dual-use lists, according to legislation and reported statements by a Swiss export control official.

Since February 2022, the Russian distributor has continued to import these Swiss-made positioning modules from companies in China, Germany, Hong Kong, Hungary, Serbia, India, Turkey, Lithuania, Kyrgyzstan, Uzbekistan, Switzerland, the Republic of China (Taiwan) and the USA. The Swiss manufacturer has not publicly explained how and when its products were originally acquired by these companies, and has suggested that they are likely harvested from civilian products containing positioning electronics. At least one of these Swiss-made electronic modules, recovered from a Russian anti-jamming module contained within a Shahed-series UAV used in Ukraine in mid-2023, was manufactured in the 18th week of 2022 according to its markings, indicating a relatively rapid supply chain.

In this case, the German distributor's knowledge of past military end-use may not have reached the legal threshold of certain knowledge in EU law that future exports to the same Russian distributor would be for military end-use. The German distributor may not therefore have had any obligation to notify the German export control authority or to seek export licences for these exports: despite being informed in 2019 about the recovery from Russian military UAVs of products it had previously exported; and despite having a two-decade history of collaboration and previous company co-ownership with the Russian military-industry supplier to which it had exported these products.

This case also highlights an even larger gap in Swiss dual-use export controls and tech-trade controls. These are ostensibly harmonised with EU controls, with the Swiss Federal Council adopting successive changes to the EU Dual Use Regulation, and successive rounds of EU Russia sanctions.[41] However, the Swiss dual use export law has only adopted part of the EU's end-use catch-all clause, and does not include the 'Military End Use catch-all' for embargoed destinations. Instead, the Swiss dual-use catch-all clause is confined only to goods which the exporter knows, or has been told by a government authority, are destined for use in weapons of mass destruction.[42]

On 27 August 2014, the Swiss Federal Council introduced a new justification for denying export licences of dual-use goods to the Russian Federation (i.e. that they are destined in whole or in part for a military usage, or to a military end-user). However, this appears only to cover listed dual-use goods, so it is not a catch-all.[43]

Thus it appears that Swiss exporters may export un-listed dual-use items to the Russian Federation without any export licensing restrictions, even if they know that they are destined for incorporation into a military weapons system.

In 2019, researchers informed both the Swiss manufacturer and the German distributor that the positioning modules exported to Russia for ostensibly civilian end-use had been recovered from Russian military UAVs downed in Ukraine and an EU member state. After receiving this information, the Swiss manufacturer continued to export its products to the Russian electronics distributor until February 2022: both directly, and via the German distributor.

At the time of these 2020-22 exports, these positioning modules were not listed on the EU or Swiss dual-use lists, according to legislation and reported statements by a Swiss export control official.

Since February 2022, the Russian distributor has continued to import these Swiss-made positioning modules from companies in China, Germany, Hong Kong, Hungary, Serbia, India, Turkey, Lithuania, Kyrgyzstan, Uzbekistan, Switzerland, the Republic of China (Taiwan) and the USA. The Swiss manufacturer has not publicly explained how and when its products were originally acquired by these companies, and has suggested that they are likely harvested from civilian products containing positioning electronics. At least one of these Swiss-made electronic modules, recovered from a Russian anti-jamming module contained within a Shahed-series UAV used in Ukraine in mid-2023, was manufactured in the 18th week of 2022 according to its markings, indicating a relatively rapid supply chain.

In this case, the German distributor's knowledge of past military end-use may not have reached the legal threshold of certain knowledge in EU law that future exports to the same Russian distributor would be for military end-use. The German distributor may not therefore have had any obligation to notify the German export control authority or to seek export licences for these exports: despite being informed in 2019 about the recovery from Russian military UAVs of products it had previously exported; and despite having a two-decade history of collaboration and previous company co-ownership with the Russian military-industry supplier to which it had exported these products.

This case also highlights an even larger gap in Swiss dual-use export controls and tech-trade controls. These are ostensibly harmonised with EU controls, with the Swiss Federal Council adopting successive changes to the EU Dual Use Regulation, and successive rounds of EU Russia sanctions.[41] However, the Swiss dual use export law has only adopted part of the EU's end-use catch-all clause, and does not include the 'Military End Use catch-all' for embargoed destinations. Instead, the Swiss dual-use catch-all clause is confined only to goods which the exporter knows, or has been told by a government authority, are destined for use in weapons of mass destruction.[42]

On 27 August 2014, the Swiss Federal Council introduced a new justification for denying export licences of dual-use goods to the Russian Federation (i.e. that they are destined in whole or in part for a military usage, or to a military end-user). However, this appears only to cover listed dual-use goods, so it is not a catch-all.[43]

Thus it appears that Swiss exporters may export un-listed dual-use items to the Russian Federation without any export licensing restrictions, even if they know that they are destined for incorporation into a military weapons system.

