SILICON LIFELINE

WESTERN ELECTRONICS AT THE HEART OF RUSSIA'S WAR MACHINE

JAMES BYRNE, GARY SOMERVILLE, JOE BYRNE, JACK WATLING, NICK REYNOLDS AND JANE BAKER

AUGUST 2022

DISCLAIMER

This document has been prepared by RUSI for informational purposes only (the 'Permitted Purpose'). While all reasonable care has been taken by RUSI to ensure the accuracy of material in this report (the 'Information'), it has been obtained primarily from fieldwork in Ukraine and open sources and RUSI makes no representations or warranties of any kind with respect to the Information.

You should not use, reproduce or rely on the Information for any purpose other than the Permitted Purpose. Any reliance you place on the Information is strictly at your own risk. If you intend to use the Information for any other purpose (including, without limitation, to commence legal proceedings, take steps or decline to take steps or otherwise deal with any named person or entity), you must first undertake and rely on your own independent research to verify the Information.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of any of the Information by you or any third party. References to RUSI include its directors and employees.

For this report, the authors have processed company, entity and individual names recorded in Russian and Chinese. In some instances, names of companies, entities and individuals have had to be translated or transliterated. Every effort has been made to ensure accuracy in translation/transliteration, and the authors do not accept liability for any unintentional errors made in this regard.

The authors also processed a large dataset of microelectronic components with serial numbers, verifying their authenticity and resolving them to specific manufacturers using open sources. However, a small number of them were not identifiable on manufacturer pages or on third-party seller pages, possibly because they are now out of production. Additionally, several components had insufficient identifiable information necessary to make a positive identification.

IDENTIFICATION OF INDIVIDUALS, COMPANIES AND GOVERNMENTS IN THIS REPORT

The purpose of this report is to explain and demonstrate how the Russian military depends on Western technology. To achieve this purpose, it identifies a number of individuals/companies/governments who are believed to be involved in the designing and manufacturing of components which have been acquired by the Russian military and are used in their military hardware. For the avoidance of doubt, RUSI does not impute any allegations of wrongdoing on the part of these individuals/companies/governments, and makes no representations or assertion that these individuals/companies/governments have any involvement in any sanctions evasion-related activity or are involved in directly or indirectly supplying the Russian military and/or Russian military customers in breach of any international (or their own domestic) laws or regulations restricting or prohibiting such action, unless expressly stated in the report.

METHODOLOGY

For this report, RUSI's Open Source Intelligence and Analysis (OSIA) and Military Sciences departments used extensive datasets of components and microelectronics sourced from disassembled Russian weapons either captured or expended in Ukraine since February 2022. These compilations of technical assessments were databased, standardised and categorised to enable further analysis.

Physical inspection of a significant sample of the weapons systems and platforms by RUSI during fieldwork confirmed the authenticity and accuracy of this data, which was also compared to product descriptions and serial numbers published by a wide variety of manufacturers. It should be noted that grey and black markets for counterfeit components and microelectronics are a global problem, meaning that fool-proof corroboration is a challenging endeavour. Given the evidence assessed here and the long history of Soviet and Russian military procurement efforts targeting the world's leading technology and microelectronic companies, the research team operated under the assumption that the majority of these parts were genuine. Assessments conducted internally by the Russian government, and seen by the authors,

highlighting critical dependence on a number of foreign manufacturers, increases the confidence that the components identified in Russian weapons are genuine. Further scrutiny, particularly X-ray analysis, could in future be used to prove the authenticity of many of the components found in these platforms. However, the ongoing conflict in Ukraine makes some of this additional work challenging.

This data was then married with a range of other sources, such as shipment-level trade data, import and export declarations, and corporate records in Russian in an attempt to better understand the country's procurement networks while also placing these weapons in their tactical, operational and strategic contexts.

ACKNOWLEDGEMENTS

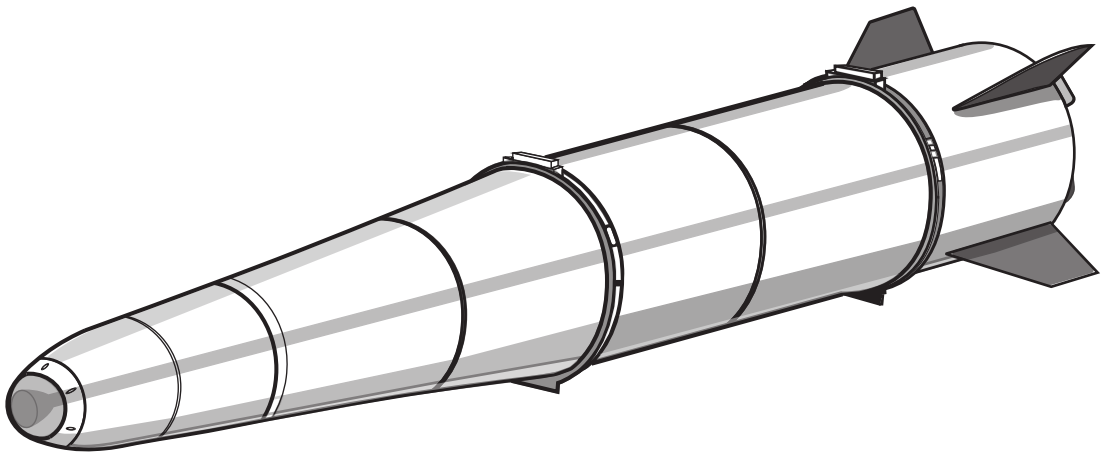
RUSI would like to thank several people and partners who have helped with this report, including Professor Peter Roberts, Dr Markus Schiller, Dr Daniel Salisbury and Sean Corbett CB MBE. RUSI would also like to thank Altana Technologies, whose 'Altana Atlas' data platform helped us to understand how semiconductor and microelectronic goods moved through the international trading system to Russian military end users.

IN PARTNERSHIP WITH

Altana

CORRECTION NOTICE, 8 AUGUST 2022

Please note that an earlier version of this report erroneously indicated the US-based company Gumstix as German based. This has now been corrected and any related figures have been updated accordingly. The authors and RUSI apologise for any confusion this may have caused. This change does not affect the analysis and conclusions presented in the report.



An outline of an Iskander missile. Source: RUSI.

Contents

Executive Summary

Russia's invasion of Ukraine on 24 February 2022 has not gone to plan. Launched in the expectation of a surgical occupation of Ukrainian cities, it has become a grinding attritional struggle that is rapidly degrading the Russian military. This report, which contains an examination of the components and functioning of 27 of Russia's most modern military systems – including cruise missiles, communications systems and electronic warfare complexes – concludes that the degradation in Russian military capability **could be made permanent** if appropriate policies are implemented.

Based on the technical inspection of Russian military equipment captured in or fired at Ukraine, this report outlines the extent to which Russia's multi-billion-dollar, decades-long military modernisation programme has depended on the extensive use of microelectronics manufactured in the US, Japan, Taiwan, South Korea, Switzerland, the Netherlands, the UK, France and Germany. In order to be permitted to use foreign components in military equipment, Russian companies must demonstrate to the Russian Ministry of Defence that there is **no domestic alternative**.

RUSI discovered at least **450 different kinds of unique foreign-made components** across these 27 systems, the majority of which were manufactured by US companies with a longstanding reputation for designing and building sophisticated microelectronics for the US military. Of these, at least **80 different kinds of components were subject to export controls by the US**, indicating that Russia's military–industrial complex has, in recent decades, been able to successfully evade these. This report details examples of this continued espionage from the Soviet Union to Russia's renewed invasion of Ukraine in 2022.

