The Use of Transshipment Hubs by Illicit Networks to Evade Sanctions

STRATEGIC TRADE RESEARCH INSTITUTE

August 2023

Introduction

In order to support its illegal invasion of Ukraine, the Russian Federation has relied on foreign-produced microelectronics and other high-technology components for its weapons systems. These products are used in satellite guidance systems for missile accuracy, tactical combat platforms, UAVs, long-range missiles, signals intelligence, communications, and electronic warfare systems. While most of these goods are produced in the United States, Europe, Taiwan, Korea, and Japan, illicit trade networks use transshipment hubs to evade trade controls and procure the items to Russian end-users. In previous indicative studies on cases of unlicensed exports discovered through end-use checks, transshipment points were used about 94 percent of the time, which indicates that the end use or end user of an export were not declared accurately, and that transshipment points were used to hide ultimate customers and destinations.[1]

Given that illicit actors seek to exploit any vulnerabilities within supply chains and trade routes, it is essential for countries that serve as major transshipment points to establish effective controls and good practices to thwart attempts by illicit procurement networks to leverage ports and other points of entry to transship sensitive components.

The Use of Transshipment Hubs by Illicit Trade Networks

Procurement agents transship goods in order to evade trade controls and hide the end-users and end-uses of sensitive goods. Transshipment occurs when goods enter a port or entry in a country but do not enter the country's customs area. Examples include moving goods from ship-to-ship at a port or briefly warehousing and repacking goods at a Free Trade Zone (FTZ). Illicit transshipment of items occurs when goods are transferred from their place of origin through an intermediary country to reach an unauthorized final destination. Often the large trade volumes

[1] https://www.gao.gov/assets/gao-12-613.pdf

at major transshipment ports camouflage the illicit shipment of diverted goods. In addition, brokers, front companies, and middlemen can facilitate sanctions evasion-related activities at these hubs, hiding their transactions among the volumes of fast-moving commercial goods.

Common tactics used by procurement agents to use transshipment points to evade trade controls include:

- Falsely declaring the transshipment point as the end-destination, and instead transshipping sanctioned goods through the purported end-destination to the true end-user
- Falsely declaring a value of shipped goods as lower than the real value, to evade having to file necessary paperwork
- Re-labeling sanctioned goods to obfuscate what they are at the transshipment point
- Removing serial numbers on goods at the transshipment point to obfuscate their origin and destination
- Re-packaging sanctioned goods at the transshipment point
- Obtaining fraudulent export licenses with false information regarding the goods, the end-use, or the end-user
- Fabrication of shipping documents.

Countering Transshipment Vulnerabilities

Because of Southeast Asia's strategic geographical position, it is essential for countries to take proactive measures to counter attempts by illicit networks to use transshipment points to evade sanctions. There are concrete actions that are key to mitigating the risks posed by transshipment point vulnerabilities.

For the public sector, this includes:

- Establishing a strong regulatory structure that establishes an authorization process for the transshipment of certain goods
- Establishing notification procedures
- Maintaining cooperation and outreach between the public and private sector to communicate about specific diversion threats focuses on specific goods and technologies that are subject to sanctions
- Establish strong risk assessment procedures to be able to identify shipments of potential concern and targeting
- End-use monitoring and checks of goods;
- Training of enforcement agencies, especially Customs, to identify red flags
- International cooperation and intelligence-sharing

For the private sector, the most important measure to ensure that the legal and reputational risks of being involved inadvertently in an illicit trade supply chain is compliance. Because of the multitude of actors involved – the manufacturers, distributors, resellers, and freight forwarders – it is up to each organization to have the compliance procedures in place to be able to recognize when a transaction or activity is inconsistent with industry norms and practices. There are common red flags that can be identified when dealing with illicit trade actors – and it is essential for compliance programs to not only consistently be able to stop transactions where red flags are identified but keep abreast of new red flags published and sanctions evasion tactics. Private sector entities must exercise heightened caution and conduct additional due diligence if they detect warning signs of potential sanctions or export violations.

Case Study

A December 2022 U.S. indictment revealed the extensive use of transshipment points and the common tactics used by illicit trade networks to leverage them. Per the indictment, several

individuals unlawfully purchased and exported highly sensitive and heavily regulated electronic components, some of which can be used in the development of nuclear and hypersonic weapons, quantum computing and other military applications. The defendants are affiliated with two Russia-based companies, Serniya Engineering and Sertal LLC, which both operate under the direction of Russian intelligence services to procure advanced electronics and sophisticated testing equipment for Russia's military industrial complex and research and development sector.

As part of the scheme to smuggle sensitive components to Russia in violation of U.S. sanctions, certain individuals acting on behalf of the trade network would fabricate shipping documents and invoices, repackaging and reshipping items to intermediate destinations – including transshipment points - around the world before eventually arriving in Russia. The network also set up and manage dozens of shell companies and corresponding bank accounts throughout the that were used in the scheme.