SAYARI

Investigation of Starlink Shipments to Russia Reveals Global Export Controls and Sanctions Evasions Network

TABLE OF CONTENTS

Executive Summary

An investigation by Sayari analysts into Starlink internet terminals illegally entering Russia[1] not only validates The Wall Street Journal's (WSJ's) original findings, but also uncovers an expansive facilitation network circumventing broader export controls and sanctions meant to limit the flow of dual-use goods to Russia.

The U.S. and EU, among other countries, imposed strict sanctions and export restrictions on Russia following its invasion of Ukraine and have continued to add new measures aimed at restraining Russia's economy and hindering its war effort.[2] These measures include the prohibition of the export of goods and technologies to Russia that have a possible military end use, including advanced technology like Starlink internet terminals. Starlink terminals provide a serious advantage to Ukrainian forces who use them to fly drones in areas with disrupted service,[3] and recent reporting, such as the WSJ article that prompted this investigation, has revealed that Russian forces are using them to fight against Ukrainian forces in contested areas despite their prohibited use in Russia.

Sayari's investigation shows individuals and their related companies collaborating — largely by using standard business practices such as transshipment, dropshipping, and mail forwarding companies registered across multiple jurisdictions — to ship prohibited goods to Russia through a network of companies in the United States, Germany, Latvia, Cyprus, Turkey, Russia, Gibraltar, Georgia, Hong Kong, and the United Arab Emirates (UAE). The patterns observed in this investigation can be utilized to identify additional networks established for sanctions evasion or the procurement of sensitive technologies, including those with possible military end use.

Global Network, Global Reach

Using Sayari Graph and open source investigative techniques, Sayari analysts uncovered a vast network of companies and individuals centered in Russia but operating around the world, using ecommerce companies and websites to move goods in contravention of sanctions and export control regulations.

Sayari analysts identified two main actors who are almost certainly Russian citizens and who manage at least 16 companies across 10 countries, the majority of which operate in the warehousing, freight forwarding, and wholesale business sectors. The individuals operate the network through at least a dozen interconnected websites that sell U.S. and EU consumer goods, openly advertise how they can help buyers get around trade restrictions, and show others how to set up their own similar businesses using the network's warehouses. These websites frequently have identical online storefronts and

1 Thomas Grove, et al., "The Black Market That Delivers Elon Musk's Starlink to U.S. Foes," *The Wall Street Journal*, April 9, 2024, https://www.wsj.com/business/telecom/starlink-musk-ukraine-russia-sudan-satellite-communications-technology-f4fc79d9.

2 "What are the sanctions on Russia and have they affected its economy?," *BBC*, February 23, 2024, https://www.bbc.com/news/world-europe-60125659.

3 Graeme Massie, "Elon Musk helps Ukraine with SpaceX's Starlink satellites," *Independent*, February 28, 2022, https://www.independent.co.uk/news/world/europe/elon-musk-helps-ukraine-satellites-b2024893.html.

stock a variety of consumer products, ensuring end buyers in Russia have a broad selection of typically restricted goods from which to choose. Domain analysis revealed that many websites in this network, despite not being located in Russia (i.e., not having .ru URLs), are nevertheless hosted by Russian IP addresses.

