Yermak-McFaul
International Working Group
on Russian Sanctions

& KSE | Institute

Foreign Components in Russian Military Drones

Olena Bilousova, Agiya Zagrebelska,
Vladyslav Vlasiuk, and Nataliia Shapoval

August 23, 2023

The International Working Group on Russian Sanctions aims to provide expertise and experience to governments and companies around the world by assisting with the formulation of sanctions proposals that will increase the cost to Russia of invading Ukraine, reduce the ability of Russia to continue its invasion of Ukraine, and will support democratic Ukraine in the defense of its territorial integrity and national sovereignty. Our working group is comprised of independent experts from many countries. We coordinate and consult with the Government of Ukraine and those governments imposing sanctions. This consultation process helps to inform our views, but our members express independently held opinions and do not take direction from or act at the behest of the Government of Ukraine or any other government or entity. All members of this working group participate in their private capacities. Like other papers produced by this working group, our aim is not to produce a consensus document, but instead to provide a menu of possible additional measures to be considered by governments, multilateral institutions, and private actors. The implications of every sanction have not been thoroughly analyzed, and not everyone necessarily agrees with every specific sanction or action proposed.

Contents

I. Executive Summary

Russia's invasion of Ukraine has confirmed the critical role of Unmanned Aerial Vehicles (UAVs) in modern warfare. UAVs are serving multiple functions in this war, including reconnaissance, offensive maneuvers, and kamikaze missions. The spectrum of capabilities extends from specialized military UAVs to repurposed commercial variants. The classification of drones includes strategic, operational, and tactical UAVs, with each contributing to distinct aspects of warfare. The production of these drones involves a high share of components that are produced by the countries in the sanctions coalition. Companies located in democratic countries are helping Russia's military in Ukraine. Since these weapons are often used to attack civilians, these companies are also supporting Russian terrorist acts inside Ukraine. This support for Russia's war efforts and terrorist acts in Ukraine must stop. We urge countries to strengthen export controls and enforcement procedures in order to limit Russia's access to such components.

Shahed-136/131, Lancet, and Orlan-10 **UAVs**

Since February 24th, 2022, Russia has deployed the Iranian-made Shahed-136/131 UAVs and Russian-made Lancet drones or loitering munitions in order to attack Ukrainian civilians and infrastructure. These drones offer a cost-effective alternative to Russian-made missiles, enabling Russia's armed forces to target energy infrastructure, overwhelm air defenses, erode Ukrainian morale through civilian casualties, and reveal Ukrainian air defense system placements. Russia has also deployed the Russian-made Orlan-10 UAV – a cost-effective reconnaissance and surveillance tool that plays a pivotal role for Russian forces in Ukraine. The Orlan-10 is integrated into the Unified Tactical Control System, coordinating different troop actions. It aids in reconnaissance, target guidance, and can disrupt communications via electronic warfare.

Foreign critical components in Russian military UAVs

We analyzed **174 foreign** components retrieved from Shahed 136/131, Lancet, and Orlan-10 drones in Ukraine. Despite import substitution efforts, the Russian military still heavily relies on foreign-made components, particularly microelectronics. Notably, **69%** of these components originate from U.S.-owned companies. Our investigation identified essential electronic components that are challenging to replace. The accessibility of these components, often obtained through publicly accessible marketplaces, presents a complex issue with regulatory oversight of critical technological transactions. Among these components, microelectronics are crucial. Components such as processors, microprocessors, voltage regulators, microchips, and transistors are prevalent in drones like Orlan-10, Lancet-3, and Shahed-136/131. GLONASS-enabled modules for navigation and electric engines are also vital components for the production of these UAVs.

Russian import of critical components

We focused on Harmonized System (HS) codes associated with components found in Russian UAVs. Using trade data, we analyzed trade patterns associated with these components.

Our investigation revealed an increase in trade volumes after a sharp downturn at the beginning of the full-scale invasion during the third quarter of 2022. These transactions amounted to **$7.2 billion** for the period from January to May 2023, which is 19% higher than the corresponding period in 2022 (**$6.1 billion**). In 2022, the total amount was **$15.8 billion**.

China stands out as a crucial supplier of critical components for Russia, responsible for a significant share of deliveries. Since the start of the full-scale invasion, China has contributed 67% of these components, with 17% routed through Hong Kong. Turkey and the United Arab Emirates also play notable roles, contributing 5% and 2%, respectively. Despite changes, the European Union maintains a 14% trade share with Russia, while the Eurasian Customs Union serves as a major trade route. Many US and EU companies operate production facilities in China, further influencing component transfer.

The top producers for the first five months of 2023 were Intel, Analog Devices, Samsung, Texas Instruments, and Xilinx (AMD), with components from these manufacturers found in Russian UAVs and other military equipment.

Sanctions evasion

Electronic components from sanctions coalition countries used in producing Russia's UAVs predominantly enter Russia through intermediary countries unaffected by sanctions. In response to escalating restrictions, Russia employs tactics to obscure its procurement efforts. These tactics involve illegal networks, disguising customs data, one-day shell companies, expanding intermediary entities, diversifying suppliers, and orchestrating fake transit operations. These strategies exemplify Russia's adaptive response to sanctions, utilizing multifaceted channels and actors to evade sanctions frameworks.

This evasion is amplified by factors like offshore production, the intricate definition of sanctioned goods, insufficient compliance procedures, and sluggish reactions to violations. These dynamics highlight the challenge in maintaining effective sanctions against Russia's acquisition of critical components for UAVs, necessitating robust countermeasures and oversight.

Policy recommendations

To prevent the provision of crucial components to Russian military manufacturing, the following measures could be implemented:

Alignment of sanctions across the sanction coalition: Aligning sanctions lists across coalition countries to encompass a broader scope of companies involved in the military complex is essential, as even some major producers of military equipment remain unsanctioned. Alignment includes adopting a centralized approach to dual-use goods lists with standardized criteria and classification based on Harmonized System codes. Improving information exchange and cooperation among coalition nations is also crucial, including the

sharing of transaction data and collaborating on investigations to prevent violations and circumvention.

Broader export controls: Expanding sanctioned product categories by utilizing broader goods classifications based on 6-digit Harmonized System (HS) codes can prevent misclassification and simplify export controls enforcement. Strengthening control over dual-use goods available on open marketplaces and ceasing production of GLONASS-enabled microelectronics by Western firms are also crucial steps.

Improve company compliance: Enhancing collaboration between critical component producers and authorities is key to improving sanctions compliance and implementing effective measures. Sharing information and experience can strengthen both sides in their efforts. Clear compliance guidance should be established, particularly for smaller enterprises lacking resources. A comprehensive database of potential business partners, including sanctions coverage and past violations, can facilitate compliance.

Increase responsibility: Companies must take responsibility for preventing their products from reaching Russian military applications. Governments should investigate well-known companies to demonstrate their commitment to enforcing sanctions. Explicit procedures and documentation requirements can establish responsibility for compliance. Equally important is applying the same regulatory oversight to products manufactured outside the sanctions coalition countries to counter on-production tactics.

Using existing institutions and frameworks more effectively: Leveraging the Anti-Money Laundering (AML) framework could fortify export control measures, as sanctions evasion often has similar patterns to money laundering. Coalition authorities can adopt this framework to trace opaque ownership structures and dynamic actor changes involved in circumventing sanctions. Applying AML practices to export controls is valuable for identifying structures in third countries vital for military input production and exports to Russia, especially if production occurs outside the sanctions coalition. Additionally, utilizing financial sector sanctions, such as targeting Russian banks and monitoring transaction patterns that facilitate these technology transfers, can enhance enforcement efforts by restricting payment channels for imports and mandating companies to disclose payment-related information to banks.

II. General Description of UAVs and Their Usage

The conflict between Russia and Ukraine has underscored the pivotal role of UAV technology in contemporary warfare. UAVs exhibit multifaceted applications encompassing reconnaissance, offensive maneuvers, barrage tactics, civilian utility with payload release systems, and First-Person-View (FPV) kamikaze missions. The comprehensive spectrum of capabilities offered by specialized military UAVs, incorporating novel proprietary innovations rooted in combat experience, as well as adapted commercial variants repurposed for combat deployment, are being actively employed.