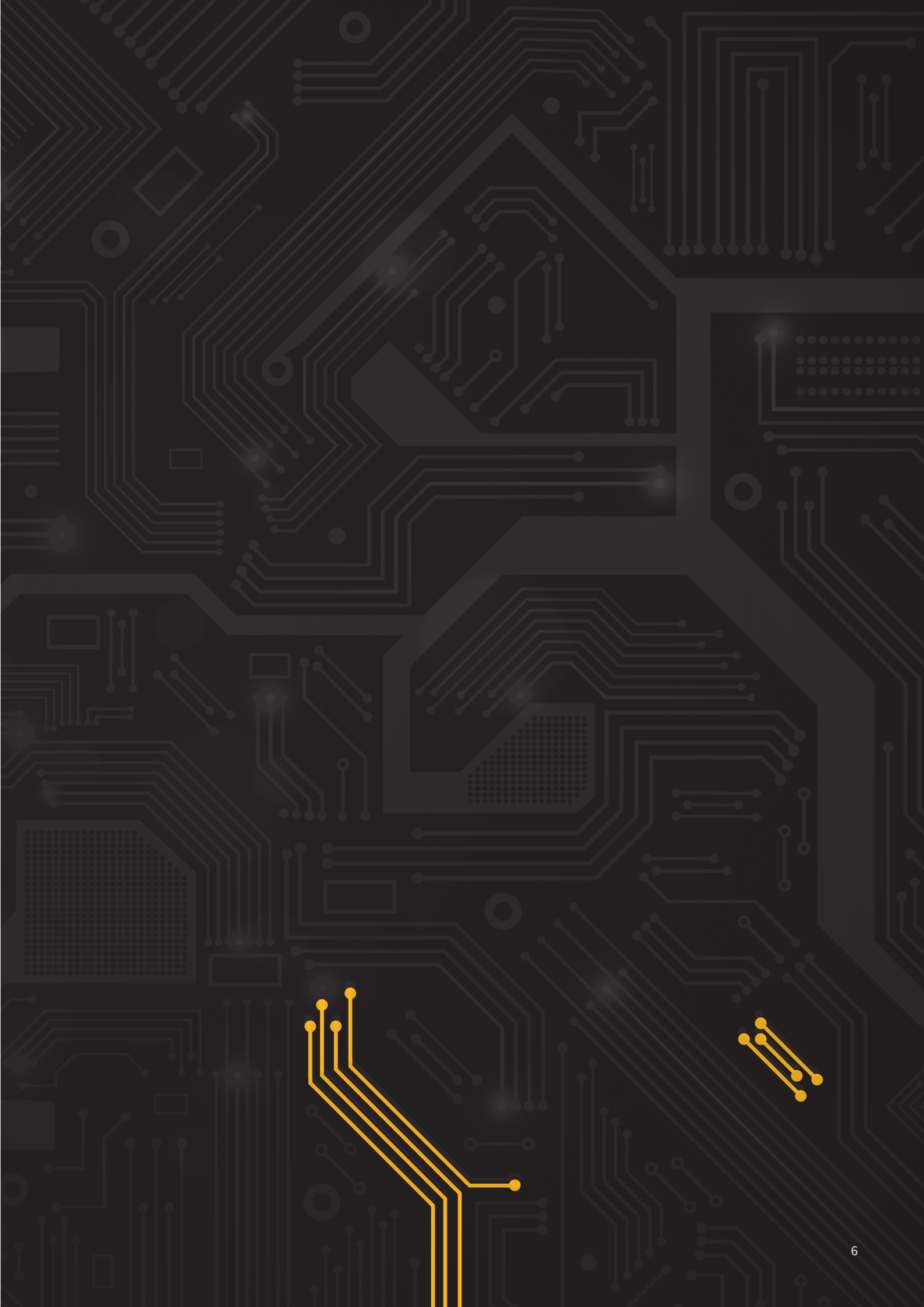
Russia has lost a vast quantity of military equipment in Ukraine and heavily depleted its arsenal of cruise and ballistic missiles. Following the imposition of new sanctions and tighter export controls, the Russian government has attempted to address the severing of access to critical components through **import substitution**. This approach has subsequently been found to be **non-viable**. As a result, Russia must now either design new and likely less-capable weapons or engage in **sanctions evasion**, which has become a critical priority for its special services.

RUSI analysis indicates that third-country transshipment hubs and clandestine networks operated by Russia's special services are now working to build new routes to secure access to Western microelectronics. For several years, Russia has operated a range of networks to illicitly procure goods in Europe and North America using a range of front companies, fraudulent end-user licences and other tried and tested techniques originally pioneered by its Soviet predecessors. But Russia has also relied on large microelectronic distributors in transshipment hubs such as Hong Kong, which have continued to move goods at volume to the country in recent years.

If Russia is to have this silicon lifeline severed, it is critical that governments:

- Review and **strengthen existing export controls** in their own countries and jurisdictions.
- **Cooperate multinationally** to identify and close down Russian covert procurement networks.
- **Prevent** sensitive microelectronics from being **manufactured under licence** in states supporting Russia.
- Discourage third countries and jurisdictions from **facilitating re-export or transshipment** of controlled goods to Russia.

Russia is scrambling to procure what it can in bulk before the net closes. The time to act is now.



Introduction

'Yes, of course, we have not managed to do everything over the previous years in the field of import substitution ... But there is nothing to fear here: in key areas, which assure our sovereignty, we have done the essential'.[1]

In shot is a wide-angle view of a Ukrainian town. The distinctive crosshairs of an Orlan-10 UAV occupy the centre of the screen. It is a Russian reconnaissance UAV designed to coordinate artillery strikes. The operator zooms in on an assortment of trucks; Ukrainian personnel can be seen gathering around them.

The video camera is produced by Sony and mounted on a gimbal motor produced by Hextronik, based in the US. It zooms in smoothly to provide positive identifications of the targets. The Orlan-10's flight control system which keeps it above the target is based on the STM32F103VC microcontroller from a Swiss company called STMicroelectronics. The UAV is powered by an engine from Japanese company Saito Seisakusho. Together, they make the Orlan-10 a reliable flying machine with an operational range of up to 120 kilometres. Its navigation chip is a u-blox Neo-M8 GNSS module, first identified in an Orlan-10 in 2018.[2] The UAV's coordinates are likely communicated to its operator via a radio-frequency agile transceiver produced by Analog Devices.

Having established visual confirmation, the Orlan-10 operator calculates the coordinates of the target in order to provide accurate positional data to the responsible fire control headquarters. Once the coordinates have been established, targeting data is relayed to the radio operator who communicates it over a VHF R-168 Akveduk radio to set up the kill chain to the artillery brigade's

1 *Izvestiya*, 'Vystuplenie Vladimira Putina na Jevrazijskom ekonomicheskom forume' ['Address of Vladimir Putin at the Eurasian Economic Forum'], 26 May 2022, <https://iz.ru/1340365/video/vystuplenie-vladimira-putina-na-evraziiskom-ekonomicheskom-forume>, accessed 18 July 2022. [Author translation from Russian: 'Da, konechno, ne vse udalos' sdelat' za predyduschie gody v oblasti importzamescheniya…No eto nichego zdes' strashnogo net: po klyuchevym napravleniyam, kotorye obespechivayut nash suverenitet, my sdelali samoe neobhodimoe']. These remarks were made during an address to the Eurasian Economic Forum addressing efforts by Russian industry to adapt to Western sanctions. In this context the word 'sovereignty' likely refers to Russian economic independence, rather than territorial sovereignty.

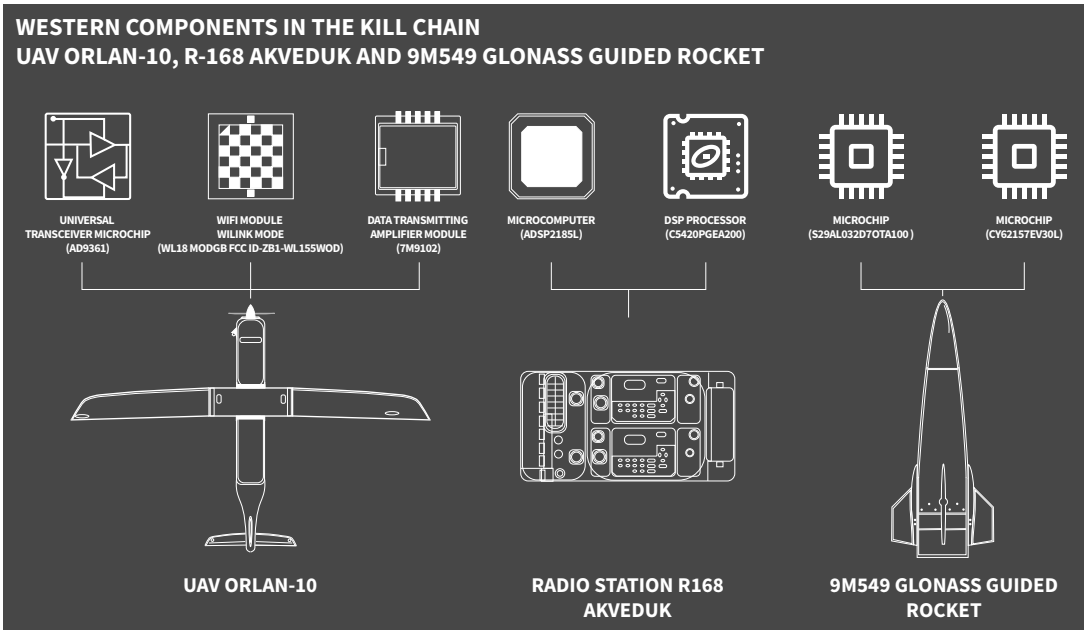
2 *Inform Napalm*, 'Russian Drone Orlan-10 Consists of Parts Produced in the USA and Other Countries – Photo Evidence', 2 June 2018, <https://informnapalm.org/en/russian-drone-orlan-10-consists-of-parts-produced-in-the-usa-and-other-countries-photo-evidence/>, accessed 18 July 2022.

command and control infrastructure.

Built by the Sarapul Radio Plant,[3] the R-168 Akveduk contains over a dozen components manufactured by Western companies. Incorporated into the radio's control board is a microcontroller manufactured by US-based Analog Devices, and a digital signal processor made by Texas Instruments. The transmitter board, through which the operator's voice is encoded and delivered up the kill chain, is also packed with Western components as well as a phase-locked loop (PLL) silicon gate manufactured by a South Korean company.

The fire-mission is assigned to a Tornado-S multiple rocket launcher battery, a relatively new system equipped with a GLONASS satellite navigation system.[4] For this fire-mission, the battery will use the 300-mm 9M549 GLONASS guided rocket. The rocket has a reported range of 120 km and circular error probability of 7–15 metres.[5] Onboard, the 300-mm rocket has a sophisticated computing unit along with a triaxial fibre-optic gyroscope and satellite navigational signals processing unit, allowing the munition's course to be corrected mid-flight, ensuring even greater accuracy at extended ranges against smaller, singular targets. The rocket's gyroscope contains a field-programmable gate array (FPGA) produced by Altera Corporation, while its satellite navigation signals processing and computing units both rely on high-speed static random-access memory (SRAM) modules produced by Cypress Semiconductor.