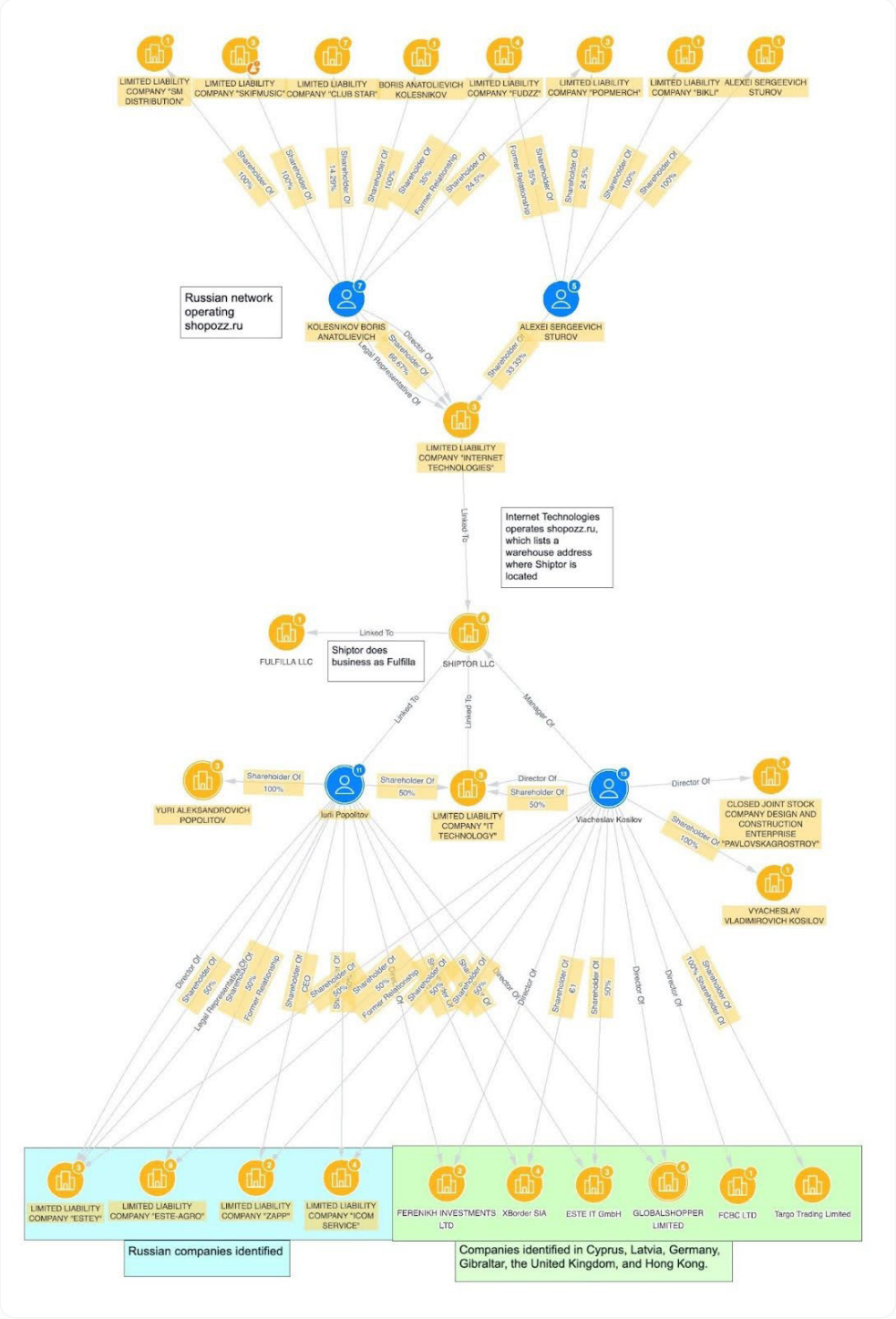

Fig. 1: *Sayari Graph network depicting the companies and individuals identified in the Shopozz network.*

As shown in the flowchart below, the network's global reach allows it to move U.S. and EU goods to Russia via more permissive jurisdictions, taking an indirect route to avoid current trade restrictions.