In the present landscape, a variety of drone classifications operate on the battlefield. Preeminent among these are strategic and operational UAVs undertaking deep-seated reconnaissance missions, strategically positioned hundreds of kilometers beyond enemy lines. Their principal objective resides in the identification of strategic targets, enemy air defense or missile forces.

Operating at the next tier are operational and tactical drones, primarily tasked with directing artillery adjustments at the battalion or brigade echelons.

Finally, tactical drones encompass a category that often consists of non-specialized vehicles such as commercial quadcopters like the Chinese DJI (commonly known as Mavic) and Autel. Curiously, an extensive demand for these drones has manifested in the conflict with Russia. The practical communication range for such devices spans approximately 5-6 km, while the stipulated range extends to 10 km.[1]

A distinctive variant, the loitering munition, represents an unmanned aerial vehicle integrating an onboard warhead. This unique UAV configuration maintains extended airborne readiness proximate to a designated target, enabling swift engagement upon command from the operator or execution of algorithmically prescribed tasks. These systems encompass aerial munitions engineered to combine UAV advantages with aerial bomb warhead attributes. The Shahed-136/131 serves as an example, effectively operating as a slow cruise missile furnished with a diminutive warhead payload.

The utilization of Iranian-conceived loitering munitions within Russia's operations has assumed considerable proportions. While these devices pose a substantial threat to Ukraine's civilian infrastructure, Russia has, up to this point, exhibited restraint in employing them against Ukrainian military objectives. However, a more formidable challenge confronts Ukraine's Armed Forces through the emergence of Lancet-3(M) loitering munitions developed in Russia, which have seen heightened deployment. These deployments are aimed at incapacitating Ukrainian artillery, radar installations, and surface-to-air missile (SAM) systems situated out of reach from Russia's ground-based assets.

Shahed-136/131

General description

The Shahed-136, an unmanned aerial vehicle categorized as both a loitering munition and kamikaze drone, features dimensions of 3.5 meters in length and a weight of 200 kg. Notably,

[1] Mind.ua, Drones of the frontline: Strategic and civilian drones in action, 2023

its design encompasses a delta-shaped wing configuration, housing a warhead in the nose section with a weight range spanning 30 to 50 kg. Positioned in the rear fuselage, the engine propels a two-blade propeller. The UAV's structural composition integrates carbon fiber and polymer materials for the body, complemented by a wooden rotor assembly. Its initiation entails deployment from a containerized launcher adaptable for installation on diverse platforms like trucks, railroad cars, or ships.

Despite its relatively straightforward fabrication, the Shahed-136 incorporates high-quality electronic components distinguished by a surplus of attributes conducive to forthcoming enhancements. Among these attributes is a potent processor system, facilitating signal processing in scenarios involving swarm drone utilization, along with provisions for potential antenna integration, potentially facilitating post-launch control.

As of the present juncture, the Shahed-136 operates without remote control intervention, its flight path and target parameters pre-programmed prior to launch. Navigation relies on GPS signals. While the design concept accommodates aerial reconnaissance capabilities, the samples employed in Ukraine lack camera equipment.

The Shahed-131, akin to a scaled-down modernized variant of the Shahed-136, features reduced dimensions, measuring 2.6 meters in length and weighing 135 kg. Furthermore, its warhead exhibits diminished proportions, ranging from 10 to 15 kg. Although a substantial portion of electronic components across both UAV models are standardized, the Shahed-131, potentially conceived and fabricated subsequent to the Shahed-136, incorporates countermeasures against GPS signal interference through electronic warfare measures. Notably, it also incorporates a rudimentary inertial system enabling approximate course and altitude maintenance in instances of satellite signal absence.

Specifics of usage in Ukraine

The adoption of Iranian Unmanned Aerial Vehicles (UAVs) finds its primary rationale in their cost-effectiveness, particularly when contrasted with pricier and technologically advanced missile armaments. Russian missile systems typically command a price range of approximately 500 thousand to 1 million US dollars per unit. In stark contrast, the Shahed-131/136 drones present a cost profile that is notably reduced, spanning roughly 10 to 20 times less at around 50 thousand US dollars.

The initial deployment of Shahed kamikaze drones was documented within the Kharkiv sector during the latter part of August 2022. Ukrainian forces achieved their inaugural interception of such drones on September 13, 2022, within Kupiansk of the Kharkiv region.

The utilization of Iranian UAVs by Russia within the Ukrainian context has been motivated by a spectrum of objectives, encompassing:

- **Infrastructural disruption:** The deliberate targeting of energy infrastructure serves the strategic purpose of instigating a humanitarian crisis within Ukraine.
- **Air defense saturation and ammunition depletion:** Employing these UAVs aids in overwhelming the Ukrainian air defense apparatus while concurrently provoking a scarcity of munitions for the pre-existing defense systems.
- **Morale undermining through civilian casualties:** By increasing the count of civilian casualties, the aggressor aims to erode the nation's morale, thereby undermining its resolve to resist.

- **Revelation of air defense system placement:** The deployment of Iranian UAVs exposes the positioning of Ukrainian air defense systems, potentially offering valuable intelligence to Russia.

These multifaceted objectives underscore the calculated and strategic employment of Iranian UAVs by Russia in the ongoing conflict in Ukraine.

Within the last three months, Russia's campaign has witnessed the deployment of over 600 Shahed-136/131 UAVs for assaults on Ukrainian cities. The ramifications of these attacks have reverberated through the civilian populace, leading to grievous casualties. Illustrative incidents include:

- October 17, 2022: In the course of a sweeping assault on Ukrainian infrastructure, an Iranian drone struck a residential edifice, claiming the lives of four individuals, among them a 28-year-old woman who was six months pregnant.
- March 22, 2023: In a distressing incident, an Iranian UAV targeted a dormitory situated in the town of Rzhyshchiv within the Kyiv region, tragically resulting in the loss of nine lives.
- June 10, 2023: The repercussions of a UAV assault manifested in a conflagration that erupted within a residential complex in Odesa. This tragic event claimed the lives of three individuals, and over ten others suffered injuries, among them a five-year-old girl.

These distressing events underscore the devastating impact of the utilization of Shahed-136/131 UAVs by Russia, precipitating significant civilian losses and underscoring the gravity of the conflict's impact on local populations.

Furthermore, augmented by the establishment of an infrastructure and substantial influx of supplies from Iran, Russia initiated a heightened frequency of drone sorties along diverse trajectories. This strategic maneuver aimed to disrupt and overwhelm Ukrainian air defense initiatives, thereby amplifying the challenges faced by Ukrainian forces.

Commencing from the period spanning April to May of the present year, a discernible surge has emerged in the volume of UAVs deployed within individual offensives. A striking exemplar of this escalated scale occurred on May 28, during which a singular assault witnessed the simultaneous launch of 54 drones. This substantial escalation not only underscores the evolving tactics employed by Russia but also portrays the growing intensity of these unmanned aerial incursions.

In their utilization within Ukraine, Russia has pursued a strategy of obscuring the Iranian origin of UAVs by presenting them as indigenous creations. This is achieved through alterations in the drone's physical appearance, incorporating divergent color schemes, and affixing Russian designations such as "M### Geranium-2" or "M### Geranium-1" onto the stabilizers. An additional measure entails inscribing "DO NOT TAKE" onto the ailerons of the monowing.

In-depth analysis has shed light on the manner in which these inscriptions have been applied. It has been discerned that these designations are affixed using readily removable adhesive films, in contrast to other inscriptions in English which are produced through methods like laser printing, adhesive-backed stickers, or labels imbued with adhesive substances. This distinction implies that the markings in question were not incorporated during the initial production phase of the UAVs. Rather, they manifest as rudimentary endeavors aimed at masking the Iranian origin of these devices

Lancet

General description

The Lancet stands as a Russian-developed loitering munition engineered for the purpose of neutralizing ground vehicles and assorted targets across both frontal and rear domains. The nomenclature ‘Lancet’ encompasses a comprehensive spectrum of UAVs and their adaptations, brought forth by the Russian enterprise ZALA AERO, a part of the Kalashnikov concern.

Within this classification, the Lancet-3 UAV occupies a notable place, representing the earlier model. A more evolved iteration, the Lancet-3M, emerges as an enhanced version of the kamikaze drone Lancet-3.