Figure 1: Western-Designed and -Manufactured Components in a Russian Kill Chain



Source: RUSI.

3 Army Guide, 'SARAPUL RADIOPLANT OJSC', <http://www.army-guide.com/eng/firm1087.html>, accessed 18 July 2022.

4 Tracy Cozzens, 'Russia Tests New GLONASS-Guided Missile', *GPS World*, 22 September 2020, <https://www.gpsworld.com/russia-tests-new-glonass-guided-missile/>, accessed 18 July 2022.

5 N R Jenzen-Jones and Charlie Randall, 'Russian 9M54-Series Cargo Missile Documented in Ukraine (2022)', Armament Research Services, 6 March 2022, <https://armamentresearch.com/russian-9m54-series-cargo-missile-documented-in-ukraine-2022/>, accessed 18 July 2022.

Following the launch of the rocket, the Orlan-10 will maintain visual contact with the target and update the battery on any changes to the target's position. Any corrections will be fed back through the kill chain, eventually to the rocket's computing unit mid-flight to ensure the most lethal effect. In this instance, the Orlan-10 operator observes the impact on their screen: at least two trucks can be seen ablaze and several Ukrainian personnel have been killed.

Real-world variations of this hypothetical kill chain, reconstructed by RUSI, have been repeated hundreds, if not thousands, of times in various iterations since Russia's 2014 and 2022 invasions of Ukraine, as well as during the country's 2015 intervention in Syria. But this process would have been impossible without critical Western components and electronics.

The systems described above are far from unique in this process, for Russia's weapons systems and military platforms contain a range of predominantly Western-sourced components and electronics that are critical to their function. From rocket systems to ballistic missiles and tactical radios to electronic warfare platforms, the Kremlin's war machine is often dependent on components sourced from abroad.

This report contains an analysis of the most comprehensive dataset of components yet released in open sources, which exposes, in stark detail, the Russian military's dependence on Western technology.

The dataset comprises close to 30 weapon systems, platforms and pieces of equipment captured from or expended by the Russian armed forces in Ukraine since the beginning of the invasion in February 2022. In several cases, these weapons were examined by RUSI staff on the ground at various locations throughout Ukraine. Some of these were legacy systems, likely built decades ago towards the end of the Soviet era. Others were state-of-the-art platforms built in recent years as part of Russia's multi-billion-dollar military modernisation programme.

Irrespective of their age and date of construction, one theme remained remarkably consistent: from the standard to the boutique, Russia's weapons contain large numbers of microelectronic components originally manufactured in North America, Europe and East Asia. While some of these, such as commercial off-the-shelf components, would have been comparatively easy for the Russian armed forces to purchase through domestic or international wholesalers, others were likely acquired by clandestine networks operated by the Russian Foreign Intelligence Service (SVR) or the GRU, Russia's military intelligence agency.

While this conclusion may be disquieting given Russia's attack on Ukraine, the Kremlin's expansive scientific and technological (S&T) espionage operations and the illicit procurement of Western components are not a new story. For close to a century, the country's intelligence services have prioritised the collection of S&T information and the acquisition of critical technology for Russia's weapons programmes.[6] Preoccupied with maintaining parity with the West, Soviet technical espionage operations and the infrastructure required to process this information were vast, comprising 100,000 individuals and 11,000 information departments affiliated with Soviet research institutes.[7]

RUSI's analysis indicates these priorities have likely never changed, for both the SVR and the GRU continue to aggressively pursue the procurement of parts, components and technical knowledge necessary to build and field weapons designed to crush their adversaries.

Now, confronted with a sweeping range of new sanctions following the February 2022 invasion of Ukraine, the Kremlin faces the daunting task of replacing these components while building alternative supply chains to move them into the country. Having lost and expended huge volumes of high-end weapons systems and platforms, Russia's military–industrial complex needs large numbers of new components to sustain its combat operations and equip its armed forces for future combat.

6 CIA, 'Interagency Intelligence Memorandum: The Technology Acquisition Efforts of the Soviet Intelligence Services', 18 June 1982. See also Kevin Riehle, *Russian Intelligence* (Bethesda, MD: National Intelligence University, 2021), p. 81.

7 CIA, 'Interagency Intelligence Memorandum', p. 7; Riehle, *Russian Intelligence*, pp. 138–40.

This problem is not lost on those at the highest levels of the Russian government. For years, the Kremlin has promoted, with little success, import substitution to hedge against Western sanctions.[8] In June 2014, Vladimir Putin highlighted the importance of import substitution for the Russian military and called for a wide-ranging transition to domestically produced military components.[9] Eight years later, however, Russia appears to have made very little effective progress in kick-starting a home-grown semiconductor revolution, a now almost-impossible aspiration in light of multilateral sanctions designed to cripple the country's military–industrial complex.

Although some components can be sourced from China, many critical components for Russian weapons cannot. Without the requisite domestic manufacturing capabilities, Russia and its armed forces remain highly vulnerable to multilateral efforts to choke off these component flows and raise the costs of its aggression in Ukraine.

8 For more on Russian efforts at import replacements, see Tatyana Mischenko, 'Podderzhali otechestvennogo proizvoditelya. Chto takoe importzamescheniye, kak ono prohodit v Rossii' ['Supporting National Producers. What is Import-Replacement, How Is It Being Implemented in Russia?'], *SovkomBlog*, 27 January 2022, <https://sovcombank.ru/blog/umnii-potrebitel/podderzhali-otechestvennogo-proizvoditelya-chto-takoe-importozameschenie-kak-ono-prohodit-v-rossii>, accessed 18 July 2022.

9 *Interfax*, 'Putin zayavil o neobhodimosti uskorennogo perehoda promyshlennosti k importzamescheniyu' ['Putin Stated the Need for Industry's Hastened Transition to Import-Substitution'], 28 July 2014, <https://www.interfax.ru/business/388216>, accessed 18 July 2022.

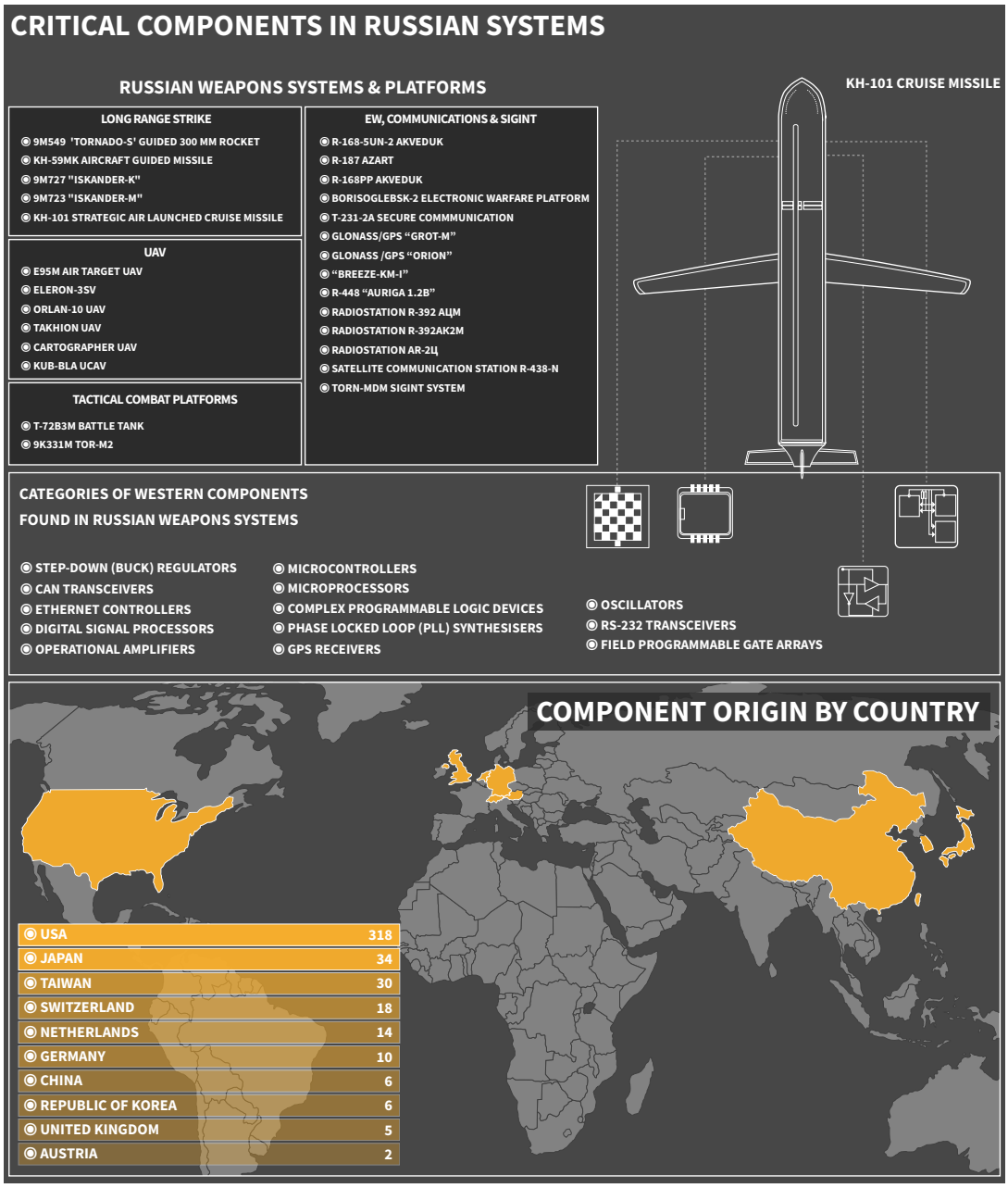
Systems and Western Components

The dataset acquired by RUSI covers 27 weapons systems, platforms, radios, and pieces of equipment either captured or expended in Ukraine since the beginning of the full-scale invasion in February 2022 up until the end of June. These systems include several long-range strike assets such as the 9M720 Iskander-M quasi-ballistic missile,[10] the 9M727 ground-launched cruise missile (GLCM) launched from the Iskander Transporter Erector Launcher (TEL), and the Kh-101 strategic air-launched cruise missile (ALCM). It also includes tactical combat platforms such as the 9K331M Tor-M2 air-defence system and a variety of UAVs, radio and satellite communication systems such as the R-168 Akveduk tactical radio, as well as electronic warfare (EW) and signals intelligence (SIGINT) platforms such as the Torn-MDM.