3. ABSENT OR INADEQUATE DUE-DILIGENCE REQUIREMENTS

The Swiss/German case reflects another common pattern with Russian military industry's acquisition of European-exported technologies: many EU exporters have had an extensive history of commercial collaboration, joint marketing and even common ownership with their Russian distributors, which have then continued to acquire their products via third parties since February 2022. Such histories of close collaboration should have presented extensive opportunities for the EU exporters to discover their Russian distributors' involvement in supplying their products to Russian weapons producers, which was often visible in public records or otherwise not concealed. Yet as explained below, these EU exporters have had no legal obligations to take positive actions to determine potential military end-uses of their products.

A major Austrian CNC machine tool manufacturer sent numerous shipments of its products to a Russian machine tool distributor after the imposition of an EU arms embargo on Russian in 2014, and indeed until at least July 2022 (well after Russia's full-scale invasion of Ukraine in February 2022).

This Russian machine tool distributor has in turn had had multiple contracts to supply CNC machine tools and their components, manufactured by the Austrian manufacturer, to Russian state-owned weapons manufacturers. Its contracts have included at least one contract in to supply the Austrian manufacturer's CNC products to Russia's main battle tank manufacturer Uralvagonzavod, and at least three contracts to supply them to missile manufacturer Almaz-Antey. These contracts, which named the brand of the Austrian CNC machine tool manufacturer, were signed after the EU had sanctioned Uralvagonzavod and Almaz-Antey from receiving dual-use goods from the EU in 2014 and 2016 respectively. Shipment-level trade records indicate that each of these contracts coincided with the supply of matching machine tools from the Austrian manufacturer to the Russian distributor.

Since 2015 the Austrian machine tool manufacturer has co-owned a Russian company with the Russian distributor, which the distributor has stated on its website has prodcued machine tools at its 'Engineering Center' in Russia. The Russian distributor named the Austrian machine tool manufacturer as a 'strategic partner' on its pre-2022 website, and extensively advertised the Austrian manufacturer's products.

The Russian distributor, and another longstanding Russian purchaser of the Austrian manufacturer's machine tools, have continued since February 2022 to act as procurers for the Austrian company's products specifically. According to trade records, in August 2022, after the end of direct exports from the Austrian manufacturer, the Russian distributor imported from a Chinese entity a range of CNC machine tools and related components described in shipment records as having been originally manufactured by the Austrian manufacturer. It is not known whether these items came from independent traders within the second-hand CNC tools market, or were recent exports from Europe via intermediaries, knowing or unknowing.

Until December 2024, exporters of dual-use goods – whether listed or unlisted – had no due-diligence obligations under EU (or UK/Swiss) export control laws. They were not even required to google the names of prospective customers, let alone conduct meaningful due-diligence. This absence of due-diligence requirements might be explicable for exporters of goods on **control lists**, who would have to apply for an export licence in any case, and could thus rely upon export licensing authorities to conduct due-diligence and end-use assessment (using information required from the exporters). Exporters of unlisted goods, however – even those exporting goods to embargoed destinations like Russia which fell into categories known to be widely used to produce weapons systems, from navigational electronics to advanced CNC machine tools - could lawfully avoid acquiring the 'awareness of military end-use' that would require them to notify export control authorities and apply for export licences for **unlisted** dual-use goods. Exporters also had no legal obligation to act upon well-known red flags highlighted by export control authorities as indicating potential diversion to Russia or for military end-use (for example: unusually large purchases by previously unknown Russian-controlled intermediaries in 'transit hub' countries in Central and East Asia).[44]

In June 2024, the European Commission introduced a requirement from 26 December 2024 that exporters of a short subset of items (the 50 customs codes on the list of Common High Priority Items) should:

- "take appropriate steps, proportionately to their nature and size, to identify and assess the risks of exportation to Russia and exportation for use in Russia for such goods or technology, and ensure that those risk assessments are documented and kept up-to-date"; and
- "implement appropriate policies, controls and procedures, proportionately to their nature and size, to mitigate and manage effectively the risks of exportation to Russia and exportation for use in Russia for such goods or technology, whether those risks were identified at their level or at the level of the Member State or of the Union."[45]

(From 26 May 2025 these requirements are extended to goods falling under two other customs codes, for 'generating sets' and 'other switches', covering items found in Chinese and Iranian UAVs used in Ukraine).[46]

The European Commission has introduced guidance for the content of such "appropriate steps" and "appropriate policies, controls and procedures";[47] but (in contrast to US dual use controls) specific red-flags, searches and information requirements are not included in the EU legislation itself. Table 2 shows how general these EU due-diligence requirements are, in comparison to US dual-use export control laws.