A pivotal attribute characterizing the Lancet UAV resides in its aerodynamic configuration, featuring two sets of planes arranged in an ‘X’ formation. This alteration is instrumental in enhancing maneuverability, flight performance, operational range, and speed.

The UAVs are characterized by an inconspicuous radar profile due to their modest dimensions and the prominent incorporation of composite and plastic components in their fabrication. Furthermore, integration of an electric motor diminishes their auditory and thermal signatures.

Key technical features encompass optoelectronic guidance alongside a TV-guided unit, facilitating precision guidance during the final flight phase. These UAVs feature navigation and communication modules capable of deriving coordinates from diverse sources. In the Lancet-3M variant, the UAV can be operated under operator control, autonomous control, or a hybrid mode.

The Lancet's combat configuration is tailored to accommodate both high-explosive fragmentation and cumulative warheads. While the Lancet-3 and Lancet-3M are equipped with standard KZ-6 cumulative warheads, recent adaptations incorporate an additional charge located at the tail, represented by a detonator-equipped plastid.

Operation necessitates deployment of a drone control station in the form of a portable case, coupled with a catapult system to facilitate launch.

Specifics of usage in Ukraine

Reports of Lancet UAVs being employed in Ukraine initially emerged in July 2022. A multitude of videos showcasing successful Lancet operations on the Ukrainian battleground began circulating on the telegram channels of Russian military bloggers and journalists during late October and early November 2022.

Russian occupation forces have progressively integrated Lancet UAVs into their operations against Ukraine. These drones are being used to target critical military assets. Notably, a tactical approach has emerged wherein Lancet barrage drones are employed to strike significant rear targets at depths of up to 40 kilometers. Such tactics involve targeting Ukrainian artillery, anti-aircraft self-propelled guns, tanks, armored personnel carriers, and radars. Moreover, Russian forces have released footage depicting attacks on Ukrainian naval vessels at the onset of the full-scale invasion.

Collaboration is a hallmark of Lancet operations, with these UAVs commonly working in concert with scout drones that identify targets and transmit coordinates.

Recent shifts in Russian UAV strategy involve integrating their usage. This entails deploying Shahed UAVs as a preliminary action, drawing air defense response, followed by the launch of Lancet drones. This strategy aids in identifying air defense emplacements and subsequently conducting targeted strikes.

The frequency of Lancet deployment by Russia has risen notably during the Ukrainian counteroffensive. Notably, instances of Lancet UAVs being deployed against civilian infrastructure have also emerged. An illustrative case is the May 20, 2023 incident, where a Lancet struck an infrastructure facility within the Sloboda district of the Kharkiv region.

Reports emanating from Russian sources suggest a surge in Lancet UAV production. Collectively, these details underscore the escalating threat posed by Lancet unmanned aerial vehicles to Ukraine's security landscape.

Orlan-10

General description

The Orlan-10 unmanned aerial vehicle has become a key asset for the Russian armed forces in Ukraine. These drones are used for reconnaissance, surveillance and suppression of Ukrainian air defense. With production costs ranging from $87,000 to $120,000, significantly less than a cruise missile, so their cost-effectiveness is obvious.

The unmanned vehicle is launched from a special collapsible catapult. The flight is powered by a low-power gasoline engine. The flight speed can range from 75 to 170 kilometers per hour. The Orlan-10 UAV can stay in the air for up to 15 hours, while the maximum distance from the ground control station should not exceed 125 kilometers.

The developer and manufacturer of the Orlan-10 UAV is the Special Technological Center Limited Liability Company (LLC), St. Petersburg.

The adaptability and affordability of the Orlan-10 has prompted the Ukrainian military to prioritize strategies aimed at countering its influence. The drone's flexibility makes it a serious challenge for Ukrainian military operations.

Specifics of usage in Ukraine

Orlan-10 UAV is part of the Unified Tactical Control System, an extremely complex hardware and software system designed to coordinate and harmonize the actions of different types of troops in a particular area. The Orlan-10 UAV is designed to conduct aerial reconnaissance in a designated area to provide targeting guidance to self-propelled artillery systems, tanks, mobile anti-aircraft missile systems and other military equipment equipped with destruction means.

To search for targets and recognize them, the UAV is equipped with various optical devices and thermal imagers. In addition, UAVs can be equipped with electronic warfare or radio reconnaissance equipment. Radio reconnaissance equipment is capable of accurately determining the coordinates of any source of electromagnetic waves. Orlan-10 can also detect "cellular user terminals" (i.e., cell phones) and disrupt the connection.

For the purpose of reconnaissance of rear positions, Orlan-10 can be used in autonomous mode, when the drone flies along a given route using GPS coordinates and records to the internal memory.

III. Description of Components

In our study, we carefully examined a comprehensive selection of 174 components recovered from Shahed 136/131, Lancet, and Orlan-10 drone models found in the Ukrainian battlefield.

Clearly, the Russian military continues to rely on foreign-made components, with a particular focus on microelectronics. This dependence remains noticeable despite attempts at import substitution.

Our analysis suggests that the vast majority – 69% - of the components studied come from U.S.-owned companies (*see full table in the Appendix 1*).

Figure 1: Producers of the Imported Critical Components in Russian UAVs

Source: KSE Institute

Our investigation has identified a selection of pivotal electronic components that exhibit a degree of indispensability, rendering their replacement with analogs a formidable task.

The crux of the challenge lies in the accessibility of these components, with a substantial portion being readily obtainable through publicly accessible channels. Commercial resources and platforms, including well-known marketplaces like AliExpress and Alibaba, serve as conduits through which these components can be procured with relative ease, devoid of any stringent end-user validation mechanisms. This accessibility introduces a complex dynamic, wherein critical technological components are readily available for acquisition, raising pertinent concerns related to the oversight and regulation of such transactions.

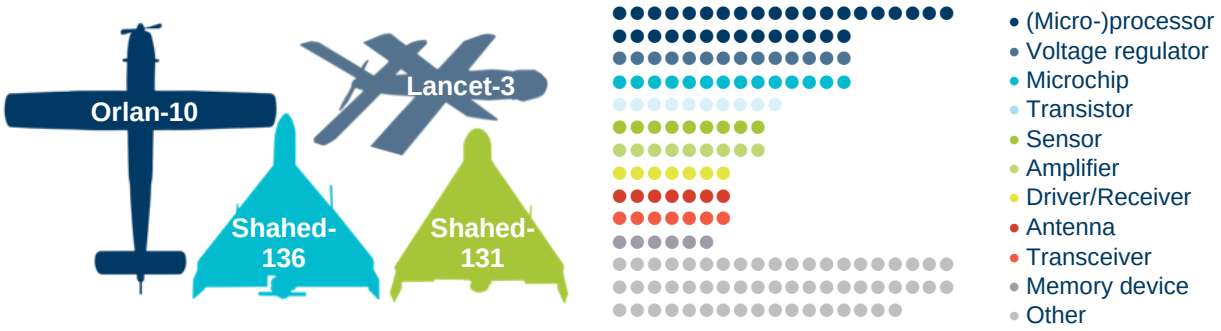
The Most Important Components Used for Russian UAV Production

Traditionally, microelectronics has been the leading foreign component of Russian military equipment. Such components are the most critical and hard to replace.

On the Figure 2 the components of Orlan-10, Lancet-3, and Shahed-136/131 are presented (each dot represents one component). The leading role in these sample of components are processors and microprocessors. Their share is 20% of total selection of 174 components. There are also voltage regulators (8%), microchips (8%), transistors (6%) and other electronic components.

In addition to electronics, components such as an engine, cooler, and others were found.

Figure 2: Components of UAVs



Source: KSE Institute

Microprocessors

UAV microprocessors generally contain both an FPGA (Field Programmable Gate Array) and an ARM Cortex-A9 processor. One of the possible uses of this microprocessor is to process video data coming from UAV cameras. The microprocessor can perform a variety of functions, such as object detection, object tracking, face recognition, real-time image processing, etc.

In addition, the microprocessor can be used to process data from other sensors that may be installed on the UAV, such as GPS, gyroscope, accelerometer, etc. Using this data together with video data, the microprocessor can implement additional functions such as automatic target acquisition, flight path correction, flight stability, etc.