10 Quasi-ballistic missiles are largely ballistic but capable of performing manoeuvres mid-flight and often have a lower trajectory.

01

Figure 2: An Overview of the Systems and Components



Source: RUSI.

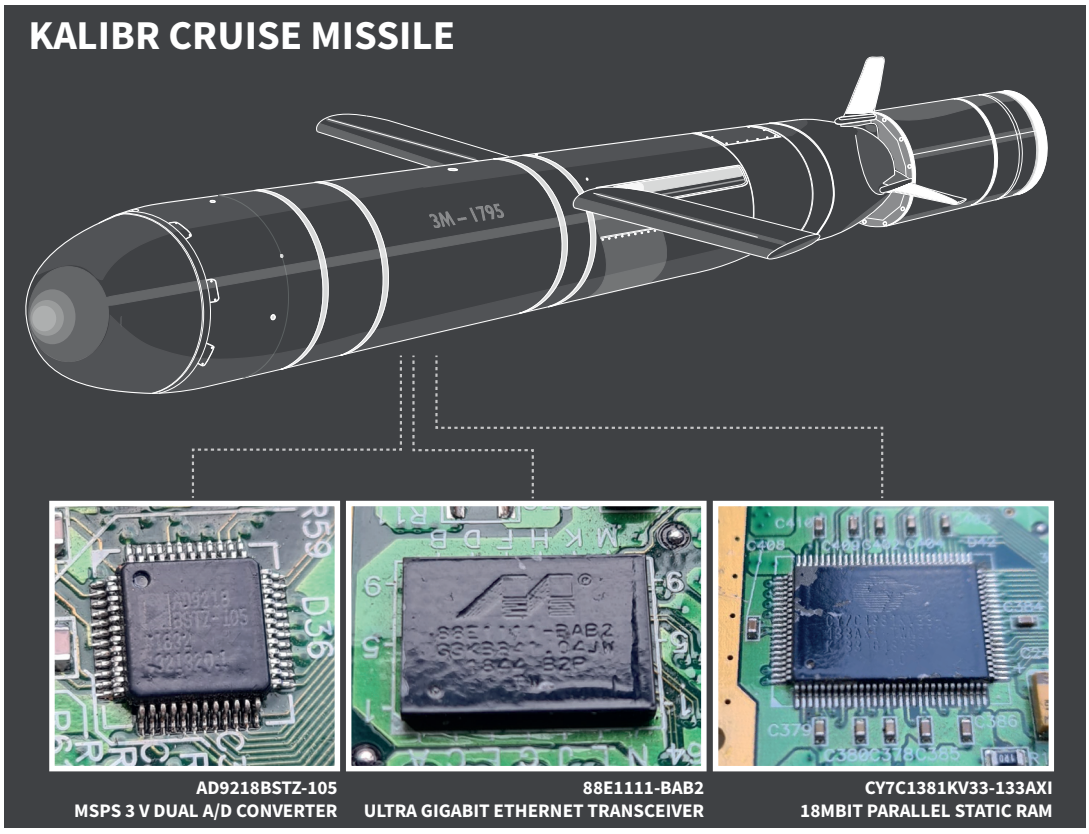
In some cases, these systems were recovered completely intact. In others, particularly in the case of expended munitions such as ballistic and cruise missiles, they were only recovered in part, meaning that their component profile was not always complete. As such, component lists for several systems presented here should not be understood as exhaustive. Despite these limitations, the capture and disassembly of these systems at this scale provides an almost unparallelled opportunity to understand how these weapons are designed, built and deployed on the battlefield.

Together, these systems contain a wide swath of Western-designed components including microelectronics, specialised cameras and sensors, transceivers and converters, air blades, motors and a range of others. Among them, RUSI identified 450 unique components primarily sourced from Western manufacturers, of which at least 318 came from US-based companies. In some instances, these systems contained several of the same components. Meanwhile, some of the same components were found across several systems and sub-systems, meaning that the total number of items was significantly higher.

Many of these components are prosaic microelectronics that can be purchased through online distributors in a range of countries and jurisdictions. In others, they are goods for which export has long been subject to controls designed to prevent them from being used for military purposes. Today, following the Kremlin's invasion of Ukraine, the vast majority are now restricted for export to Russia especially if destined for a military end user.

The dates of manufacture of the components and microelectronics vary. While some were built and likely procured as far back as the early 1980s, others were manufactured in recent years. Western-designed components found in a Kalibr cruise missile, for example, appear to date to 2018 and 2019 – four years after a wide range of sanctions and export controls targeted Russian military end users following the Kremlin's invasion of Ukraine.

Figure 3: Kalibr Cruise Missile Modern Components



Source: RUSI.

However, regardless of their particular classification, the presence at this scale of Western-manufactured microelectronics and other components highlights Russia's ongoing failure to produce domestic counterparts or source analogous items from elsewhere. It also underscores the challenges facing the country's military–industrial complex in replacing equipment and material lost since the beginning of the invasion, particularly in light of multilateral efforts to strengthen controls on the export of dual-use goods and critical components.

WORLDWIDE SOURCING

The majority of the components in the dataset originate from 57 US-based companies. Among these, the most prevalent were items produced by leading microelectronics manufacturers such as Analog Devices Inc, Texas Instruments, Maxim Integrated,[11] Xilinx Inc,[12] Microchip Technology

11 Operates as a subsidiary of Analog Devices Inc since August 2021. See Analog Devices, 'Analog Devices Completes Acquisition of Maxim Integrated', press release, 26 August 2021, <https://www.analog.com/en/about-adi/news-room/press-releases/2021/8-26-21-adi-completes-acquisition-of-maxim-integrated.html>, accessed 18 July 2022.

12 Acquired by Advanced Micro Devices Inc in February 2022. See Advanced Micro Devices, 'AMD Completes Acquisition of

Inc, ON Semiconductor, Altera Corporation,[13] Intel Corporation, Atmel Corporation[14] and Cypress Semiconductor.[15] Together, a total of 208 unique components produced by these 10 companies were recovered from 26 of the above-mentioned systems used by the Russian armed forces.

Outside of the US, a further 77 components were designed and produced by companies based in Japan, Taiwan, South Korea, China and Singapore. Thirteen of these were found to have been produced by Japan's Murata Manufacturing Co Ltd, while seven were produced by Taiwan's Yageo Corporation.

At least 55 unique components were found to have originated from European companies. Notably, the largest volume of products came from Netherlands-based NXP Semiconductors NV and Switzerland-based STMicroelectronics. Other manufacturers include Switzerland's u-blox, Germany's EPCOS, France's Thales Group, as well as UK-based companies CML Microcircuits and Golledge Electronics.

While most of these components had serial numbers that could be verified and resolved to specific manufacturers, a small number were not identifiable on manufacturer pages and are likely out of production. In addition, some components had insufficient identifiable information necessary to make a positive identification. It should also be noted that the counterfeiting of components is an increasingly common phenomenon, meaning that specific parts can sometimes be fraudulent, lower-quality copies manufactured elsewhere.

These components were categorised into types and subtypes in order to understand the most common ones used across these Russian systems. Most prevalent were microcontrollers and microprocessors, as well as complex programmable logic devices (CPLD) and FPGAs, which allow customers and engineers to configure the integrated circuit after it has been manufactured.[16]

Other common Western-manufactured components include PLL synthesisers, operational amplifiers, oscillators, RS-232 transceivers, CAN transceivers, step-down regulators, ethernet controllers, analogue-to-digital (A/D) converters and thermal imaging cameras.

While these kinds of devices play a huge number of different roles in commercial electronic systems, they also sit at the heart of how modern wars are fought. Complex sensors, information processing systems, targeting and navigation complexes, encrypted communication equipment and many other modern platforms rely for their very function on these kinds of microelectronics. Because of this, their construction or procurement will always remain a priority for Russia's technology-hungry military–industrial complex.

Xilinx', press release, 14 February 2022, <https://ir.amd.com/news-events/press-releases/detail/1047/amd-completes-acquisition-of-xilinx>, accessed 18 July 2022.