The EU due-diligence requirements introduced in December 2024, moreover, apply only to exports of a short list of High Priority Items, not to exports of the much larger lists of specialized dual-use and industrial items found on the EU Dual-Use List, Annex VIII of Regulation 833/2014, and Annex XXIII of Regulation 833/2014; nor to other non-listed goods or materials widely used in military production.

Table 2: Due diligence requirements in EU and US dual-use export controls

	US	EU
Goods covered	All controlled exports with a 'knowledge' threshold (including exports of unlisted goods that may be intended for for military end-use in Russia and Belarus; other non-proliferation related 'catch-alls'; and transactions where a violation of the Export Administration Regulations may occur;	Common High Priority Items only (customs codes listed in Annex XL of Regulation 833/2014)
Legal obligations	Exporters must • look for evidence of a (non-exhaustive) list of 27 specific red flags for potential unlawful diversion;[48] If one of these red flags is identified, the exporter must • go beyond the information and representations their customer has provided, and establish the end-use, end-user, or ultimate country of destination of the items, including through obtaining specific documentation including specified forms completed by the ultimate consignee and purchasers;[49]	Exporters should • take appropriate steps, proportionately to their nature and size, to identify and assess the risks of exportation to Russia and exportation for use in Russia for such goods or technology, and ensure that those risk assessments are documented and kept up-to-date; • implement appropriate policies, controls and procedures, proportionately to their nature and size, to mitigate and manage effectively the risks of exportation to Russia and exportation for use in Russia for such goods or technology, whether those risks were identified at their

	• If red flags remain after this process, exporters must notify the US Bureau of Industry and Security, and apply for an export licence;[50] • Exporters are forbidden from 'self-blinding' i.e. instructing sales personnel not to enquire about or discuss specific information.[51]	• level or at the level of the Member State or of the Union.[52]

The European Commission, in its due-diligence guidance, has claimed that due-diligence obligations extend beyond Common High Priority List items. It has pointed to language in the preambular paragraphs ('recitals') to Regulation (EU) 2024/1739, implementing the EU's 14th Sanctions Package on Russia, to claim that exporters of all products whose exports might infringe the EU's trade sanctions on Russia have basic due-diligence obligations.[53] The preambular language in this Regulation states that:

"It is appropriate to clarify that the protection against liability that is granted to Union operators if they did not know, and had no reasonable cause to suspect, that their actions would infringe Union restrictive measures cannot be invoked where Union operators have failed to carry out appropriate due diligence. It is appropriate for publicly or readily available information to be duly taken into account when carrying out such due diligence. Therefore, for example, a Union operator cannot successfully invoke such protection when it is accused of breaching the relevant restrictive measures because it has failed to carry out simple checks or inspections."[54]

However, recitals/preambular paragraphs of Council Regulations are for interpretation, and are not themselves legally binding. Legal scholars have argued that the use of recitals in EU Regulations for normative statements of this kind do not have legal force, and indeed the fact that the accompanying body of legislation in the EU's 14th Sanctions Package (in which this recital appears) only introduces explicit due-diligence requirements for Common High Priority Items would suggest that this is the Council's intended limit of these due-diligence obligations.[55]

OLD PROBLEMS, NEW URGENCY

The sections above lay out three obstacles to generating criminal or administrative liability for EU exporters engaged in tech-trade with Russian military industry. These three obstacles are obviously interlinked: necessarily finite control lists require reliance on catch-all clauses; the EU's military end-use catch-all has a very high knowledge threshold; the absence of due-diligence requirements means that EU exporters can easily and actively avoid reaching this knowledge threshold.

Legislative options

These problems are not new challenges in EU export controls, or unique to post-2022 Russia tech-trade sanctions.

In 2016, the Commission introduced a proposal to revise the Dual Use Regulation.[56] The Commission proposed inter alia to:

- Apply EU controls on the brokering of dual-use goods to subsidiaries of EU companies in third countries;
- Impose an obligation for exporters to conduct "due-diligence" on customers in relation to the catch-all clauses, including the Military End Use catch-all clause.