In Lancet, Xilinx microprocessor is used. Shahed 136/131 uses STMicroelectronics.

GLONASS-enabled modules

A pivotal element within UAVs is the navigation system, integral in ensuring precise positioning and orientation during flight. This system empowers UAVs to adhere to designated routes, track targets, facilitate takeoff and landing, and circumvent obstacles. Its role extends to enhancing safety, reliability, and autonomy, enabling complex missions across diverse environments.

The GLONASS (Global Navigation Satellite System) stands as Russia's satellite navigation system, furnishing worldwide civilian signals and free navigation services. Its heightened accuracy, geared for specialized applications, relies on microchips sourced from foreign manufacturers.

In the context of UAVs operating within Ukrainian territory, the Lancet UAVs were outfitted with U-blox navigation information receivers.

Several foreign companies remain actively engaged in producing GLONASS-enabled modules, encompassing entities such as Linx Technologies, Broadcom, Qualcomm, Telit, Maxim Integrated, TRIMBLE, Cavli Wireless, STMicroelectronics, Sierra Wireless, NovAtel, Septentrio, and Antenova.

However, a crucial step toward curbing the utilization of GLONASS modules in Russian UAVs involves international companies ceasing the production of chips supportive of GLONASS

navigation technology. Such a measure carries the potential to significantly impact the landscape of navigation technology within Russian UAVs.

It is important to highlight that one of the reasons the Russians can adjust their technology is because they can switch out components and are flexible with circuit board layouts. This adaptability is made possible through software used to design these circuit boards, which is also provided by the companies from sanctions coalition countries.

This flexibility in design is especially significant when it comes to devices that have features like GLONASS. These devices need careful arrangement of parts to prevent signals leakage. The process of designing and planning these circuit boards, including using computer simulations to test them, is a major factor that enables the creation of such adaptable layouts for Russian technology.

Electric engines

The use of electric motors in UAVs plays an important role in ensuring high performance and low visibility, which allows for efficient operations and reduces the UAV's vulnerability.

This important component is also imported by Russian UAV producers. For example, Lancet UAV engine bore the markings of the Czech company Model Motors. Model Motors specializes in the production of high-quality engines and accessories for model aircraft.

According to the information received, the only company that has imported Model Motors engines to Russia since the large-scale invasion of Ukraine is Legion Komplekt LLC. The possible route of shipment of Model Motors goods to Russia is through Lithuania, using intermediaries related to Russia.

In addition, one of the main suppliers of components for the Lancet manufacturer, OMP LLC, has imported engines manufactured by the Chinese companies Jiangxi Xintuo Enterprise Co. Ltd, Hefei Huanxin Technology Development Co. Ltd, Foshan Shunde Green Motor Technology Co. Ltd.

Other components

Analysis of deployed Lancet UAV samples in Ukraine underscores their reliance on printed circuit boards with foreign-made electronic components. These boards, pivotal to UAV functionality, are composed of materials such as photoresist and foil fiberglass. Additionally, the construction employs carbon fiber fabric, enhancing the drones' structural integrity. Restricting their supply to Russia would disrupt the production of microelectronics and the supply of basic components for UAVs and other weapons.

Machinery and equipment

According to available information, the following CNC machines may be used in the new production of Iranian UAVs:

- Grinding OGC-1240, iMachine, TopKing, (Taiwan)
- Grinding PSGC-1240, Proth (Taiwan)

The following equipment can be used for this purpose:

- OLDENG dispensing furnaces (Russia)

- Casting furnaces OLDENG C300D, C480D, C600D (Russia)
- Lathe iMachine G-207 (Taiwan)
- Turning and milling machine CHIAH-CHYUN CT2-52YM (Taiwan)
- CHIAH-CHYUN CT2-52Y2M turning and milling centre (Taiwan)
- Milling Dekay LS500 (China)
- Dekay SG650 milling machine (China)
- Dekay SG870 milling machine (China)
- Milling machine Dekay FA400 (China)
- Milling Dekay FA630 (China)
- AMS Tech AD6L (head office in Germany)

According to a report by the Russian propaganda TV channel Rossiya-1, the Lancet UAV components are manufactured using equipment from the Swiss company Essemtec, which specializes in the production of electronic assembly and manufacturing equipment. The company develops and manufactures automatic component placement systems (SMT machines), equipment for printing boards, soldering systems, dosing modules and other equipment required for electronics production.

It is imperative to curtail supplies from these companies to Russia to prevent potential escalation in its production capabilities. Moreover, these companies might furnish spare parts to previously acquired machinery, warranting careful consideration to impede unintended augmentation in Russia's production capacity.

In this regard, it is important to impose sanctions on companies that supply the relevant goods to the Russian Federation, as well as to constantly monitor compliance with export restrictions on the supply of the relevant goods.

IV. Critical Components Trade Investigation

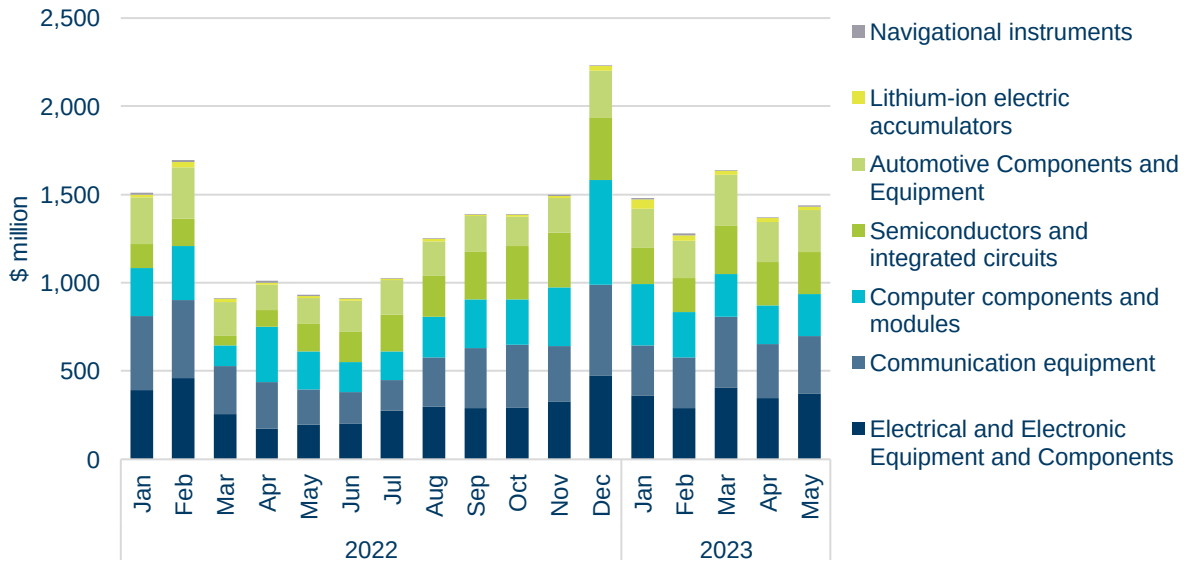
In this study, we focused on Harmonized System (HS) codes (on 4-digits and 6-digits level) associated with components found in Russian UAVs. Using trade data, we analyzed trade patterns associated with these components.

Our investigation revealed a stabilization in trade volumes after the downfall at the beginning of the full-scale invasion during the third quarter of 2022, followed by a subsequent period where trade volumes were at a fairly steady level. Total amount of these transactions amounted **$7.2 billion** for the period from January to May 2023, which is 19% higher from the similar period in 2022 (**$6.1 billion**). In 2022, the total amount was **15.8 billion**.

Notably, a surge in trade volumes observed in December 2022 can be attributed to two key factors:

- **Preparation for intensive military operations**: The heightened trade activity aligns with the period leading up to intensified military operations, indicating a correlation between trade patterns and impending military endeavors.
- **Peak in consumer spending**: Additionally, the surge in December trade could be attributed to heightened consumer spending, as certain components have potential applications in civilian goods.