13 Acquired by Intel Corporation in December 2015. See Intel Newsroom, 'Intel Completes Acquisition of Altera', news release, 28 December 2015, <https://newsroom.intel.com/news-releases/intel-completes-acquisition-of-altera/#gs.5eb5ck>, accessed 18 July 2022.

14 Acquired and subsumed by Microchip Technology in 2016. See Claudia Assis, 'Microchip Technology Buys Chip Maker Atmel in $3.56 Billion Deal', MarketWatch, 19 January 2016, <https://www.marketwatch.com/story/microchip-technology-buys-chip-maker-atmel-in-356-billion-deal-2016-01-19>, accessed 19 July 2022.

15 Acquired by Infineon Technologies AG in April 2020. See Infineon Technologies, 'Infineon Technologies AG Completes Acquisition of Cypress Semiconductor Corporation', press release, 16 April 2020, <https://www.infineon.com/cms/en/about-infineon/press/press-releases/2020/INFXX202004-049.html>, accessed 18 July 2022.

16 These devices also require a programming device in order to be configured by the user either in development or at the factory. These programming devices, usually sold by the chip manufacturer, contain a number of complex parts and may be export controlled. This would mean that users wishing to import CPLDs and FPGAs would also need to import these supporting tools in order to programme them correctly. Xilinx, 'Field Programmable Gate Array (FPGA)', <https://www.xilinx.com/products/silicon-devices/fpga/what-is-an-fpga.html>, accessed 21 July 2022; techopedia, 'Complex Programmable Logic Device (CPLD)', <https://www.techopedia.com/definition/6655/complex-programmable-logic-device-cpld>, accessed 21 July 2022.

STEMMING THE FLOW: SANCTIONS AND EXPORT CONTROLS

Following the February 2022 invasion of Ukraine, the US, the UK and the EU passed a range of sweeping sanctions on Russia.[17] These included targeted financial and sectoral sanctions, in addition to the extension of wide-ranging export controls designed to curtail the country's access to military technology and critical components.[18] A variety of other countries and jurisdictions, including Japan, South Korea, Taiwan, Canada, Australia and Switzerland, committed to implementing similar export controls.

While prior to the invasion many of the US-manufactured components found in Russia's weapons systems were cleared for export to Russia under the Export Administration Regulation (EAR99), US exporters of these products still had a due-diligence obligation to make sure they were not destined for a prohibited end user, or to be used in prohibited end use.[19]

Russian weapons examined for this report, however, contained a long list of EAR99-classified components manufactured by US companies. Texas Instruments, Analog Devices, Maxim Integrated and Xilinx were the primary manufacturers of these, accounting for approximately 30% of the total. Notably, they included a wide variety of parts important for geolocation and calculation, aggregated under roughly four categories: microcontrollers and microprocessors; interfaces; amplifiers; and FPGAs.

Clearly, the presence of large numbers of US-manufactured EAR99 components in Russian weapons systems is strong evidence that these parts were either purchased from distributors in Russia or that they were being procured and diverted for military purposes.

In several other cases, components found in Russian weapon systems were subject to more stringent export controls even before the February 2022 invasion.[20] This is true for US-manufactured parts,[21] but also often others made elsewhere such as in the UK, the EU, Japan, South Korea and Taiwan, meaning these will likely have been procured illicitly and clandestinely shipped to Russia or fraudulently diverted to military end users at some point prior to the invasion.

Several leaked cables from 2007 show internal US government deliberations over controlled exports to Russia. One of these concerns an A/D converter produced by Analog Devices that is very similar to those discovered in several weapons systems in Ukraine.[22] While the Russian importer was ultimately deemed a civilian entity at the time, direct exports of controlled US technology would have required both a licence and possible post-shipment verification to ensure the product was used for non-military purposes.[23]

17 For UK measures, see Foreign, Commonwealth and Development Office, 'UK Sanctions Relating to Russia', 19 July 2022, <https://www.gov.uk/government/collections/uk-sanctions-on-russia>, accessed 20 July 2022; for US measures, see US Department of the Treasury, 'Ukraine-/Russia-Related Sanctions', <https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/ukraine-russia-related-sanctions>, accessed 20 July 2022; for EU measures, see European Commission, 'Sanctions Adopted Following Russia's Military Aggression Against Ukraine', <https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions/sanctions-adopted-following-russias-military-aggression-against-ukraine_en>, accessed 20 July 2022.

18 *Ibid.*

19 International Trade Administration of the US Department of Commerce, 'Export Control Classification Number (ECCN) and Export Administration Regulation (EAR99)', <https://www.trade.gov/eccn-and-export-administration-regulation-ear99>, accessed 18 July 2022.

20 Components for this project were cross-referenced against open sources to determine if they were classified under ECCN or EAR99 regulations. See 'Methodology'.

21 Foreign-made components using US-origin technology commingled above a certain degree will still be subject to US export controls and may require an export licence. See Bureau of Industry and Security of the US Department of Commerce, 'Deemed Exports FAQs – What Technologies Are Subject to the Commerce Department Controls?', <https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faqs/faq/48-what-technologies-are-subject-to-the-commerce-department-controls>, accessed 25 July 2022.

22 WikiLeaks, 'EXTRANCHECK: PRE-LICENSE CHECK: JSC VREMYA- CH, NIZHNY NOVGOROD, RUSSIA, LICENSE NO. D368426', 12 January 2007, <https://wikileaks.org/plusd/cables/07MOSCOW86_a.html>, accessed 19 July 2022.

23 International Trade Administration of the US Department of Commerce, 'Export Control Classification Number (ECCN)

However, following Russia's 2014 invasion and annexation of Crimea, a range of countries had already been engaged in attempts to restrict the supply of components to Russia's military–industrial complex. In early 2014, the US Bureau of Industry and Security (BIS) expanded export restrictions to Russia, denying pending applications for licences to export or re-export any high-technology items subject to EAR to Russia or Crimea that contribute to Russia's military capabilities or defence industrial base.[24] In July the same year, the EU followed suit and introduced sanctions which included an embargo on arms and related materials, and dual-use goods and technology intended for military use or military end users.[25]

Since then, US export restrictions have been gradually expanded. For example, in December 2020, BIS published a 'Military End User' (MEU) list compromising 58 Chinese and 45 Russian companies which required exporters, re-exporters and those looking to transfer components in-country to obtain an export licence to move EAR products to these entities.[26]

In March 2021, BIS also narrowed the range of EAR licence exceptions significantly, suspending License Exception RPL (Service and Replacement of Parts and Equipment), License Exception TSU (Technology and Software Unrestricted) and License Exception APR (Additional Permissive Reexports) for transactions involving items controlled for national security reasons that are destined for Russia.[27]

The BIS Entity List

Following the 2022 invasion, BIS has added a large number of Russian and Belarusian companies to its Entity List, a trade restriction list consisting of foreign persons, entities and governments subject to EAR that regulates dual-use items.[28] Parties listed are involved in activities that are either sanctioned by the US State Department or contrary to the US's national security or foreign policy interests.[29]
The Entity List imposes a licence requirement on listed parties, regardless of other licence requirements imposed elsewhere in the EAR. In some of these entries, even goods classified as EAR99 would require a licence by the exporter to be exported, re-exported or transferred (in-country) to that party.[30] While not as restrictive as being placed on the BIS's Unverified List or being designated a 'denied person', for most of the parties on the Entity List, BIS imposes a licence review policy of presumption of denial, effectively blocking those listed parties receiving Export Control Classification Number (ECCN) and EAR99 dual-use goods from US exporters.

Hence, while the huge swath of sanctions and the tightening of export controls will likely significantly impact Russia's ability to procure

and Export Administration Regulation (EAR99)', <https://www.trade.gov/eccn-and-export-administration-regulation-ear99>, accessed 18 July 2022.

24 Bureau of Industry and Security of the US Department of Commerce, 'Commerce Department Announces Expansion of Export Restrictions on Russia', press release, 28 April 2014, <https://www.bis.doc.gov/index.php/all-articles/107-about-bis/newsroom/press-releases/press-release-2014/665-commerce-dept-announces-expansion-of-export-restrictions-on-russia>, accessed 19 July 2022.

25 Council of the EU, 'Timeline – EU Restrictive Measures Against Russia Over Ukraine', <https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/>, accessed 19 July 2022.

26 Bureau of Industry and Security of the US Department of Commerce, 'Supplement No. 4 to Part 744 – ENTITY LIST', 28 June 2022, <https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file>, accessed 19 July 2022.

27 Alexandre (Alex) Lamy, Lise S Test and Paul Amberg, 'BIS and DDTC Implement Strengthened US Export Controls on Russia in Response to Poisoning and Imprisonment of Navalny', Sanctions and Export Controls Update, 29 March 2021, <https://sanctionsnews.bakermckenzie.com/bis-and-ddtc-implement-strengthened-us-export-controls-on-russia-in-response-to-poisoning-and-imprisonment-of-navalny/>, accessed 19 July 2022.

28 Bureau of Industry and Security of the US Department of Commerce, 'Entity List', <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>, accessed 19 July 2022.