A working paper to the Council Working Party on Dual Use Goods in January 2018 argued that due-diligence requirements should not be mandatory, and should only pertain to 'internal compliance programmes' required to take advantage of certain blanket 'global licences' for multiple uncontroversial end users and countries: "The administrative burden should be proportionate. Already today, ICPs, as appropriate, are in practice in place within the EU in the risk assessment process. Hence, there is no need for additional mandatory requirements but, if used, the term "due diligence" refers to (self-regulating) compliance measures in the form of organizational approaches provided by the companies, e.g. in the form of Internal Compliance Programs (ICPs)".[57]

The European Council negotiating mandate developed by the EU member states governments in 2019, in response to the Commission proposal, removed both of these proposals, but did propose an additional measure instead:

- That individual Member State governments could if they wished impose a lower knowledge threshold for the Military End-Use catch-all clause through national legislation, allowing it to apply if the exporter "has grounds for suspecting" that the goods are destined for military end-use in an embargoed destination.[58]

Though this provision remains in the final recast Dual-Use Regulation passed in 2021, research for this paper has been unable to identify EU member states that have yet introduced such a lower knowledge threshold through national legislation.

In addition, the new 2021 Dual-Use Regulation re-introduced the due-diligence obligation proposed by the Commission, but only for exports of a narrow category of cybersurveillance equipment and technologies.[59]

With new security threats to the Union and its neighbours, and Member States' post-2022 expansion of the Restrictive Measures toolbox, it may now be time to reconsider amendments to the EU's core technology trade control laws to make them fit for purpose. As shown by the examples above, at least three changes would ensure that EU exporters of goods destined for Russia's military industry do not avoid export controls, and cannot escape enforcement if they deliberately seek to avoid such controls:

1. Reduce the threshold that triggers export licensing requirements in the military end-use catch-all clause for embargoed destinations (Article 4 of Regulation 821/2021), from 'is aware…are intended, in their entirety or part" to **"is aware, or has reasonable cause to suspect…may be intended, in their entirety or part."**
2. Introduce mandatory due-diligence requirements on exporters of all goods listed in the EU Dual-Use List, Annex VII of Regulation 833/2021 and Annex XXIII of Regulation 833/2021. Harmonise these due-diligence requirements with those in Supplement No. 3 to Part 732 of the US Export Administration Regulations, to include a list of key documentation/information that all exporters must obtain from customers, and a list of red-flag checks that exporters must check. As with the US Export Administration Regulations, inability to 'clear' these red-flag checks should trigger a notification/licensing requirement to Member State export licensing authorities.
3. Also apply these mandatory due-diligence requirements to exporters of all goods in certain key sectors useful for military production, including machine tools and related components and consumables of all kinds, so that suspicious transactions in these sectors trigger the notification/export licensing requirements in the EU's military-end-use catch-all clause.

Enforcement strategies under existing controls

EU legislative change along US lines is not a panacea. Recent Congressional investigation of US enforcement of dual-use export controls indicates that although the US Bureau of Industry and Security has the legal authority to bring enforcement actions against exporters "knowingly" violating the Export Administration Regulations on the lower knowledge threshold of **"an awareness of a high probability of [the] existence or future occurrence"** of a violation (see Table 1 above), it has never yet done so.[60] Legislative change must be accompanied by reformed enforcement strategies to take advantage of new powers and thresholds.

Similarly, enforcement may be more effective under the constraints of existing EU law if it follows different strategies or priorities.

- Investigating 2014-22 export control violations by post-2022 exporters: The examples of Italian machine tool exporters and Swiss/German navigation component exporters indicate that EU exporters whose products have reached Russian military industry since 2022 via circuitous third-country supply chains, previously exported their products directly to Russian military industry or their known procurers between 2014 and 2022. During this period there was an EU arms embargo on Russia which made the 'military catch-all clause' operative, prohibited exports of listed dual-use goods to Russia where the items "are or may be intended, in their entirety or in part, for military use or for a military end-user", and prohibited exports of listed dual-use goods to a (short) list of major Russian arms

manufacturers such as OAO Almaz Antey or OAO NPO Bazalt: state-owned arms companies to which, as we have seen above, EU exporters' closely collaborating (or sometimes co-owned) Russian distributors directly contracted to supply EU products in some cases.[61]

- The comparative directness of these 2014-22 supplies to Russian military industry and their undisguised procurers, and the relative lack of caution of such trade with Russia, arguably makes it easier for prosecutors to prove exporter knowledge, which should have activated the licensing requirement and export prohibitions under the EU military catch-all clause or Article 2 and 2a of Regulation 833/2014.

- Prosecutions for 2014-22 export control violations, targeted at post-2022 exporters, may thus be an efficient way of stopping current export control violators or circumventers.