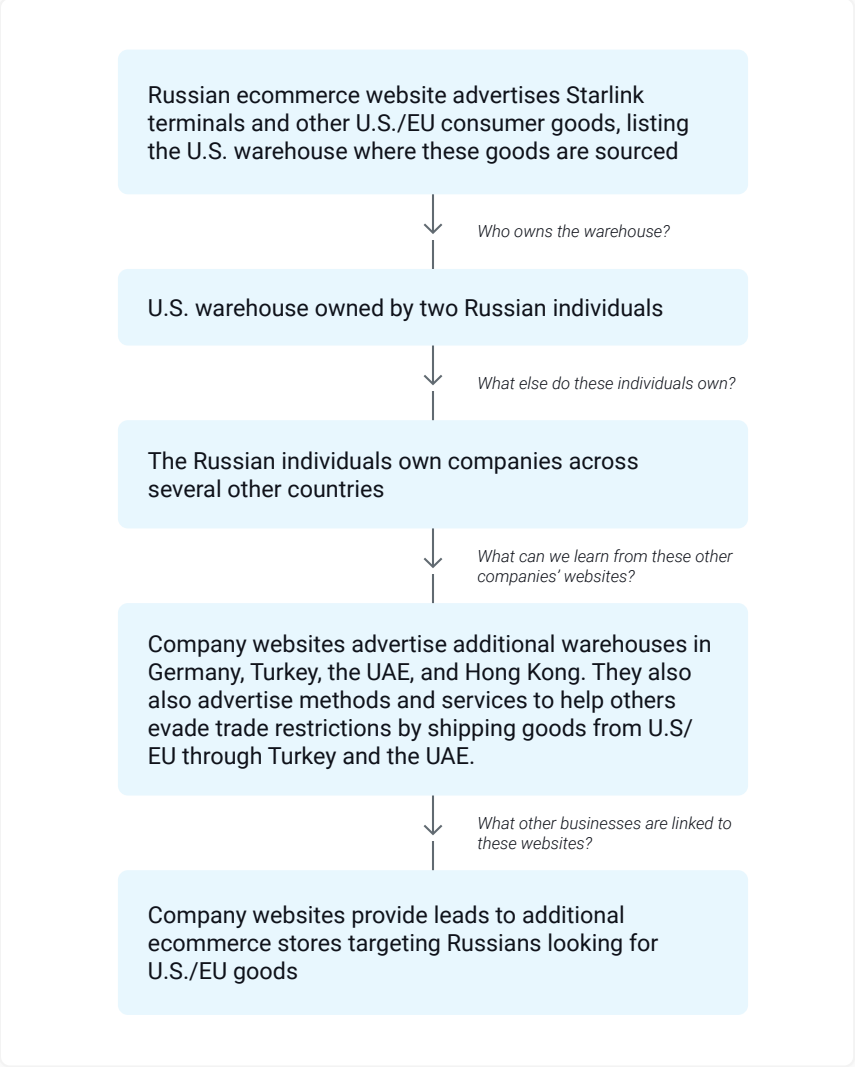

Fig. 2: *Flowchart detailing the line of inquiry that revealed the network's interconnected, global reach through companies in multiple jurisdictions and dozens of interlinked websites.*

The two Russian individuals identified by Sayari analysts maintain warehousing businesses in the U.S. and Germany as well as additional businesses in Latvia, Cyprus, Turkey, Hong Kong, and Gibraltar. They also own businesses in the UAE through an individual located there. The companies' online presences allude to the function of each jurisdiction: the U.S. and EU-based businesses are sources for goods advertised on their ecommerce sites; the Turkish, Hong Kong, and UAE-based businesses are intermediary destinations for the goods before they end up in the hands of consumers in Russia.[4]

4 The U.S. and EU have placed trade restrictions on the flow of goods to Russia and Turkey. The UAE and Hong Kong, among others, have not.

Illegitimate Use of Legitimate Practices

This network is able to operate openly and expansively by taking advantage of standard business practices such as dropshipping and mail forwarding that, when used in a certain way, allow it to avoid sanctions and export restrictions. Registering different companies in multiple jurisdictions, although a legal business practice, also helps the individuals in this network facilitate their illicit activities. These tactics present a challenge to investigators, as many of these businesses appear at first glance to be operating legitimately. The process of using these standard practices — in this case for illegitimate purposes — is described in the flowchart below.