Figure 3: Imports of Critical Components by Type



Source: KSE Institute

Within the investigated subset of goods, there are following groups of components:

- **Electrical and electronic equipment and components:** share of **24%** of total trade amount for the period 2022 – 5m 2023. This group consists of electrical transformers, static converters, capacitors, resistors, switches, relays, and other components.
- **Communication equipment:** constitutes **23%** of the analyzed subset. This category includes electrical devices for telephony or telegraphy (excluding usual smartphones for the purpose of focusing on goods, which can be used for military production), radar,

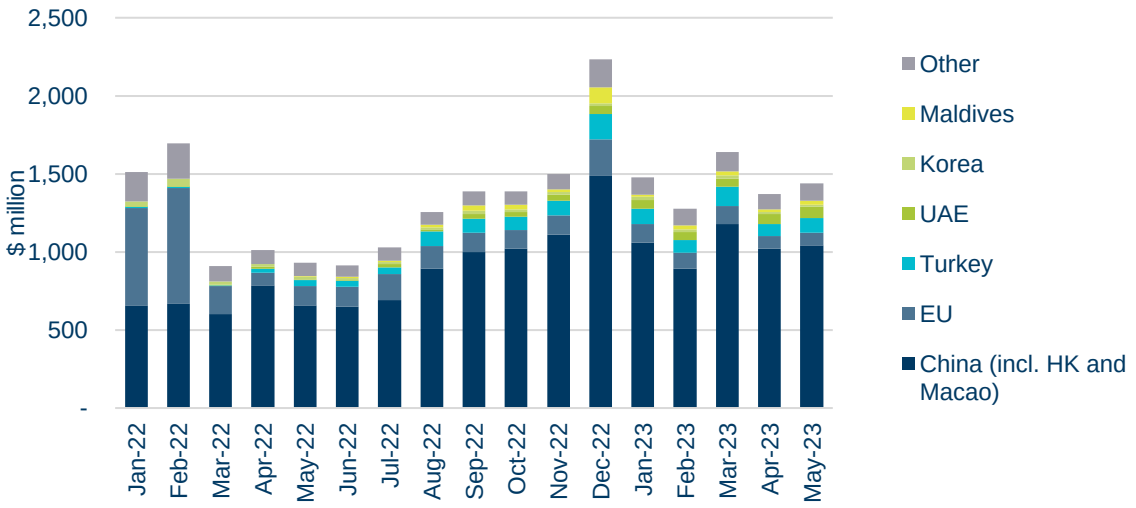
radio navigational aid and radio remote control devices and spare parts, video, and audio recorders and other.

- **Computer components and modules:** a significant **20%** share is attributed to computer components and modules, representing automatic data-processing machines and units and spare parts
- **Semiconductors and integrated circuits**: This category, encompassing semiconductors and integrated circuits, amounting to 16% of the examined subset.

China emerges as the primary conduit for the supply of critical components, accounting for an extensive portion of deliveries to Russia. Since the commencement of the full-scale invasion, China contributed to 67% of these foreign components, with a noteworthy subset of 17% channeling through Hong Kong. Moreover, Turkey and the United Arab Emirates have gained prominence as pivotal sources of components for Russia, contributing 5% and 2%, respectively.

After the full-scale invasion, the European Union (EU) has experienced a notable reduction in its trade engagement with Russia. However, even amid these changes, the EU maintains a discernible presence, accounting for 14% of the trade share. It should be noted that significant volumes of trade pass through the Eurasian Customs Union, encompassing Kazakhstan, Kyrgyzstan, and Armenia. However, it's important to highlight that detailed data concerning this specific trade route remains unavailable within our analyzed trade dataset.

Figure 4: Imports of Critical Components by Country of Delivery



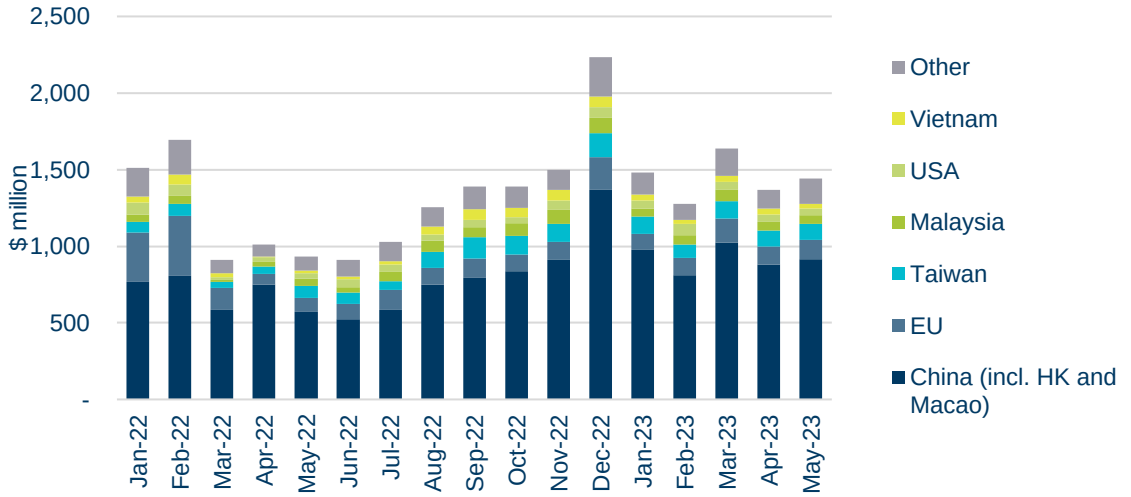
Source: KSE Institute

If we delve into the country of origin of these components, we see that China also plays a leading role. Roughly 60% of the goods studied originate in China, including 3% goods produced in Hong Kong. If we compare imports by country of delivery and origin, we see that goods of Chinese origin comprise only 85-90% of what was delivered from China. So Chinese intermediaries play a significant role in the transfer of critical components to Russia.

In addition, there is a noticeable trend whereby numerous US and EU companies have set up production facilities in China. As a result, a significant portion of components originating in China is actually under control of the entities from sanctions coalition countries.

As for the origin from the European Union and the United States, the share is 11% and 4%, respectively. However, as already mentioned, these figures do not provide a comprehensive representation of the share of companies from these countries, as many of them have production facilities in different Asian countries. Figure 5 shows that Taiwan, Malaysia, and Vietnam play an important role in component manufacturing (7%, 4% and 3% respectively).

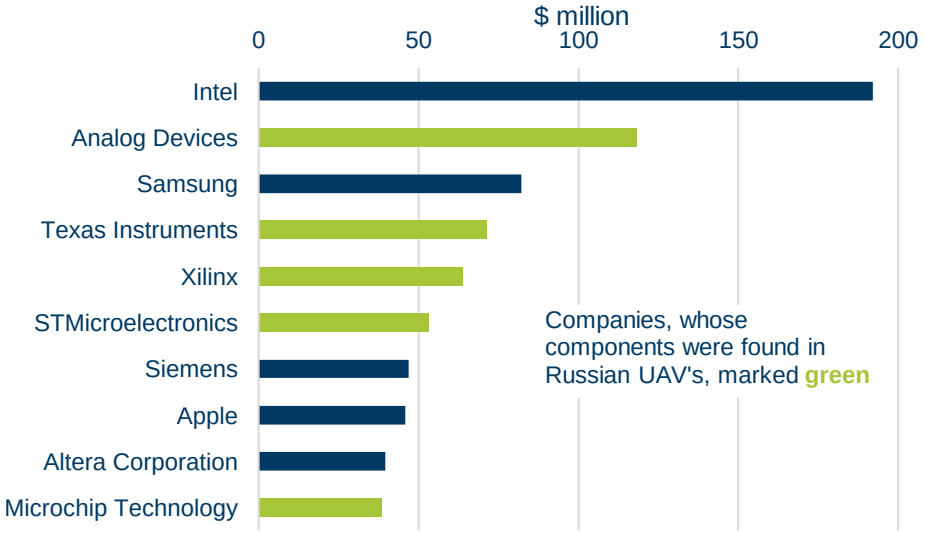
Figure 5: Imports of Critical Components by Country of Origin



Source: KSE Institute

For the past five months of 2023, top producers of the investigated components were: Intel ($192 million), Analog Devices ($118 million), Samsung ($82 million), Texas Instruments ($71 million) and Xilinx ($64 million). Components produced by 5 of these top 10 manufacturers were found in Russian UAVs. Also, Intel, Samsung and Intel's subsidiary Altera Corporation produced components, which were found in other Russian military equipment. Siemens produced machinery and equipment, which is used by Russia in military production, and spare parts for it.