- This prosecutorial strategy was widely used by the US Department of Justice and its Kleptocapture taskforce prior to its 2025 disbandment.[62] A recent case in Germany, where a German machine-tool exporter was imprisoned for 7 years for pre-2022 efforts to supply machine tools to Russian weapons producers, shows that such a strategy can be successful in the EU also.[63]

- Discussions with EU lawyers and prosecutors suggests that some prosecutors are unwilling to examine pre-2022 offences, since they may detract from post-2022 targets. The case examples given in this report, and the prosecution examples above, show that this is a false dichotomy: many EU exporters implicated in large-scale or strategically significant post-2022 supplies have also been supplying goods to Russia during 2014-22.

ENDNOTES

[1] EU Regulation 833/2014 (as amended), Annex XXIII

[2] E.g. the expansion of sanctions circumvention due-diligence to non-EU companies controlled by EU persons (EU Regulation 2024/1745 of 24 June 2024, Article 1(22)); and the clarification that circumvention encompasses acts which have the effect of circumventing sanctions **"without deliberately seeking that object or effect but being aware that the participation may have that object or effect and accepting that possibility"** (EU Regulation 2024/1745 of 24 June 2024, Article 1(25)) – similar to the legal standard of dolus eventualis, and consistent with case law of the European Court of Justice, which ruled in 2011 that existing prohibitions in EU sanctions law of knowing and intentional sanctions circumvention **"covers activities which, under cover of a formal appearance which enables them to avoid the constituent elements of an infringement…none the less have the object or effect, direct or indirect, of frustrating the prohibition laid down in that provision; [and] the terms 'knowingly' and 'intentionally' imply cumulative requirements of knowledge and intent, which are met where the person participating in an activity having such an object or such an effect deliberately seeks that object or effect or is at least aware that his participation may have that object or that effect and he accepts that possibility."** (emphasis added; see judgement of 21 December 2011 in Case C-72/11, Afrasiabi et al, https://curia.europa.eu/juris/document/document.jsf;jsessionid=4071DB98246BECB444FC0E9A03BA6959?text=&docid=117186&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=254541)

[3] Duane Morris LLP, 'European Sanctions Enforcement – milestone of over 2000 announced and active investigations reached', 22 April 2024, https://blogs.duanemorris.com/europeansanctionsenforcement/2024/04/22/european-sanctions-enforcement-milestone-of-over-2000-announced-and-active-investigations-reached/

[4] SWR Research Unit, 'Deutsche Maschinen für Russlands Militär', 10 October 2024, https://www.tagesschau.de/investigativ/swr/embargo-russland-maschinen-100.html ; C4ADS, **War Machine: the networks supplying and sustaining the Russian precision machine tool arsenal** (18 June 2024), https://c4ads.org/reports/war-machine/ ; 'How Russia Imports Machinery for Arms Production and Can It Be Stopped', IStories, 17 April 2024, https://istories.media/en/stories/2024/04/17/machinery-for-arms-production-imports/

[5] SWR Research Unit, 'Russland-Sanktionen: Mehr als 1.400 Ermittlungsverfahren wegen mutmaßlicher Sanktionsverstöße - Bundesweite SWR-Umfrage bei Ministerien und Staatsanwaltschaften', 19 July 2024, https://www.daserste.de/information/politik-weltgeschehen/report-mainz/swr-recherche-unit/Russland-Sanktionen-104.html

[6] SWR Research Unit, 'Russland-Sanktionen: Mehr als 1.400 Ermittlungsverfahren wegen mutmaßlicher Sanktionsverstöße - Bundesweite SWR-Umfrage bei Ministerien und Staatsanwaltschaften', 19 July 2024, https://www.daserste.de/information/politik-weltgeschehen/report-mainz/swr-recherche-unit/Russland-Sanktionen-104.html

[7] Duane Morris LLP, 'European Sanctions Enforcement – milestone of over 2000 announced and active investigations reached', 22 April 2024, https://blogs.duanemorris.com/europeansanctionsenforcement/2024/04/22/european-sanctions-enforcement-milestone-of-over-2000-announced-and-active-investigations-reached/

[8] HM Revenue and Customs, **Notice to Exporters NTE 2024/29**, 4 November 2024, https://www.gov.uk/government/publications/notice-to-exporters-202429-compound-settlement-for-breaches-of-russian-sanctions-august-2024/4aaf2dcb-e79b-407c-bd7b-a2ea4c245c7f

[9] https://www.bbc.co.uk/news/articles/c39n4wdzdy4o

[10] Pascal Hansens, 'EU Dropping the Ball on Sanctions Enforcement', Investigate Europe, 27 February 2025, https://www.investigate-europe.eu/posts/eu-dropping-the-ball-on-sanctions-enforcement