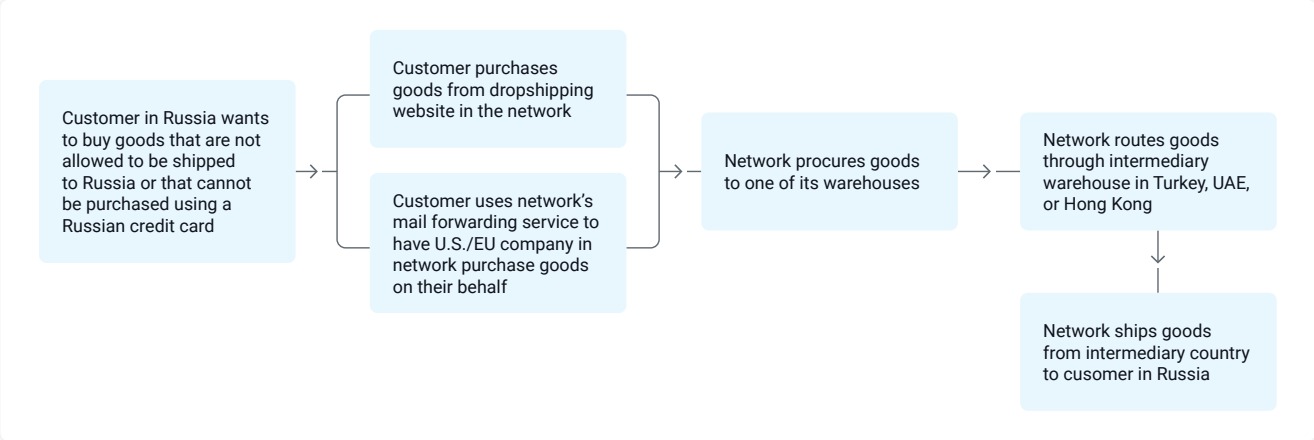

Fig. 3: *Flowchart depicting how the network operates.*

Dropshipping / Third-Party Logistics

Dropshipping is the practice of outsourcing ecommerce logistics processes — including inventory management, warehousing, and fulfillment — to third-party businesses. In this model, a retailer might take an order but not keep stock on hand, instead transferring the order details to a logistics company, which in turn ships the order directly to the customer.

This network operates several dropshipping websites advertising goods from hundreds of U.S. and EU brands to Russian consumers. The websites themselves are not connected to the registered legal entities through corporate filings; rather, the warehouses fulfilling the websites' orders are.

Most of the websites identified as part of this network are dropshipping websites, some of which encourage visitors to set up their own dropshipping sites using the network's warehouses, thereby broadening the network's reach. While dropshipping is a legitimate practice that allows businesses to operate without large upstart costs, its use in this network helps to confirm that the warehouses in the U.S. and Germany, among others, are likely furnishing Russia-bound orders due to their access to Western goods.

Transshipment

Transshipment is the shipment of goods through one or more intermediary countries en route to a final destination. Transshipment can occur naturally in international trade but can also be used to evade trade restrictions and sanctions by obfuscating the origin and/or destination of the goods being shipped.

Because the U.S. and EU have imposed restrictions on goods destined for Russia, the network has to leverage transshipment to evade restrictions. One website in the network explains how, since some goods for sale are not permitted to ship to Russia, it will transit those goods through Turkey to evade restrictions. Because Turkey has not placed similar restrictions on goods shipping to Russia, transshipment through Turkey enables Russian consumers to continue to purchase and receive goods that are otherwise restricted.

Mail Forwarding

Mail forwarding allows individuals and businesses to redirect mail from one address to another. It can be used for a variety of legitimate reasons, such as when moving to a new house, but it can also be used to mask the end recipient of a shipment. If a recipient wants to conceal their address, they can sign up for a virtual mailbox or office, order goods to that address, and set up mail forwarding to their actual address.

One website in the network advertises itself as a mail forwarding service that buys goods for clients from the U.S., Europe, UAE, Turkey, and China and delivers them to clients in Russia. The same website also openly advertises that it will enable purchases from stores that do not ship to Russia by placing orders — even of banned items — on the customer's behalf and facilitating their delivery, presumably through some sort of mail forwarding service.

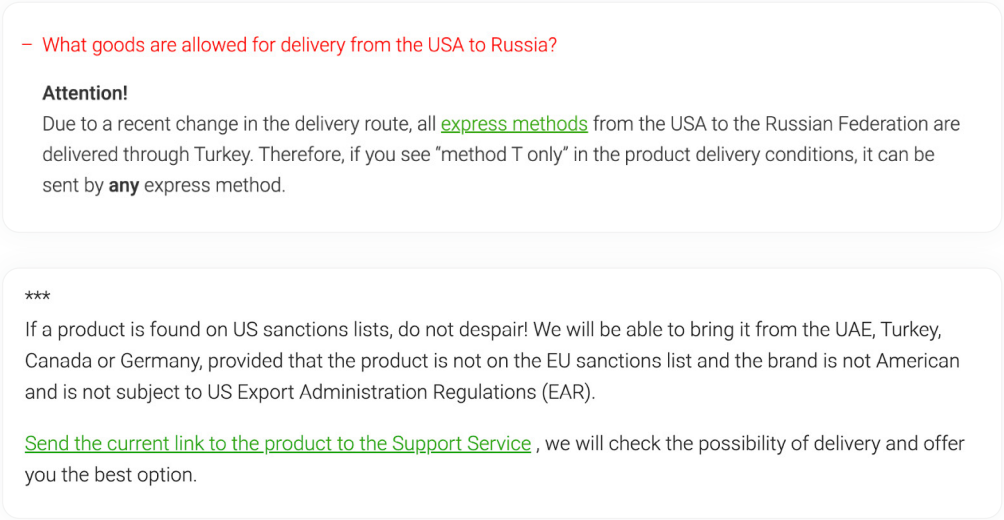

Fig. 4: *Excerpts pulled from one of the websites' FAQ pages detailing how shipments from the U.S. to Russia now proceed through Turkey and that goods on U.S. sanctions lists can be delivered from the UAE, Turkey, Canada, or Germany.*