Figure 6: Top-10 Producers of Critical Components in Import for 5m 2023



Source: KSE Institute

V. Sanction Evasion Practices

The electronic components from countries of the sanctions coalition used in UAVs reach Russia mainly through intermediary countries that are not subject to these sanctions. Moreover, in response to the escalation of sanctions and strategies aimed at preventing the circumvention of sanctions, Russia is actively stepping up measures to conceal its procurement, including:

- **Use of illegal networks:** Illegal networks, sometimes controlled by personnel with ties to intelligence services, are used as distribution channels**.**
- **Concealment of customs data:** Efforts are made to hide the name of the product in the customs data. This may include using vague descriptions, providing inaccurate details, or lack of documentation of border crossings.
- **One-day shell companies:** Procurement endeavors involve the frequent creation and alteration of short-lived shell companies.
- **Proliferation of intermediary entities:** The intermediary layer between manufacturers and Russian recipients is expanding, sometimes encompassing a multitude of entities.
- **Diversification of suppliers:** Entities not previously involved in supplying electronic components are now enlisted for procurement.
- **Fake transit operations:** Goods crossing the Russian border purportedly on their way to other countries, such as Kazakhstan, never reach a final intended buyer. Instead, the goods end up in Russia.

These multifaceted tactics underscore the dynamic nature of Russia's response to sanctions, reflecting a comprehensive strategy to sidestep the sanctions framework.

Circumvention of sanctions is increasingly prevalent due to several factors, including:

- **On-production:** A substantial portion of crucial components is manufactured beyond the borders of countries within the sanctions coalition. Companies based in these countries may relocate production, often to regions like Central Asia. This maneuver ensures that goods remain within non-sanctioned boundaries, sidestepping the export controls of coalition nations.
- **Challenges in definition of sanctioned goods:** The complexity in defining sanctioned goods arises from the specificity of dual-use goods lists, which focus on detailed subtypes rather than comprehensively sanctioning entire categories. This situation can be exploited by companies to export goods resembling but not explicitly banned, exploiting the lack of rigorous verification measures.
- **Insufficient compliance procedures:** The absence of a defined standard for adequate compliance procedures poses a challenge. Companies are left to determine their own sufficiency, potentially resulting in circumvention of sanctions due to the lack of accountability for inadequate compliance measures. Clear guidance with assistance in implementation of these procedures could help companies to implement effective procedures.
- **Slow reaction:** The delay in investigating and sanctioning companies and individuals involved in the military industry has a cascading effect. This delay allows Russia to develop alternative methods of circumventing sanctions and mitigating the impact of new restrictions on the supply of critical components. As a result, the effectiveness of the sanctions is reduced due to the evolution of strategies used by sanctioned entities.

VI. Policy Recommendations

Our findings reveal that Russia's ongoing imports of critical components reflect distinct challenges within the export controls regime:

- **Sanctions violations by coalition entities:** Entities within coalition jurisdictions are implicated in sanctions violations, engaging in activities that breach legal bounds.
- **Sanctions circumvention by coalition entities:** Entities under coalition jurisdictions employ legal activities that, while within the law, undermine the sanctions regime's objectives.
- **Third-country involvement in violations/circumvention:** Entities beyond coalition jurisdictions, i.e., third-country actors, contribute to violations and/or circumvention of sanctions.
- **Certain goods are still not covered by export controls:** As a result, Russian imports of some critical components do not in all cases represent sanctions violations and/or circumvention.

It is also worth noting that the sanctions system is currently very complicated, which prevents the authorities from having full control over the implementation of such sanctions.

Despite the imposition of sanctions on the sale of dual-use goods to Russia in 2014, the mechanisms governing their operation remain inadequately established and warrant substantial improvement. We consider that the implementation of the changes described below will significantly limit Russia's ability to obtain the necessary components for the production of military equipment.

Alignment of sanctions across the sanction coalition

Aligning of the sanctions lists

The Russian military complex encompasses approximately 1500 diverse enterprises. Evidently, the sanctions imposed by coalition countries have not comprehensively addressed this extensive network. Many crucial industry enterprises remain either partially sanctioned or entirely unaffected. Addressing this requires unifying sanctions lists among countries and extending them to encompass additional companies identified as producers, developers, or suppliers of military production components.

The lists of dual-use goods are now better aligned among the countries of the sanction's coalition, but nonetheless have some differences. A centralized approach to the formation of dual-use goods lists will facilitate better regulation of critical components supplies. The same goods should be classified as "dual use" in all countries and criteria for licensed approval should be standardized. In addition, it is critical that authorities define dual-use goods based on Harmonized System (HS) codes; otherwise, the monitoring of transactions will be significantly more challenging.

Improve cooperation

To enhance enforcement, improved information exchange is vital. Comprehensive and timely transaction data, especially for sensitive trade involving critical military or dual-use components, should be shared among coalition countries. Customs services' data from coalition and third countries, accessible directly or through platforms like Export Genius, should be efficiently shared. Setting up effective information-sharing systems, including with academic and think tank communities, is crucial.

Countries should collaborate in investigating sanctions violations or circumvention. Given the multi-jurisdictional nature of transactions with critical components, joint investigations among coalition countries can prevent supplying critical components to unreliable partners. This may also lead to an increase in the pace of sanctions enforcement, making it more difficult for Russia to adapt to changes and seek workarounds. Authorities must proactively monitor developments, leveraging all available data sources, to identify evolving schemes in response to restrictions.

Broader export controls

Expanding sanctioned product categories

The current approach often targets specific products, leaving similar products unregulated, potentially enabling customs evasion. This loophole allows for the misclassification of goods in customs declarations based on limited physical inspection. In addition, in-depth knowledge is required to distinguish controlled from non-controlled goods, which complicates enforcement.

As mentioned above, the use of broader categories of goods, based on HS codes, can simplify the restriction of supply of such goods to Russia. We suggest establishing dual-use goods classification at the 6-digit HS code level. This approach broadens the range of controlled items. Additionally, 6-digit codes are unified across countries, in contrast to more detailed level of classifications.

The list of dual-use goods should be reviewed and updated regularly, in order to include any goods, important for Russian military production, immediately when they were identified.

Elimination of the Exceptions

Exceptions, such as for Rosatom, create certain difficulties. Approval of exports of critical components to Russia for any purpose could lead to redirection to support the war effort, reducing the effectiveness of controls.

Better Control of Civil Goods

According to the concept of dual-use goods, these products can be used both for military purposes, as well as civil uses. This leads to the fact that dual-use goods are easily available on marketplaces, where there are no customers verification and control over the subsequent use of goods. We suggest withdrawal of such components from any open marketplaces, to avoid the circumvention of export controls.

Export Trend Quotas

Another consideration is the use of export quotas. This mechanism stipulates that if a company has sold an average of 5,000 units to Turkey between 2017 and 2022, then if the same company plans to sell 50,000 units to Turkey in 2023, it will be subject to a thorough audit and due diligence. The rationale for this measure is that it can limit the percentage of these goods that can be allowed for further sale to third countries. Such precautions are taken to prevent shortages of these goods for domestic consumption.

Stop Production for Russia

Russian military equipment relies heavily on navigation, especially through the integration of GLONASS into modern weapons. Some Western firms continue to produce GLONASS-enabled microelectronics. Given its exceptional military utility for Russia, these companies should be forced to cease production.

Improve companies' compliance

Increase collaboration between companies and authorities

Collaboration between authorities and critical component producers for the Russian military industry could enhance sanctions compliance and bolster new measures. Information and experience exchange can amplify effectiveness.

Numerous major companies possess robust risk management and compliance systems to mitigate inadvertent export control breaches. The results of the internal investigations can be utilized on the governmental level to extend the sanctions lists.