[11] Sanktionsdurchsetzungsgesetz of 19 December 2022 (BGBl. I S. 2606), Section 2, https://www.gesetze-im-internet.de/sanktdg/BJNR260610022.html . Even the ZfS is relatively lightly resourced: as of May 2024, it had only 40 full-time employees (and two part-time employees), only 24 financial investigators, and at that time was working on 111 open investigations. See Federal Government response to parliamentary question 20/11063, 13 May 2024, https://dserver.bundestag.de/btd/20/112/2011258.pdf . This is actually a decrease from the number reported in July 2023, when there were 58 employees (of a planned total of 91), of which 47 were financial investigators. See Federal Government response to parliamentary question 20/7515, 13 July 2023, https://dserver.bundestag.de/btd/20/077/2007755.pdf

[12] Speech of Industry and Economic Security Minister Nusrat Ghani, 11 December 2024, https://www.gov.uk/government/speeches/office-of-trade-sanctions-implementation-announcement

[13] Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, entered into force on 10 October 2024, https://www.legislation.gov.uk/uksi/2024/948/regulation/1/made

[14] Minister of State, Department for Business and Trade, response to parliamentary question, 14013, 18 November 2024, https://questions-statements.parliament.uk/written-questions/detail/2024-11-13/14013

[15] US Congress Permanent Subcommittee on Investigations, **The US Technology Fuelling Russia's War in Ukraine: Examining the Bureau of Industry and Security's Enforcement of Semiconductor Export Controls**, Majority Staff Report, 18 December 2024, pp. 18-20, https://www.hsgac.senate.gov/wp-content/uploads/The-U.S.-Technology-Fueling-Russias-War-in-Ukraine-Examing-BISs-Enforcement-of-Semiconductor-Export-Controls.pdf

[16] US Congress Permanent Subcommittee on Investigations, **The US Technology Fuelling Russia's War in Ukraine: Examining the Bureau of Industry and Security's Enforcement of Semiconductor Export Controls**, Majority Staff Report, 18 December 2024, p.16 https://www.hsgac.senate.gov/wp-content/uploads/The-U.S.-Technology-Fueling-Russias-War-in-Ukraine-Examing-BISs-Enforcement-of-Semiconductor-Export-Controls.pdf

[17] FINCEN and BIS Joint Alert (FIN-2022-Alert003), 28 June 2022, p. 5, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf

[18] US Congress Permanent Subcommittee on Investigations, **The US Technology Fuelling Russia's War in Ukraine: Examining the Bureau of Industry and Security's Enforcement of Semiconductor Export Controls**, Majority Staff Report, 18 December 2024, p.16 https://www.hsgac.senate.gov/wp-content/uploads/The-U.S.-Technology-Fueling-Russias-War-in-Ukraine-Examing-BISs-Enforcement-of-Semiconductor-Export-Controls.pdf

[19] Though not described in detail in this briefing note, we draw upon informal discussions with sanctions policymakers, investigators and prosecutors from the EU Commission, EU Member States, the UK, Switzerland and EU neighbourhood states at a conference jointly convened by the European Commission and the United States in Brussels in April 2023; and subsequent discussions during 2023-24 with enforcement personnel engaged with tech-trade sanctions enforcement in the UK, southern and southeast Europe.

[20] SWR Research Unit, 'Russland-Sanktionen: Mehr als 1.400 Ermittlungsverfahren wegen mutmaßlicher Sanktionsverstöße - Bundesweite SWR-Umfrage bei Ministerien und Staatsanwaltschaften', 19 July 2024, https://www.daserste.de/information/politik-weltgeschehen/report-mainz/swr-recherche-unit/Russland-Sanktionen-104.html (N.B. This is mostly reported speech, and the journalist uses the word 'Tatmotiv' (criminal motive) whereas the legally relevant question is not the existence of a motive but the suspect's intent ('Vorsatz'). The original quote in German is: "den Beschuldigten häufig an Vorsatz fehle, weil sie sich „in einem Irrtum über die Reichweite des Russland-Embargos" befanden oder weil in manchen Fällen nur eine geringe Schuld feststellbar sei. Ein typischer Fall sei, dass ein Mitarbeiter einer Firma zwar rechtswidrig Ware nach Russland verkaufe, daraus aber keinen eigenen finanziellen Vorteil ziehe. Dadurch fehle ein Tatmotiv. In solchen Fällen könne eine Unternehmensgeldbuße wegen Organisationsmängel in Betracht kommen.")

[21] EU Regulation 821/2021 (as amended).

