US Cos. Must Guard Against Russian Diversion Of Goods

By **Cate Baskin, Henry Morris and Deborah Curtis** (January 25, 2024)

Cate Baskin

Henry Morris

Deborah Curtis

Taking a page out of the history books on the military conflicts in Afghanistan and Iraq, U.S. law enforcement authorities have begun dismantling Russian weapons systems seized on the battlefield in Ukraine to launch criminal investigations into the provenance of U.S.-origin electronic components found inside.

In Iraq and Afghanistan, the weapon of choice was the improvised explosive device, or IED. More than a decade ago, after painstakingly dissecting IED ordnances and using serial numbers as evidence, the U.S. Department of Justice brought criminal charges[1] against numerous individuals and companies involved in the supply chain of U.S.-origin radio frequency technology critical to the operation of the IEDs.[2]

In today's global conflicts, the key technology is the microchip. And while the Russian military is officially denied U.S.-origin microelectronics — owing to stringent sanctions and export control measures — the battlefield in Ukraine has proven a verdant ground for advanced forensic examination, yielding evidence that U.S.-origin technology is still finding its way into Russian hands.

As a result, U.S. enforcement officials are on the hunt, and in late October and early November 2023, the DOJ arrested and charged multiple individuals with unlawfully acquiring, concealing and shipping export-controlled, dual-use technologies to the Russian military, including more than $7 million worth of semiconductors, integrated circuits and other controlled technologies to be utilized in support of Russia's aggressions in Ukraine.[3]

The ubiquity of microelectronics in common, everyday products — from electric breast pumps to microwave ovens to washing machines — presents manifold opportunities for the Russian military apparatus to illegally divert and acquire U.S.-origin technologies.

As DOJ Deputy Assistant Attorney General Eun Young Choi recently remarked, the DOJ is targeting those who facilitate illicit Russian conduct — "such as lawyers and money managers — as well as procurement networks that supply the Russian military with munitions and other military and tactical equipment."[4]

This article discusses certain surprising high-priority items for the Russian military, and advises how companies can avoid being a facilitator of the illicit Russian supply chain.

A Curious Trade Spike With Russian Neighbors

On Oct. 31, 2023, a criminal complaint in the U.S. District Court for the Eastern District of New York was unsealed. The complaint in U.S. v. Goltsev charged three individuals — one U.S. national and two Canadian nationals — for engaging in a global procurement scheme involving Brooklyn-registered corporate entities that purchased millions of dollars' worth of

dual-use electronics on behalf of Russian end users.[5]

These controlled technologies were shipped via points in Turkey, Hong Kong, India, China and the United Arab Emirates, and some match the make, model and part number of components found in seized weapons utilized by Russia in its war effort.

In this case, the complaint alleges that one of the charged individuals received orders from Russian end users in the defense sector seeking a specific item or part from the U.S., then communicated directly with domestic manufacturers and distributors to procure the items using aliases and acting under the guise of a Brooklyn-incorporated entity.

Then, acting with the assistance of foreign intermediaries, the individual allegedly transferred the items and ultimately rerouted them to Russia.

Perhaps most concerning, many of the discovered items and parts are classified as dual-use goods, meaning they can be sold legally in the U.S. and exported to certain foreign countries for consumer and commercial use.

However, through the illicit practice referred to as transshipment — wherein a product is diverted from its original destination — these goods can be resold in secondary markets to different countries for a banned military use.

U.S. authorities believe the Russian military is using this tactic and obtaining otherwise blocked U.S.-origin technology by diverting dual-use goods.

There is empirical evidence supporting the diversion hypothesis. According to reporting by the KSE Institute, an analytical center at the Kyiv School of Economics, there has been a sudden boom in sales of everyday household items containing microelectronics, including washing machines, refrigerators and electric breast pumps to Russia's neighbors.

Indeed, according to data compiled by Bloomberg from the EU's Eurostat database, "Armenia imported more washing machines from the European Union during the first eight months of [2022] than the past two years combined." Meanwhile, "Kazakhstan imported $21.4 million worth of European refrigerators through August [2022], more than triple the amount for the same period" of 2021.[6]

In another telling instance,

> the trade data show … that EU exports of electric breast pumps to Armenia nearly tripled in the first half of 2022 versus the prior year, despite a 4.3% drop in the Armenian birth rate. Likewise, Kazakhstan's demand for breast pumps from the EU soared 633% in the first half of 2022 even though the national birth rate fell 8.4% during the same period.[7]

The implication is clear: Russia is end-running trade sanctions through the diversion of otherwise innocuous, everyday goods.