Make clear guidance

While some companies implemented sufficient compliance procedures on the workplace, others, especially small-and-medium enterprises, lack the resources and experience to do so. While most of the manufacturers of the components found in Russian UAVs are large multinationals that obviously have the resources to conduct proper compliance procedures, they may also cooperate with smaller distribution companies. Therefore, clear compliance guidance should be developed and approved as obligatory for all manufacturers and distributors. Authorities should also provide technical assistance to the companies on implementation of the compliance principles.

Companies would also benefit from the setting-up of a database through which they can access information about potential business partners, including company structures, ownership, related parties, coverage by sanctions and/or information about previous violations. Providing easily accessible database can make compliance more affordable for companies and increase a quality of compliance procedures.

Furthermore, implementation of the guidance would increase accountability. In case of any sanction's violation detection, authorities can verify proper compliance procedure execution. Conversely, companies can defend itself, by retaining the documentation of the compliance procedures performed.

The guidance should undergo periodic reviews and updates, incorporating new controls informed by the latest intelligence on sanction evasion.

Increase the responsibility

Publicly, companies have a strong incentive to avoid linking their products to Russian weapons on the battlefield or being used in attacks on Ukrainian civilians. Our findings emphasize that many critical components available to Russia are produced by Western companies that may not be conducting sufficient due diligence on goods subject to export controls. Therefore, we argue that authorities should demonstrate their commitment to preventing and prosecuting violations by conducting investigations involving well-known companies.

As mentioned earlier, the implementation of explicit procedures and more rigorous documentation requirements is essential. This approach allows for a distinct determination of whether a company has taken adequate measures to prevent the trade of critical components with Russia. Consequently, responsibility can be established. This framework delineates that while a company may not be fully responsible for the entire flow of its goods, it is accountable for adhering to the compliance procedure.

In order to prove company's responsibility in the supply of components for Russian military production, mandatory tamper-evident serial numbers or ID technologies could be introduced. Serial numbers should be protected from deliberate damage, as Russian manufacturers often attempt to hide the origin of components by damaging any identifiers.

Implementation of the same controls in foreign production facilities

Companies must ensure that their products are subjected to the same regulatory oversight, regardless of whether they were manufactured outside of countries within the sanction's coalition. This will help to address the issue with on-production.

Using existing institutions and frameworks

Utilizing AML framework

The schemes used to violate or bypass sanctions, including export controls, mirror those seen in money laundering and proliferation, featuring opaque ownership structures and frequent changes of structures and actors involved. Utilizing the existing Anti-Money Laundering (AML) framework, coalition authorities can enhance enforcement efforts, extending its application to export controls. This framework is particularly valuable for tracing structures in third countries pivotal to both military input production and exports to Russia, especially if production is located outside of the sanction's coalition.

Financial sector

Financial sector sanctions can serve as a crucial enforcement mechanism, effectively supporting various restrictions. By targeting Russian banks and limiting payment channels for imports, stricter monitoring of specific transaction patterns becomes possible. Companies must disclose information to banks regarding payments linked to shipments of goods potentially under export controls.

Authors

Note: The inclusion of affiliations is for identification purposes only and does not represent an endorsement of shared views with the co-signer. The lead authors of this paper were Olena Bilousova, Agiya Zagrebelska, Vladyslav Vlasiuk, and Nataliia Shapoval.

Olena Bilousova, Strategy Consultant on Defense Industry Sanctions, Kyiv School of Economics.

Agiya Zagrebelska, Head of the NACP sanctions direction.

Bronte Kass, Program Manager, Freeman Spogli Institute for International Studies (FSI), Stanford University; Assistant Coordinator, International Working Group on Russian Sanctions.

Michael McFaul, Director, Freeman Spogli Institute for International Studies (FSI), Professor of Political Science, and Hoover Institution Senior Fellow, Stanford University; Coordinator, International Working Group on Russian Sanctions.

James Hodson, AI Researcher, CEO at AI for Good Foundation

Vladyslav Vlasiuk, PhD, Secretary of Ukrainian Working Group on Russian Sanctions.

Natalia Shapoval, Vice President for Policy Research, Kyiv School of Economics.

Appendix 1. Manufacturers of the Components Found in Russian UAV's

Manufacturer	Number of types of ECBs and components			
	Shahed-131	Shahed-136	Lancet	Orlan-10
AMPRO COMPUTERS INC (USA)		1		
Analog Devices (USA)	5	6	6	3
Atmel (USA)			2	
AVX Corporation (USA)			1	
Brushless fan (China)	1			
Cirocomm (Taiwan)				4
CTS Corporation (USA)	1	1		
Delta Electronics, Inc (Taiwan)	1			
Fairchild Semiconductor (USA)	1			
Glenair (USA)		1		
Gumstix (USA)				3
Hemisphere GNSS (USA)	4	3		
HiTec (USA)	1			
Hittite Microwave Corporation (USA)	1	1		
International Rectifier (parent company Infineon Technologies AG) (USA, Germany)	2	2	1	
JST (Japan)				4
Marvell Technology (USA)		1	1	
Maxim Integrated Products (USA)	2	1		
Micrel Semiconductor (USA)		1		
Microchip Technology Inc. (USA)	1	3	1	3
Micron Technology (USA)	1	1	1	2
Murata Manufacturing Co., Ltd (Japan)	2	4		
New Jersey Semiconductor Products Inc. (USA)	1	1		
NXP Semiconductor (Netherlands)	2	1		2
ON Semiconductor (USA)		1		
Panasonic Semiconductor (Japan)	1			
Pulse Electronics Corporation (USA)				1
Qorvo (USA)				6
Renesas Electronics (Japan)				1
RN2 Technologies (Korea)				1
ROHM Semiconductor (Japan)		1		
Saito Seiaskusho (Japan)				1
SanDisk Corporation (USA)				1

Semtech Corporation (USA)				1
SIMCom Wireless Solutions (China)				1
SMC Diode Solutions (parent company Sensitron Semiconductor) (USA)		1		
SPANSION (USA)	1			
Spreadtrum (China)	1			
STMicroelectronics (Switzerland)	4	2	1	1
System Logic Semiconductor (South Korea)	1			
Tai-Saw Technology (Taiwan)				1
Tallysman (Canada)	1	1		1
TDK Corporation (Japan)				1
Texas Instruments (USA)	12	19	3	2
Ti Automotive Gmbh (parent company of TI Fluid Systems) (Germany, United Kingdom)		1		
Token Electronics Industry Co (Taiwan)	1			
Traco Power (Switzerland)				1
U-BLOX (Switzerland)	1	1		3
VBsemi Electronics Co., Ltd (China)		1	1	
Vishay Intertechnology (USA)	1			
Winbond (Taiwan)	1	1		
Xilinx Inc. (USA)	1		1	2
Total	**52**	**57**	**19**	**46**

Appendix 2. Legal Entities Involved in the Production and Supply of UAVs and Components