[22] EU Regulation 833/2014 (as amended), Article 2a and Annex VII.

[23] EU Regulation 833/2014 (as amended), Article 3k and Annex XXIII.

[24] Introduced into Annex XXIII of Regulation 833/2014 (as amended) by Regulation 2022/576 of 8 April 2022.

[25] Code 8537 10 introduced into Annex VII of Regulation 833/2014 (as amended) by Regulation 2023/427 of 25 February 2023; Code 8528 introduced in Annex XXIII of Regulation 833/2014 (as amended) by Regulation 2024/1745 of 24 June 2024, Annex V.

[26] Regulation 2022/2474 of 16 December 2022.

[27] Regulation 833/2014 (as amended) Article 2(7). Annex IV of Regulation 833/2014 contains the list of 'sanctioned' Russian military-industrial companies.

[28] Annex I of Regulation 269/2014 (as amended). For a discussion of whether providing goods or services (rather than funds) to 'Annex I' companies violates the prohibition on "making economic resources available" to them, see Commission Opinion of 19 June 2020 on Article 2 of Council Regulation (EU) No 269/2020 (https://finance.ec.europa.eu/document/download/320cea0c-2f2e-4337-827e-d55b1080dc05_en).

[29] Regulation 821/2021, Article 4.

[30] Regulation 821/2021, Article 4.

[31] Regulation 821/2021, Article 4(3).

[32] Regulation 833/2014 (as amended), Article 10. N.B. the UK High Court has recently ruled that the "reasonable cause to suspect" standard in parallel (transposed) UK legislation does not in fact apply on its own, in contrast to UK government guidance issued by the Financial Conduct Authority and OFSI, and that for a person to commit an offence they must not only have reasonable grounds to suspect, but also that the prohibited thing must indeed be true (i.e. an asset to be frozen must indeed be owned or controlled by a sanctioned entity, or the goods must indeed be destined to a prohibited destination or end-use, for the 'reasonable cause to suspect' test to apply): Vneshprombank LLC v. Bedzhamov et al (case No BL-2023-000277), High Court of Justice, Chancery Division, 3 May 2024.

[33] EU Regulation 2024/1745 of 24 June 2024, Article 1(25). In 2011 the ECJ ruled that prohibitions in EU sanctions law of knowing and intentional sanctions circumvention **"covers activities which, under cover of a formal appearance which enables them to avoid the constituent elements of an infringement...none the less have the object or effect, direct or indirect, of frustrating the prohibition laid down in that provision; [and] the terms 'knowingly' and 'intentionally' imply cumulative requirements of knowledge and intent, which are met where the person participating in an activity having such an object or such an effect deliberately seeks that object or effect or is at least aware that his participation may have that object or that effect and he accepts that possibility."** (Judgement of 21 December 2011 in Case C-72/11, Afrasiabi et al, https://curia.europa.eu/juris/document/document.jsf;jsessionid=4071DB98246BECB444FC0E9A03BA6959?text=&docid=117186&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=254541)

[34] Regulation 833/2014 (as amended), Article 10.

[35] Export Administration Regulations (US Code of Federal Regulations, Title 15, Subtitle B, Chapter VII, Subchapter C), as amended, § 736.2, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-736/section-736.2

[36] Export Administration Regulations (US Code of Federal Regulations, Title 15, Subtitle B, Chapter VII, Subchapter C), as amended, § 772.1, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-772/section-772.1

[37] Regulation 821/2021, Article 4.

[38] Export Administration Regulations (US Code of Federal Regulations, Title 15, Subtitle B, Chapter VII, Subchapter C), as amended, § 744.21, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/section-744.21

[39] Export Administration Regulations (US Code of Federal Regulations, Title 15, Subtitle B, Chapter VII, Subchapter C), as amended, § 772.1, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-772/section-772.1

[40] Regulation 833/2014, Article 12.

[41] E.g. Swiss Federal Council, 'Ukraine: Switzerland implements the EU's 13th package of sanctions', 1 March 2024, https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-100270.html ; Swiss Federal Council, 'Export controls: Federal Council to continue internationally harmonised control lists for dual-use goods', 13 December 2024, https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-103569.html

[42] Verordnung vom 25. Juni 1997 über die Aus-, Ein- und Durchfuhr zivil und militärisch verwendbarer Güter sowie besonderer militärischer Güter (Güterkontrollverordnung, GKV) (SE 946.202.1), Article 4, https://www.fedlex.admin.ch/eli/cc/1997/1704_1704_1704/de

[43] Verordnung über Massnahmen im Zusammenhang mit der Situation in der Ukraine (946.231.176.72, 22 April 2014, as amended on 27 August 2014, Article 1, https://www.fedlex.admin.ch/eli/cc/2014/486/de

[44] E.g. European Commission, **Guidance for EU Operators: implementing enhanced due-diligence to shield against Russia sanctions circumvention** (2023), https://finance.ec.europa.eu/document/download/3c86c9a8-f09e-4092-ab8c-a9e678df1494_en?filename=guidance-eu-operators-russia-sanctions-circumvention_en.pdf

[45] Regulation 833/2014 (as amended), Article 12gb; Regulation 2024/1745 of 24 June 2024, Article 1(28).