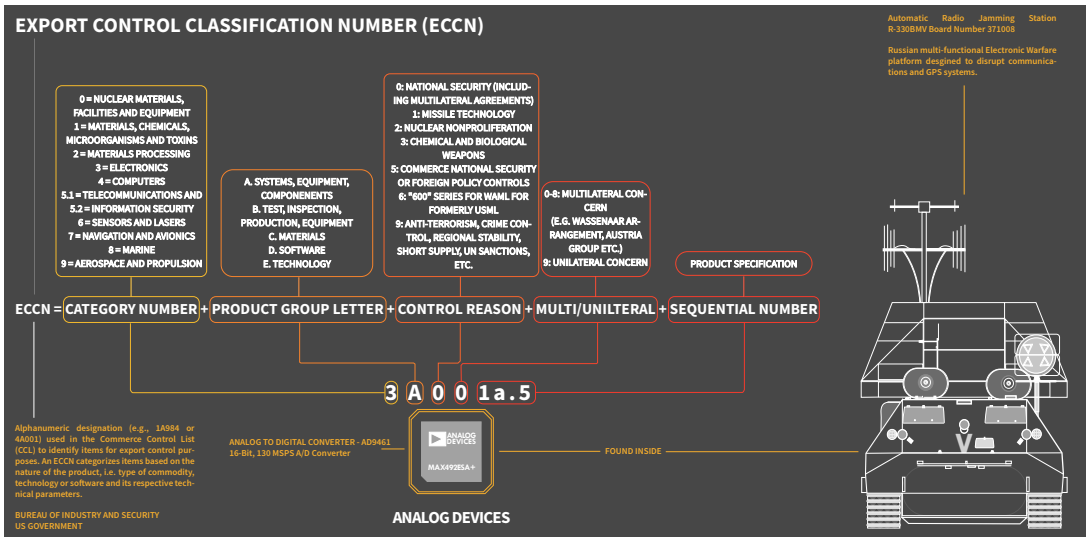
29 *Ibid.*

30 *Ibid.*

Western components for its weapons, many of those found in the country's weapons platforms were already controlled prior to the 2014 and 2022 invasions.[31]

In fact, a total of 81 unique components found in Russian weapons systems are classified as dual-use goods with associated Export Control Classification Numbers (ECCNs) on the US government's Commerce Control List.[32] The ECCN system uses five-character alpha-numeric designations for determining if goods require an export licence from the US Department of Commerce. If a good has an ECCN, then the product has been classified as a dual-use good and an exporter must acquire this licence for shipment abroad.

Figure 4: Understanding Export Control Classification Numbers



Sources: US Bureau of Industry and Security; MIT Export Control, 'Guide to Export Control Classification Numbers (ECCNs)'; RUSI.

Many of these US-manufactured, controlled components were found in Russia's most critical weapons systems such as the 9M549 300-mm GLONASS-guided rocket, the Kh-59 anti-ship missile (AShM) and the R-330BMV EW system. The 9M549 rocket and Kh-59 contained flash memory and SRAM modules that are ECCN controlled. Meanwhile, the R-330BMV contained a variety of ECCN-controlled components including FPGAs, CPLDs, microprocessors, digital signal processors and A/D converters.

Other goods with an ECCN included Dutch semiconductors in the Kh-101 ALCM and a high-performance CMOS static RAM chip inside the 9M727 GLCM. Five separate ECCN components were also found in the Torn-MDM SIGINT system, including Western-manufactured microcontrollers and RF amplifiers. However, the systems which contained the most ECCN-controlled components were generally instances of radio equipment. For example, the R-392 ACM radio contained at least six unique ECCN-classified components.

A high percentage of these controlled goods were originally manufactured by US-headquartered companies, making up 78% of ECCN goods in the dataset. Taken together, Analog Devices and Texas Instruments were the original manufacturers of approximately 25% of the overall ECCN-classified goods found in Russian weapons systems.

Other US manufacturers of ECCN-classified components include Intel Corporation, Atmel Corporation, Cypress Semiconductors and Microchip Technology. Japanese and Taiwanese manufacturers follow in close second and third with 10 and nine items, respectively.

31 Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List (CCL)', <https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>, accessed 19 July 2022.

32 Components for this project were cross-referenced with open sources to determine if they were classified under ECCN or EAR99 regulations. See 'Methodology'.

AMERICA'S MOST WANTED

For decades, Russian intelligence agencies and their Soviet predecessors have targeted the US's leading computer and microelectronic companies as part of their espionage and procurement efforts. In 1985, a US government assessment of Soviet acquisition targets listed IBM and Texas Instruments as priority penetration targets for the Soviets.[33] KGB archives, published by the defector Vasili Mitrokhin, showed the agency had even managed to place a spy in the French office of Texas Instruments in 1964.[34] But the startling extent of these operations was only exposed in 1981, when Vladimir Vetrov – a Soviet engineer working for the KGB – provided French intelligence with 4,000 secret documents concerning the activities of Line X, a technical collection department subordinate to Directorate T of the First Chief Directorate of the KGB.[35] According to what was later to be named the Farewell Dossier, the Soviet effort was expansive, employing over 100 KGB operatives across the world.[36] The dossier also proved that these agents were prolific, collecting huge volumes of S&T information and materials from Western countries. Reportedly, 61.5% of S&T espionage materials came from the US, 10.5% from West Germany, 8% from France, 7.5% from the UK and 3% from Japan.[37]

Line X efforts were a dazzling success. According to the CIA's own 1982 assessments, the Soviets had acquired and 'copied in its entirety' the US AIM-9 Sidewinder air-to-air missile, which gave the country its first infrared homing missile, the Vympel K-13.[38] The Sidewinder was but one example among hundreds. The Soviets had acquired other missiles, such as the shoulder-fired FIM-43 Redeye MANPAD system, data on the guidance subsystem of the US LGM-30 Minuteman ICBM, data on solid-propellant missiles, radar data on systems used aboard F-14s, F-15s, F-18s and information on a huge range of other systems.[39]

33 Office of the Secretary of Defense, 'Soviet Acquisition of Militarily Significant Western Technology: An Update', September 1985, <https://apps.dtic.mil/sti/pdfs/ADA160564.pdf>, accessed 19 July 2022.

34 Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive* (London: Penguin Press, 1999), p. 245.

35 David G Major, 'Farewell', 1999, <https://cdn.ymaws.com/cicentre.com/resource/resmgr/articles/farewell_old_reason_by_david.pdf>, accessed 19 July 2022.

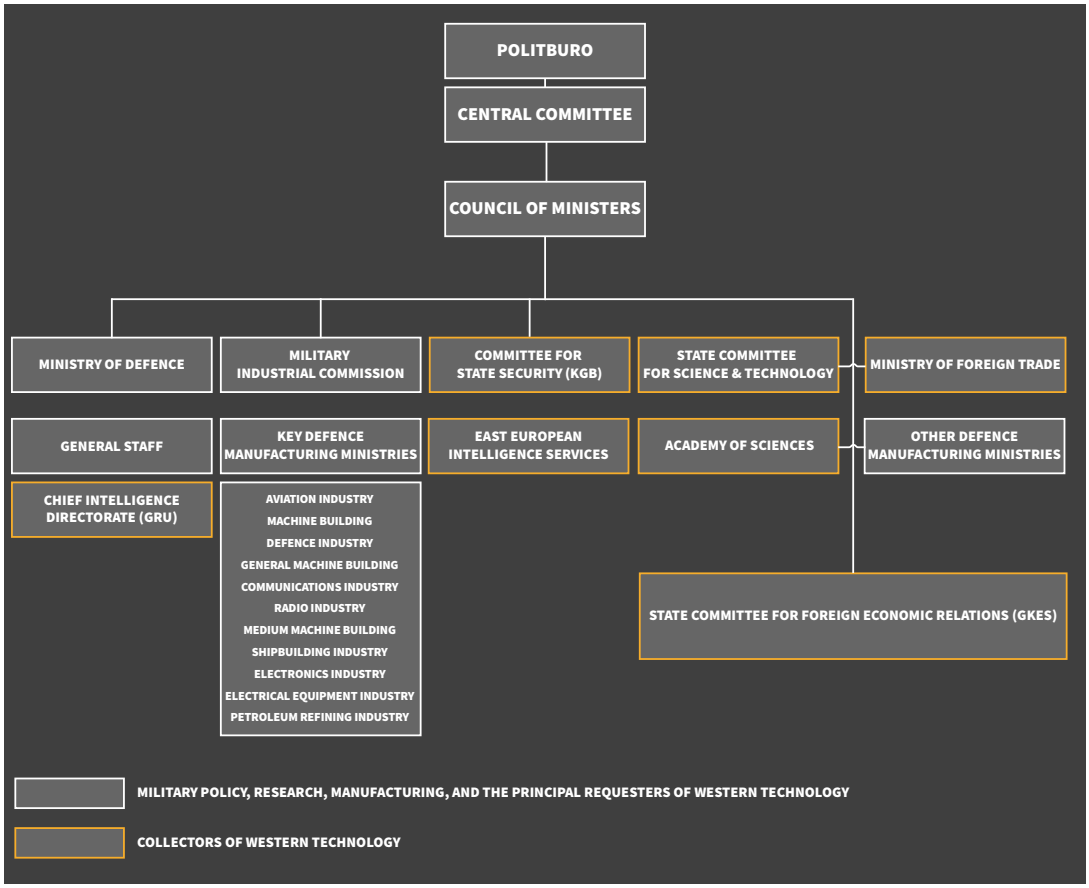
36 *Ibid.*

37 Christopher Andrew and Vasili Mitrokhin, *The Mitrokhin Archive II: The KGB and the World* (London: Penguin Press, 2006), p. 306.