	Company	ID	UA	EU	UK	US	CA	CH	AU	JP	NZ
Companies involved in the development, production and supply of Shahed UAVs to Russia											
1	Iran Aircraft Manufacturing Industrial Company (HESA) - manufacturing Shahed 136/131		✓	✓	✗	✓	✓	✓	✗	✗	✗
2	Shahed Aviation Industries Company - development Shahed 136/131		✓	✓	✓	✓	✓	✓	✓	✗	✓
3	Oje Parvaz Mado Nafar Company - production of engines for Shahed 136/131	10590042155	✗	✓	✓	✗	✗	✓	✓	✗	✓
4	Paravar Pars Company - research, development and production Shahed-171	10101373495	✓	✓	✓	✓	✓	✓	✓	✗	✓
5	Design and Manufacturing of Aircraft Engines - procurement of components for UAVs and jet engines, research, development and production of Shahed-171	DAMA, 14005160213	✓	✓	✓	✓	✓	✓	✓	✗	✓
6	Baharestan Kish Company - production of components for Shahed	10861531217	✓	✗	✗	✓	✓	✗	✗	✗	✗
7	Safiran Airport Services - Coordination of air cargo transportation from Iran to Russia, including the delivery of UAVs, personnel, and equipment		✓	✗	✗	✓	✓	✗	✓	✗	✗
8	Kimia Part Sivan Company - improvement of combat UAV programs, flight testing of UAVs, technical support and procurement of components for UAV production. The company's specialists could have been in the temporarily occupied Crimea to conduct flight tests of the UAVs supplied to Russia	10320661315	✓	✗	✗	✗	✗	✗	✗	✗	✗
9	Iran Aviation Industries Organization - manages the military aviation industry of Iran, subordinated to the Ministry of Defense and Logistics of the Armed Forces of Iran		✓	✗	✗	✗	✗	✗	✗	✗	✗
10	Sharif University of Technology- development and design of UAVs		✓	✗	✗	✗	✗	✗	✗	✗	✗
11	Qods Aviation Industry Company - design and development Mohajer-6	14005441856	✓	✗	✗	✗	✗	✗	✗	✗	✗
12	Success Aviation Services FZC - an air transportation company that cooperated with the Iranian company Safiran Airport Services to coordinate flights between Iran and Russia, including flights that transported UAVs, personnel and related equipment	OAE, 16039	✓	✓	✗	✓	✗	✓	✗	✗	✗
13	I Jet Global DMCC- an air transportation company that cooperated with the Iranian company Safiran Airport Services to coordinate flights between Iran and Russia, including flights that transported UAVs, personnel and related equipment.	OAE, DMCC19501	✓	✓	✗	✓	✗	✓	✗	✗	✗
14	Pardazan System Namad Arman- the company is involved in circumventing sanctions and supplying electronic components for Iran's UAV program		✗	✗	✗	✓	✗	✗	✗	✗	✗
15	Pouya Air - is an Iranian airline that is part of the IRGC. The company's planes are likely to be involved in the transportation of UAVs, personnel and related equipment from Iran to Russia		✓	✗	✗	✗	✗	✗	✗	✗	✗
16	223 Flight Unit - a part of the Russian Ministry of Defense, the boards are likely to be involved in the	5050017062	✓	✗	✗	✓	✗	✗	✗	✗	✗

	transportation of UAVs, personnel and related equipment from Iran to Russia										
17	The 924th Unmanned Aerial Vehicle Center (Military Unit 20924) - the center's personnel were sent to Iran for training in the use of Iranian UAVs. The centre was directly involved in the transfer of Iranian UAVs to Russia	5022050639	✗	✗	✗	✓	✗	✗	✗	✗	✗
18	Sarmad Electronics Sepahan Co. - The Iranian company, among other things, produces flow metres used in the Shahed-131		✗	✗	✗	✗	✗	✗	✗	✗	✗
Companies involved in the development, production and supply of Lancet UAVs to Russia											
1	CST LLC - main legal entity of ZALA AERO; manufacturer of UAV Lancet	1841015504	✓	✓	✓	✗	✗	✗	✓	✗	✗
2	Representative office of CST LLC in the Republic of Kazakhstan	191242001693	✗	✗	✗	✗	✗	✗	✗	✗	✗
3	Scientific and Technical Centre Orion LLC is one of the main suppliers of CST LLC, owned by Zakharov's daughter Maria. The main activity is software development, creation of new communication tools and research in the field of artificial intelligence, neural networks and machine learning	9715302790	✗	✗	✗	✗	✗	✗	✗	✗	✗
4	RTK LLC is owned by Zakharov's son Nikita. The company's principal activity is computer software development	9715415169	✗	✗	✗	✗	✗	✗	✗	✗	✗
5	Aeroscan LLC is one of the main suppliers of CST LLC. The main activity is aerial photography, airborne laser scanning, remote sensing services	5603045794	✓	✗	✗	✗	✗	✗	✗	✗	✗
6	EDS LLC The company's main activity is computer software development	9715315319	✗	✗	✗	✗	✗	✗	✗	✗	✗
7	OMP LLC is a supplier of components and electrical equipment for CST LLC	5403049953	✗	✗	✗	✗	✗	✗	✗	✗	✗
8	Hartis DV LLC is a supplier of components and electrical equipment for CST LLC	7733753978	✗	✗	✗	✗	✗	✗	✗	✗	✗
9	ID Solution LLC - supplier of components and accessories for CCT LLC	5003091492	✗	✗	✗	✗	✗	✗	✗	✗	✗
10	MVizion LLC (Uzbekistan) is a supplier of components and electrical equipment to ID Solution LLC, which is a supplier to CST LLC	309644860	✗	✗	✗	✗	✗	✗	✗	✗	✗
11	LLC Spel – supplier of components for LLC CST	7801339983	✗	✗	✗	✗	✗	✗	✗	✗	✗
Companies involved in the development, production, and supply of Orlan-10 UAVs to Russia											
1	Special Technology Centre LLC develops and produces Thorn-8P radio control equipment, Leer-3 electronic warfare systems and a number of UAVs, including Orlan-10	7802170553	✓	✓	✓	✓	✓	✓	✗	✓	✗
2	Kazan Plant "Electric Device" OJSC specializes in the development and production of sensors, electronic equipment, DC motors, etc. for aircraft of all types. It also produces attachments and a gyro-stabilized platform for Orlan-10 UAVs.	1655064494	✓	✗	✗	✗	✗	✗	✗	✗	✗
3	LLC "STD-Radix" specializes in the production of automatic regulation and control equipment, develops and manufactures optoelectronic systems and software for Orlan-10 UAVs	7720790926	✓	✗	✗	✗	✗	✗	✗	✗	✗

4	JSC "VNIIR-PROGRESS" produces small-sized interference-proof satellite navigation receivers/antennas "Kometa" for UAVs "Orlan-10"	2130094170	✓	✗	✗	✗	✗	✗	✗	✗	✗
5	The Federal State Budgetary Institution of Science "Institute of Theoretical and Applied Electrodynamics of the Russian Academy of Sciences" develops radio-absorbing and finishing coatings for the Orlan-10 UAV	7713020549	✗	✗	✗	✗	✗	✗	✗	✗	✗
6	Limited liability company "Smt-ilogic" importing foreign-made components and materials and supplying them to manufacturers of Orlan-10 UAVs and other aircraft	7804552300	✓	✗	✓	✓	✓	✓	✗	✗	✗
7	NVS Technologies AG produces satellite navigation receivers and antennas. Its products are supplied through a number of intermediaries to the manufacturers of the Orlan-10 UAV.	CH-112.162.851.	✗	✗	✗	✗	✗	✗	✗	✗	✗
8	JSC "Navis Group" specializes in the import of navigation equipment components and their supply to the manufacturers of the Orlan-10 UAV.	7730671533	✗	✗	✗	✗	✗	✗	✗	✗	✗
9	LLC "NVS Navigation Technologies" is a subsidiary of the abovementioned Navis Group	7730637821	✓	✗	✗	✗	✗	✗	✗	✗	✗
10	JSC "Navis-electronics" is a subsidiary of the abovementioned Navis Group	7730702460	✓	✗	✗	✗	✗	✗	✗	✗	✗
11	IK Tech Corporation is a shell company owned by a Russian citizen that was engaged in the purchase of electronic components		✗	✗	✗	✗	✗	✗	✗	✗	✗
12	GeoSat is a shell company owned by a Russian citizen that was engaged in the purchase of electronic components		✗	✗	✗	✗	✗	✗	✗	✗	✗
13	LLC "Device Consulting" was involved in a shadow scheme for the purchase of foreign components		✓	✗	✗	✓	✓	✓	✗	✗	✗
14	Asia Pacific Links Limited is a supplier of components and electrical equipment for Orlan-10, responsible for near 25% of purchases	2182045	✓	✗	✗	✗	✗	✗	✗	✗	✗
15	Xinghua Co. Ltd is a supplier of components and electrical equipment for Orlan-10	110108012686211	✗	✗	✗	✓	✗	✗	✗	✗	✗
16	Sinno Electronics Co. Ltd is a supplier of components and electrical equipment for Orlan-10		✓	✗	✗	✓	✗	✗	✗	✗	✗
17	LLC "Ultran Electronic Components" imports electronic components from manufacturers that can be used in Russian weapons	7802669110	✓	✗	✗	✗	✗	✗	✗	✗	✗
18	RG SOLUTIONS LIMITED is a Hong Kong shell company owned by Russian created for import of critical components		✗	✗	✗	✗	✗	✗	✗	✗	✗
19	NeWay Technologies Ltd is a Hong Kong shell company owned by Russian created for import of critical components		✗	✗	✗	✗	✗	✗	✗	✗	✗