How to Distinguish Illicit from Licit

Sayari analysts began their investigation into the Starlink terminal transshipment network by looking at entities associated with the website shopozz.ru, which was cited in the initial WSJ report. Building out the network from there, analysts used Sayari Graph to interrogate corporate and trade relationships in tandem with various investigative techniques. Although global transshipment networks are explicitly designed to evade detection, analysts are able to apply open source investigative techniques to uncover their illicit activity.

The majority of illicit activities must touch licit systems in order to operate: websites have to be registered online; businesses must be registered with the relevant authorities; and businesses need to advertise to reach their target markets. Investigators can therefore scan these systems for patterns indicative of illicit activity.

Opening and operating companies in the U.S. and EU, while simultaneously operating in countries like Turkey, the UAE, and Hong Kong/China (or in any jurisdictions that do not maintain the same trade restrictions as the U.S. and EU) without clear geographic necessity, may indicate potentially evasive business practices, for example. A company in this type of global network describing its business activity as warehousing, dropshipping, or mail forwarding may also indicate an intent to avoid trade restrictions.

When investigating a suspected sanctions or export controls evasion scheme, combining the techniques below can help reveal illicit procurement networks and the individuals behind them.

Investigative Step	Current Case Result
Use known address(es), identifiers, and/or names to search a corporate network analysis tool such as Sayari Graph for individuals or companies that might be involved in the network.	Analysts searched an address on the initial website of interest in Graph and uncovered a U.S.-based company and two individuals behind the network.
Build out company and individual networks to determine previously unknown businesses and individuals that could be associated with the network.	Using the globally connected data in Sayari Graph, analysts uncovered an additional 16 companies in 6 countries.
Search for those businesses online to see if they have any online presence.	Analysts found that several of the businesses had websites, which linked to more websites, thereby expanding the network and providing more insight into its operations.
Use social media to find any relevant posts connected to the account of a business or individual in the network.	Social media profiles for the two individuals behind the network led to two additional companies in Delaware and Russia that were not immediately traceable in corporate data.
Look up domain registrations for any known websites, which can confirm ownership of businesses, list contact information, and identify previously unknown individuals operating in the network.	Domain registrations confirmed that most websites were owned by already-identified individuals in the network.

Table 1: *Steps in the open source investigative process and their results in the Starlink transshipment network case.*

Conclusion

The interconnected nature of today's global economy makes enforcing sanctions and export controls more difficult than when countries primarily sourced goods domestically. Sanctions have restrained some of Russia's ability to prop up its war machine, forcing Moscow to identify new avenues of generating revenue. Russia has done this primarily by relying on China as a supply channel and strengthening ties with other global partners, convincing those without strong opinions on the war in Ukraine to remain neutral. Neutral countries that are supporting the type of network detailed in this investigation serve as domiciles for nodes in the network and/or as transshipment points for goods destined for Russia.

The initial investigation into the illegal procurement of Starlink terminals — an item with a critical military applications — revealed a network moving a wide variety of prohibited goods, many of which are intended for more standard, everyday use. The fact that sensitive technologies can be moved into Russia using the same techniques as American-made cosmetics and vitamins underscores the likely ubiquitousness and utility of this type of network: no additional special channels are necessary to import this much more critical item in contravention of restrictions.

While this investigation explored the workings of a Russian network circumventing export controls and sanctions in great detail, using a corporate and trade network analysis tool like Sayari Graph can help investigators arrive at such insights quickly, uncovering how critical, U.S.-made items like integrated circuits can be transshipped through Hong Kong and other third-countries to Russia.

ABOUT SAYARI

Sayari is the counterparty and supply chain risk intelligence provider trusted by government agencies, multinational corporations, and financial institutions. Its intuitive network analysis platform surfaces hidden risk through integrated corporate ownership, supply chain, trade transaction and risk intelligence data from over 250 jurisdictions.

Sayari is headquartered in Washington, D.C., and its solutions are used by thousands of frontline analysts in over 35 countries.

To learn how Sayari powers safer global commerce, please visit sayari.com. >