Regulation, With A Call for Industry Diligence

In response to the threat of illegal diversion, the U.S. Department of Commerce's Bureau of Industry and Security, or BIS, has issued a warning to industry, identifying 45 common high-priority items because of their importance to Russia's war efforts.[8]

Prominent among those items are integrated circuits and radio frequency transceiver modules that have extensive commercial applications — however, they've also been found in Russian missiles and drones on the battlefield in Ukraine.

This warning followed a joint agency compliance note published earlier in 2023 by the DOJ, the U.S. Department of the Treasury, and the Commerce Department, seeking to educate businesses and enlist their aid in cracking down on illegal diversions to Russia.[9]

And most recently, on Dec. 22, 2023, the Biden administration issued Executive Order No. 14114, which grants the Treasury's Office of Foreign Assets Control new and broader authorities to target foreign financial institutions for engaging in conduct that facilitates transactions involving Russia's military-industrial base.[10]

The U.S. government is not alone — foreign authorities have recognized the difficulty of stopping diversion to Russia and have called upon commercial actors to play a larger role.

In early December 2023, U.K. authorities issued a red alert concerning the trade of high-priority items that can be critical to the Russian military and its arsenal.[11]

Much like the U.S. agencies' compliance note, U.K. authorities warned against transactions where the end user is obscured, and added other red flags, like transactions with (1) companies that have little or no online presence, (2) companies that were incorporated after Russia's invasion of Ukraine, (3) customers involving counterparties tied to a Russian military end user, or (4) companies that are either co-located or maintain shared ownership with a sanctioned Russian end user.

Beyond entreaties for private sector assistance, export enforcement agencies are also warning businesses that ship overseas about the potential legal consequences of failing to act with diligence.

As the BIS warning stated bluntly, the agency sees significant risk for U.S. and non-U.S. persons to "become (even inadvertently) entangled in violation of U.S. export controls and sanctions laws, resulting in potentially significant civil or criminal liability."

While it is clear that bad actors — like those alleged in the unsealed Eastern District of New York complaint — will draw enforcement if detected, U.S. authorities have emphasized that even nonmalicious transactions may land a company in hot water, especially if the business failed to engage in adequate due diligence.

As the joint agency compliance note warned, "[b]usinesses of all stripes should act responsibly by implementing rigorous compliance controls, or they or their business partners risk being the targets of regulatory action, administrative enforcement action, or criminal investigation."

The Folly of Willful Blindness

Today, most, if not all, electrical appliances use integrated circuits. Any product with a display screen, timers or automatic control may be of use in a weapons system. And while most of these technologies will not trigger strict U.S. export restrictions, technology diverted to Russia could violate U.S. sanctions.

To avoid the real possibility of playing an unwitting role in the weapons proliferation cycle benefiting Russia, industry involved in the manufacture or distribution of electric products

should step up due diligence on its customers and business partners.

Based upon the red flags identified by authorities and our own experience in the field, we recommend companies take the following precautions.

1. Keep a close eye on high-priority harmonized system codes that may encompass your items.

BIS has identified nine harmonized system codes in its list of common high-priority items. Particular attention and care must be paid to items in tiers 1 and 2 of the list, which include items like integrated circuits and radio frequency transceivers, as they have repeatedly been found in Russian missiles and drones.

2. Stay attuned to suspicious end use or end user signs.

Because diversion to Russia is illegal, bad actors will attempt to obfuscate their process. Unusual characteristics in the business or distribution transactions may be relatively easy to identify. For example, any refusal by the customer to provide details about the end user, intended end use or company ownership is a significant red flag.

Beyond that, sellers should be wary if the customer does not express a desire for a warranty or provisions of maintenance and software updates, as these exhibit (1) the buyer is likely not, in fact, the expected end user, and/or (2) the end user does not want or expect a transparent or enduring business relationship with the seller.