38 CIA, 'Interagency Intelligence Memorandum', p. 9. An alternative theory of how the Soviet Union acquired an AIM-9 Sidewinder was that an unexploded AIM-9B had lodged into a Chinese MiG-17 during an air engagement with Taiwanese F-86 Sabres in September 1958. The intact missile was then reportedly sent to the Soviet Union to be reverse-engineered to develop the Vympel K-13. See Federation of American Scientists, 'AA-2 ATOLL K-13 (R-3 or Object 310) PL-2 / PL-3 / PL-5', <https://web.archive.org/web/20160304041942/http://fas.org/man/dod-101/sys/missile/row/aa-2.htm>, accessed 20 July 2022.

39 CIA, 'Interagency Intelligence Memorandum', p. 9.

Figure 5: Soviet Entities Responsible for the Direction and Procurement of Western Technology



Sources: Frank Dittmann, 'Microelectronics under Socialism'; RUSI.

The collapse of the Soviet Union only appears to have temporarily slowed these activities. In 2012, for example, 11 individuals were indicted for allegedly operating a smuggling ring seeking to export critical technology such as microelectronics 'primarily for Russian government agencies, including Russian military and intelligence agencies'.[40] According to media reports at the time,[41] the smuggling ring targeted several US companies, including Texas Instruments and Analog Devices, which claimed they were duped by Russian operatives working for Arc Electronics, a front company used to procure these items and transport them back to Russia.[42] Documents filed by the US Department of Justice alleged that, between 2002 and 2012, Arc Electronics shipped $50 million worth of goods to suppliers of military equipment to the Russian Ministry of Defence.[43]

In recent months, the US government has continued to pursue Russia's clandestine procurement networks. Just one month after the 2022 invasion, the US Treasury designated over 30 individuals and companies allegedly procuring critical Western technology on behalf of Russian intelligence agencies. These designations included a network centred on a Russian entity named Serniya Engineering, which the US Treasury

40 US District Court Eastern District of New York, 'United States of America Against Alexander Fishenko, et al.', indictment, 28 September 2012, <https://www.wired.com/images_blogs/dangerroom/2012/10/indictment.pdf>, accessed 20 July 2022.

41 Christie Smythe, Iain King and Bloomberg News, 'Texas Instruments, Xilinx Duped by Russia Export Ring, U.S. Says', *Washington Post*, 26 September 2015.

42 *Ibid.*

43 US Attorney's Office of the Department of Justice, 'Exporter of Microelectronics to Russian Military Sentenced to 135 Months in Prison Following Convictions on All Counts at Trial', 28 February 2017, <https://www.justice.gov/usao-edny/pr/exporter-microelectronics-russian-military-sentenced>, accessed 20 July 2022.

claimed directed a complex web of companies in the UK, Malta, Singapore, Spain and Russia.[44]

While Serniya Engineering was reportedly set up in 2017,[45] the company which previously used the domain of 'Serniya Engineering', NPO Sernia, used to be registered to the same domain and lists the same business scope as Serniya Engineering. Additional reporting notes that NPO Sernia was dissolved in 2016,[46] while Serniya Engineering was incorporated in 2017.

However, these timelines do not align in other open source reporting. Archived instances of Serniya Engineering's website show it was incorporated around 1998,[47] and articles published in April 2021 note that Serniya Engineering was founded in the late 1980s under the Moscow Department of Physics – the exact same location where NPO Sernia was addressed for years.[48]

Archived pages from NPO Sernia's website stated that some of its key projects were on behalf of the Ministry of Foreign Affairs and other governmental agencies. The crests of these agencies, published on its website between 2007 and 2013, include the Federal Security Service (FSB) and the Federal Protective Service (FSO).[49]

44 US Department of the Treasury, 'Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War', press release, 31 March 2022, <https://home.treasury.gov/news/press-releases/jy0692>, accessed 20 July 2022.

45 rusprofile, 'LLC "Serniya Engineering"', last updated 21 July 2022, can be found at <https://www.rusprofile.ru/id/10885594>, accessed 23 July 2022.

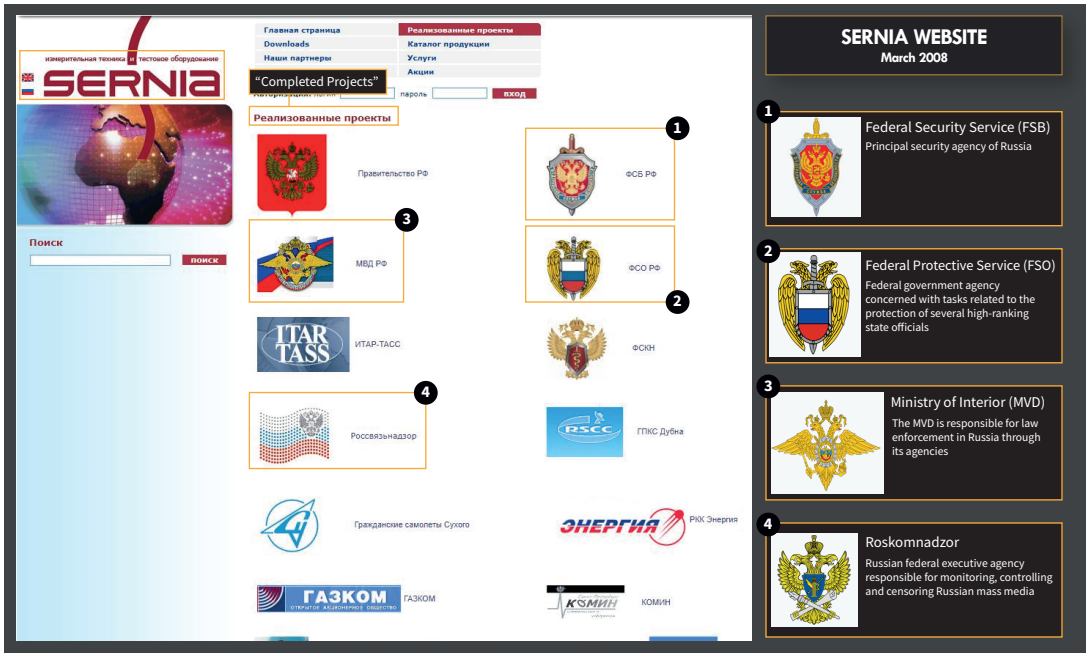
46 Reporting by the *Financial Times*, which was in correspondence with Serniya Engineering, notes NPO Sernia was dissolved in March 2016. See Jamie Powell, 'What on Earth is Djeco Group?', *Financial Times*, 25 March 2022. The information can be found at <https://www.ft.com/content/63c80363-644d-4981-a144-c618144845e6>, accessed 22 July 2022.

47 For the archived page from July 2007, see Sernia.ru, 'O Kompanii' ['About the Company'], accessed through Wayback Machine, <https://web.archive.org/web/20070715005149/http:/www.sernia.ru/?aux_page=about_company>, accessed 19 July 2022.

48 TMC, 'Interview with Sernia Engineering Employee', <https://go.techmfg.com/l/910112/2021-04-29/9r3l>, accessed 20 July 2022.

49 For the archived page from August 2013, see Sernia.ru, 'Realizovannnye proekti' ['Completed Projects'], accessed through Wayback Machine, <https://web.archive.org/web/20130830145236/http://www.sernia.ru/relized_projects>, accessed 19 July 2022. See also Powell, 'What on Earth is Djeco Group?'.

Figure 6: Sernia's Old Website Displaying the Crests of the FSB and FSO



Source: Serniya.ru; RUSI.

A central node in the Serniya Engineering network was the Russia-based Sertal LLC.[50] Addressed to a nondescript apartment block on the outskirts of Moscow, the company's website advertised itself as a 'supplier of electronic components' manufactured by Texas Instruments, Analog Devices, Cypress Semiconductors, NXP Semiconductors, STMicroelectronics and a range of others.[51] Notably, components manufactured by these companies were some of the most numerous found in Russian weapons platforms in Ukraine.

50 US Department of the Treasury, 'Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War', press release, 31 March 2022, <https://home.treasury.gov/news/press-releases/jy0692>, accessed 19 July 2022.

51 The archived version of Sertal.ru can be found at <https://web.archive.org/web/20220000000000*/sertal.ru>, accessed 19 July 2022.

Figure 7: Sertal's Webpage in February 2022

Sources: Sertal.ru; RUSI.

Shipment-level trade records confirm that Sertal was moving these types of US-manufactured goods. As recently as March 2021, for example, Sertal imported $600,000 worth of electronic integrated circuits manufactured by Texas Instruments through a Hong Kong intermediary.[52] Seven months later, the company imported another $1.1 million worth of electronic integrated circuits from the same Hong Kong exporter, this time manufactured by Xilinx.[53]

GRAND THEFT ANALOG

While Russia has long sought to cultivate a home-grown semiconductor industry, data analysed for this report shows that the country's weapons are packed with components originally manufactured by US companies. The two most prominent are Analog Devices and Texas Instruments, both microelectronics manufacturers which offer products specialised in defence applications.

In fact, out of 450 unique components in RUSI's dataset, products manufactured by Analog Devices and Texas Instruments account for nearly a quarter of those found in Russian weapons. These components, ranging from the mundane to the highly specialised, were found in the most critical systems such as ballistic and cruise missiles, other precision munitions and EW platforms.

