

Russia Suicide Drones

STRATEGIC TRADE RESEARCH INSTITUTE

August 2023

Suicide drones, also called Shahed drones, loitering munitions or kamikaze drones, are aerial weapons systems that are programmed with coordinates ahead of time and rely on GPS to hit their targets. In the last few years, dozens of countries worldwide have acquired these weapons as part of their weapons arsenal – making their production and trade a high priority as well as the necessity to implement measures prevent their illicit trade and acquisition by countries using them in violation of sanctions programs.

In October 2022, the Russian Federation used 28 Shahed drones in successive wave attacks in the Ukrainian capital city, Kiev, killing at least four civilians. While it is difficult to hit large targets with suicide drones due to their size, their relatively low cost and ability to be employed without personnel make them an option for countries seeking to use massive numbers of them to saturate a target or to terrorize a population.

The worldwide production of these drones is increasing, with major producers located in for example, the United States, several European countries, Israel, India, Iran, Taiwan, China, and more. The Shahed drones used by Russia were acquired from Iran, but importantly, the majority of parts in the Iranian drones were of U.S., Canadian, Japanese, Swiss, and Chinese origin. These foreign components, used for functions such as navigation to data processing, are the following:

- Microchips
- Microprocessors
- Circuit board components
- Microcontrollers
- Voltage regulators
- Digital signal controllers
- GPS modules

Many countries have established sanctions programs that include some of these items as subject to export authorization or as prohibited for export to certain end-users and destinations. It is increasingly important for companies as well as government agencies to ensure that appropriate

measures to prevent these goods from being inadvertently part of the suicide drone supply chain to Russia.

Most of the goods listed above are considered dual-use, meaning that they can be used for both civilian and military uses, and are subject to strict authorization requirements or prohibitions from being sold to certain end-users in specific destinations. However, illicit trade networks utilize a number of tactics to obfuscate the true end-use and end-user of the goods, such as the use of corporate vehicles to obscure the transaction's source of funds, the use of shell companies to conduct international wire transfers, the use of transshipment points to change the ultimate destination of the goods, and many more. It is essential for parties involved along the supply chain to be aware of the kinds of components that could potentially end up in suicide drones acquired and used by Russia and implement safeguarding measures to ensure compliance with relevant national and international trade controls. This includes being aware of red flags that may signal illegal trade activity, including trade-based money laundering.

In some cases, where goods are very common and sold in bulk, such as computer chips, companies sell to large overseas distributors located in offices worldwide. It is key for the companies involved in the supply chains of these items to have strong internal compliance systems (ICPs) in order to ensure that they are not distributing to sanctioned end-users and end-uses. These include:

- Management commitment
- Training and awareness
- Screening and checking
- Recordkeeping
- Written policies
- Self-audits
- Change management
- Software automation

In particular, companies that produce components that can potentially be used in suicide drones must remain consistently vigilant with regards to the end-use and end-users of their products.

Common red flags, which are consistently updated by government agencies, can help identify problematic transactions.