3. Be aware of any atypical sales patterns.

If your company is seeing an unusual uptick in sales — especially of items falling under one of BIS' high-priority harmonized system codes — that could indicate that some buyers are engaging in diversion.

New customers should also be vetted more seriously in this climate. And, in particular, any uptick in sales coming from entities in locations neighboring Russia should raise red flags.

4. Continue to monitor other suspicious behavior.

Consider (1) the willingness of a buyer to pay above-market prices; (2) if a buyer lacks an online profile or otherwise lacks accessible background information; (3) if the buyer did not exist or did not make purchases prior to the invasion of Ukraine in 2022; and (4) if the buyer is not the type of business that would utilize the commodity at issue.

This list is far from exhaustive. Industry participants should stay vigilant and use common sense checks on their transactions, knowing their own businesses and the nature of their typical sales.

5. Compare your transactions against existing sanctions lists.

Last but not least, industry participants must stay up-to-date on U.S. sanctions, applying to Russia and elsewhere. If the customer or their address is similar to one of the parties on a proscribed parties list, such as the BIS Entity List, the Specially Designated Nationals And Blocked Persons List, or the U.S. Department of State's statutorily debarred parties list, take action to confirm the customer's identity, and avoid dealing with sanctioned persons.

Conclusion

U.S. enforcement agencies have made clear that if red flags appear, it is the responsibility of industry participants to complete their due diligence and ensure they are not violating export controls.

The simplest and most effective route for businesses will be direct inquiries of all parties opposite a transaction, to gain as much visibility as possible regarding the item's end use and end users.

Companies facing such concerns should be sure to document their efforts and their findings, in case there is government scrutiny of the transaction in the future.

In light of the U.S. government's aggressive criminal enforcement posture and repeated warnings, no one should turn a blind eye to the threat of illegal diversion to Russia — even of seemingly wholesome items.

In 2024, we expect widespread government enforcement actions and innovative regulation in this area. A recent op-ed in The New York Times went so far to suggest that the U.S. government should require industry to install tamper-proof geolocation devices on certain products.[12]

Ultimately, industry participants' and U.S. agencies' interests are aligned in this extraordinary time of conflict — no company wants its name or product to be featured in the next indictment and press release, plucked from the wreckage of a battlefield.

Cate Baskin is an associate at Arnold & Porter Kaye Scholer LLP.

Henry B. Morris is an associate at the firm.

Deborah A. Curtis is a partner at the firm. She previously served as chief counsel for industry and security at the Commerce Department, and as a trial attorney and deputy chief in the DOJ National Security Division's Counterintelligence and Export Control Section.

[1] On September 15, 2010, five individuals and four of their companies, including Corezing International, were indicted in U.S. District Court in the District of Columbia on charges of conspiracy, smuggling, the illegal export of dual-use items from the United States to Iran, false statements, and obstruction of justice. The conspiracy involved the illegal export of thousands of radio frequency modules (RFMs) through Singapore to Iran. These are dual-use telecommunications items, at least 16 of which were later found in remote detonation systems of unexploded IEDs in Iraq.

[2] In April 2016, Lim Yong Nam, aka Steven Lim, 42 and a citizen of Singapore, was extradited from Indonesia to stand trial in the District of Columbia on charges of taking part in a conspiracy that allegedly caused thousands of radio frequency modules to be illegally exported from the United States to Iran, at least 16 of which were later found in unexploded

IEDs in Iraq.

[3] https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2023/11/joint-strike-force-deals-a-blow.

[4] https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-eun-young-choi-delivers-keynote-remarks-gir-live.

[5] United States v. Nikolay Goltsev et al., (No. 23-M-956).

[6] https://time.com/6226484/russia-appliance-imports-weapons/.

[7] Id.

[8] https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items.

[9] https://www.justice.gov/media/1277536/dl?inline=.

[10] "Taking Additional Steps With Respect to the Russian Federation's Harmful Activities," https://www.federalregister.gov/documents/2023/12/26/2023-28662/taking-additional-steps-with-respect-to-the-russian-federations-harmful-activities.

[11] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/687-necc-red-alert-exporting-high-risk-goods/file.

[12] https://www.nytimes.com/2023/12/29/opinion/chips-semiconductor-china-russia-military.html?smid=nytcore-ios-share&referringSource=articleShare.