[46] Regulation 833/2014 (as amended), Article 12gb; Regulation 2025/395 of 24 February 2025, Article 1(34).

[47] European Commission, **Guidance for EU Operators: implementing enhanced due-diligence to shield against Russia sanctions circumvention** (2023), https://finance.ec.europa.eu/document/download/3c86c9a8-f09e-4092-ab8c-a9e678df1494_en?filename=guidance-eu-operators-russia-sanctions-circumvention_en.pdf; European Commission, **Circumvention and Due Diligence: Frequently Asked Questions as of 11 December 2024**, https://finance.ec.europa.eu/system/files/2023-06/faqs-sanctions-russia-circumvention-due-diligence_en.pdf

[48] Supplement No. 3 to Part 732 of Export Administration Regulations (BIS's "Know Your Customer" Guidance and Red Flags)

[49] Supplement No. 3 to Part 748 of Export Administration Regulations ('Statement by Ultimate Consignee and Purchaser Content Requirements)

[50] Supplement No. 3 to Part 732 of Export Administration Regulations (BIS's "Know Your Customer" Guidance and Red Flags)

[51] Supplement No. 3 to Part 732 of Export Administration Regulations (BIS's "Know Your Customer" Guidance and Red Flags)

[52] Regulation 833/2014 (as amended), Article 12gb; Regulation 2024/1745 of 24 June 2024, Article 1(28).

[53] European Commission, **Circumvention and Due Diligence: Frequently Asked Questions as of 11 December 2024**, p.5, https://finance.ec.europa.eu/system/files/2023-06/faqs-sanctions-russia-circumvention-due-diligence_en.pdf

[54] Regulation 2024/1739 of 24 June 2024, Recital 3.

[55] Maarten den Heijer, Teun van Os van den Abeelen, Antanina Maslyka, 'On the Use and Misuse of Recitals in European Union Law', Amsterdam Law School Research Paper No. 2019-31 (30 August 2019), https://ssrn.com/abstract=3445372

[56] Document 52016PC0616, **Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)**, COM/2016/0616 final - 2016/0295 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0616

[57] https://www.euractiv.com/wp-content/uploads/sites/2/2018/02/11_member_states_dual-use.pdf

[58] General Secretariat of the Council, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT ANDOF THE COUNCIL setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) – Mandate for negotiations with the European Parliament, 5 June 2019, https://www.consilium.europa.eu//media/39555/mandate-for-negociations.pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Dual-use+goods%3a+Council+agrees+negotiating+mandate

[59] Council Regulation (EU) 821/2021, Article 5.

[60] US Congress Permanent Subcommittee on Investigations, **The US Technology Fuelling Russia's War in Ukraine: Examining the Bureau of Industry and Security's Enforcement of Semiconductor Export Controls**, Majority Staff Report, 18 December 2024, p.23, https://www.hsgac.senate.gov/wp-content/uploads/The-U.S.-Technology-Fueling-Russias-War-in-Ukraine-Examing-BISs-Enforcement-of-Semiconductor-Export-Controls.pdf

[61] Regulation 833/2014 as amended by Regulation 960/2014 of 8 September 2014, Article 2, Article 2a, Annex IV.

[62] See e.g. USA v. Grinin et al (https://www.justice.gov/usao-edny/pr/five-russian-nationals-including-suspected-fsb-officer-and-two-us-nationals-charged); USA v. Ilya Khan (https://casetext.com/case/united-states-v-khan-192); USA v. Orekhov et al (https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money); USA v. Romanyuk et al (https://www.justice.gov/usao-ct/pr/ukrainian-national-pleads-guilty-money-laundering-charge-stemming-attempt-export-dual);

[63] https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2023/Pressemitteilung-vom-13-11-2023-02.html?nn=1650120 ; https://english.nv.ua/nation/german-businessman-sentenced-to-7-years-for-selling-machining-tools-to-russian-weapons-manufacturer-50464754.html

B4Ukraine

AUTHORS:

Mike Lewis, Director, Secta Research Ltd

b4ukraine.org