In total, the dataset contained 50 unique components produced by Analog Devices, 13 of which were classified as dual-use goods under US law, meaning that exporters would likely have needed a licence to export them abroad. These components were primarily microprocessors and microcontrollers,[54] but also included mobile

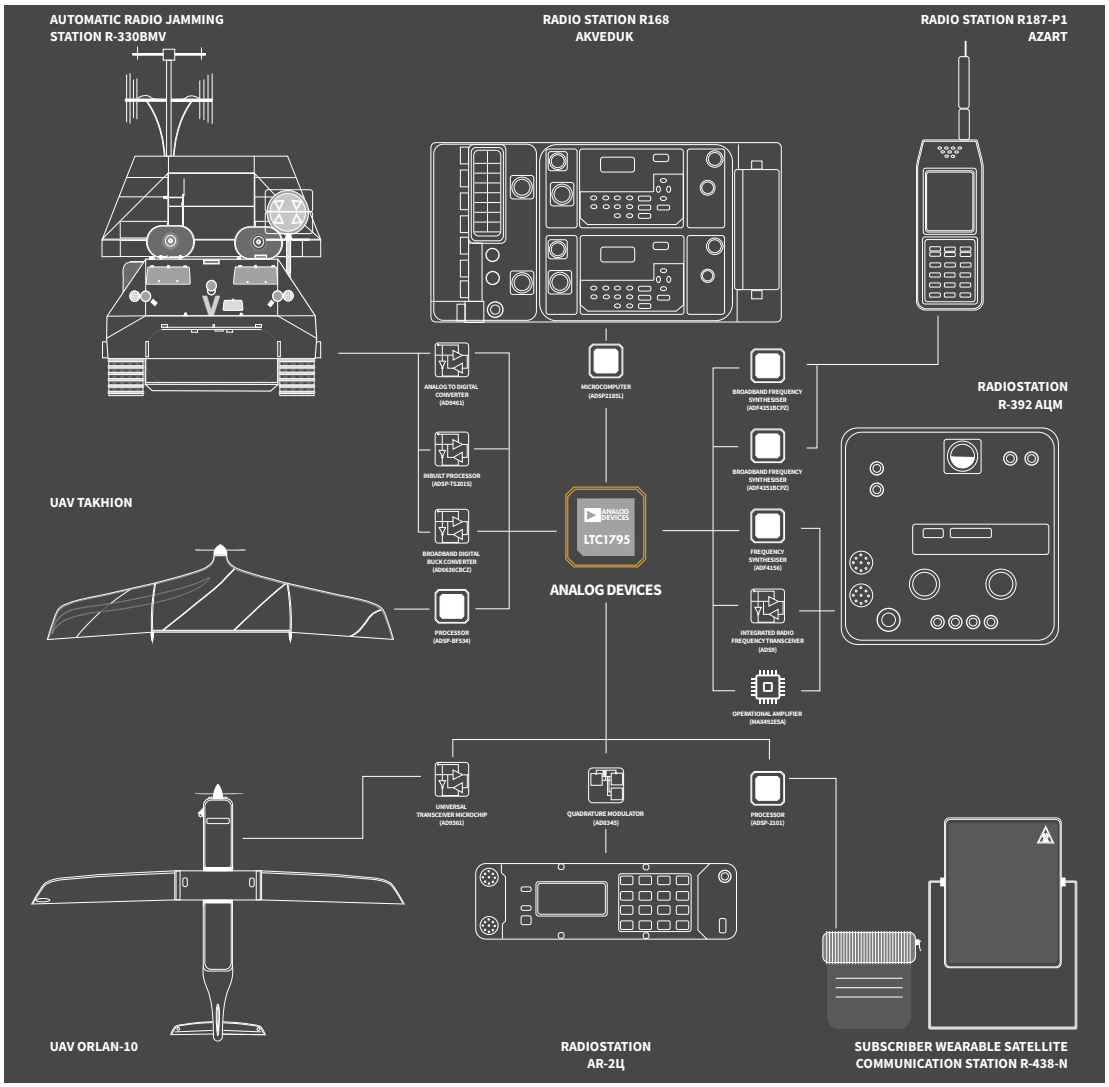
52 Trade data provided by third-party commercial provider.

53 *Ibid.*

54 ECCN 3A991.a.2 – a microprocessor or microcontroller with a clock frequency rate exceeding 25 MHz. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 – ELECTRONICS', <https://www.bis.doc.gov/index.php/documents/regulations-docs/442-category-3-electronics-design-development-and-production/file>, accessed 19 July 2022.

communications equipment,[55] telecommunication transmission equipment[56] and A/D converters.[57]

Figure 8: Analog Devices-Manufactured ECCN Components in Russian Weapons



Source: RUSI.

Established in 1965, Analog Devices is a world-leading producer of semiconductors specialising in integrated circuits for data conversion, signal processing and power management.[58] Many of these products are specifically designed for defence and aerospace applications and are employed by the US military in precision munitions, avionics, phased array

55 ECCN 5A991.g – mobile communications equipment. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 5 – TELECOMMUNICATIONS AND "INFORMATION SECURITY"', <https://www.bis.doc.gov/index.php/documents/regulations-docs/2336-ccl5-pt1-3/file>, accessed 19 July 2022.

56 ECCN 5A991.b – telecommunication transmission equipment and systems designed for use in single or multi-channel communication. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 5 – TELECOMMUNICATIONS AND "INFORMATION SECURITY"'.

57 ECCN 3A001.a.5.a.5 – an A/D converter with a 16-bit or greater resolution and output rate greater than 65 million words per second. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 – ELECTRONICS'.

58 Analog Devices, 'Corporate Information', <https://www.analog.com/en/about-adi/corporate-information.html>, accessed 19 July 2022.

systems, military communications, electronic surveillance systems and UAVs.[59]

For example, the company's A/D converters are often used in US missile systems such as the MIM-104 Patriot SAM and the AIM-120 AMRAAM.[60] These components translate analogue, real-world signals collected by onboard sensors into digital outputs that can be processed by computers.[61] In a cruise missile, they can enable the system's sensors to transmit real-time data to onboard computers responsible for guiding the payload to its target.[62]

One of Analog Devices' A/D converters, the AD9461, was discovered in the jamming board of a Russian Army R-330BMV Borisoglebsk-2 EW system. In these types of platforms, A/D converters enhance performance by allowing a receiver to operate over a wide frequency band to identify threat signals.[63] Like many other components found in Russian weapons platforms, this specific converter is classified as a dual-use good and is restricted for export,[64] likely meaning that it was procured clandestinely on behalf of the Russian armed forces or intelligence agencies.

Several other controlled components originally manufactured by Analog Devices were found in Russian weapon systems. These include a AD6636CBCZ wideband (digital) receiver signal processor found in the same jamming board of the R-330BMV Borisoglebsk-2 EW system, an AD9361 radio frequency agile transceiver in the payload information transmission module of the Orlan-10 UAV, and a Blackfin Processor in the navigation and positioning module of a Takhion UAV.

While RUSI found over a dozen different kinds of these controlled components in Russian weapons platforms, another 37 of the company's parts were discovered in several other systems. These included items in a Kh-59MK AShM, and the Torn-MDM SIGINT platform. These non-controlled items included operational amplifiers, RS-232 transceivers, power management microchips, radio frequency switches and temperature sensors, among others.

EVERYTHING'S BETTER IN TEXAS

Items manufactured by Texas Instruments are also preponderant in several critical Russian weapons systems disassembled in Ukraine. Founded in 1930, Texas Instruments has evolved into one of the world's largest semiconductor companies based on sales volume,[65] reportedly holding over 41,000 patents.[66] Like Analog Devices, Dallas-based Texas Instruments also designs high-end components for the aerospace and defence industries and has a long history of being at the cutting edge of military electronics.[67]

59 Analog Devices, 'Aerospace and Defense', <https://www.analog.com/en/applications/markets/aerospace-and-defense-pavilion-home.html>, accessed 19 July 2022.

60 Military Aerospace Electronics, 'Analog Devices to Supply New A-D Converter for Patriot Missile', 1 February 2000, <https://www.militaryaerospace.com/communications/article/16706596/analog-devices-to-supply-new-ad-converter-for-patriot-missile>, accessed 19 July 2022.

61 Arrow, 'Analog-to-Digital (ADC) Converter Types & Basic Functions', 5 February 2019, <https://www.arrow.com/en/research-and-events/articles/analog-to-digital-adc-converter-types-and-basic-functions>, accessed 19 July 2022.

62 Department for International Trade, 'OGEL and Goods Checker Tools', <https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/OGEL_GOODS_CHECKER_LANDING_PAGE/new>, accessed 20 July 2022.

63 Rajesh Uppal, 'DARPA's Ultrahigh Speed Analog-to-Digital Converter (ADC) to Improve Performance of Radar, Electronic Warfare and Communications', IDST, 25 January 2017, <https://idstch.com/technology/electronics/darpa-s-analog-to-digital-converter-adc-programs-to-improve-performance-of-radar-electronic-warfare-and-communications/>, accessed 20 July 2022.

64 ECCN 3A001.a.5.a.5 – an A/D converter with a 16-bit or greater resolution and output rate greater than 65 million words per second. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 – ELECTRONICS'.

65 Texas Instruments, 'TI At a Glance', <https://www.ti.com/about-ti/company/ti-at-a-glance.html>, accessed 19 July 2022.

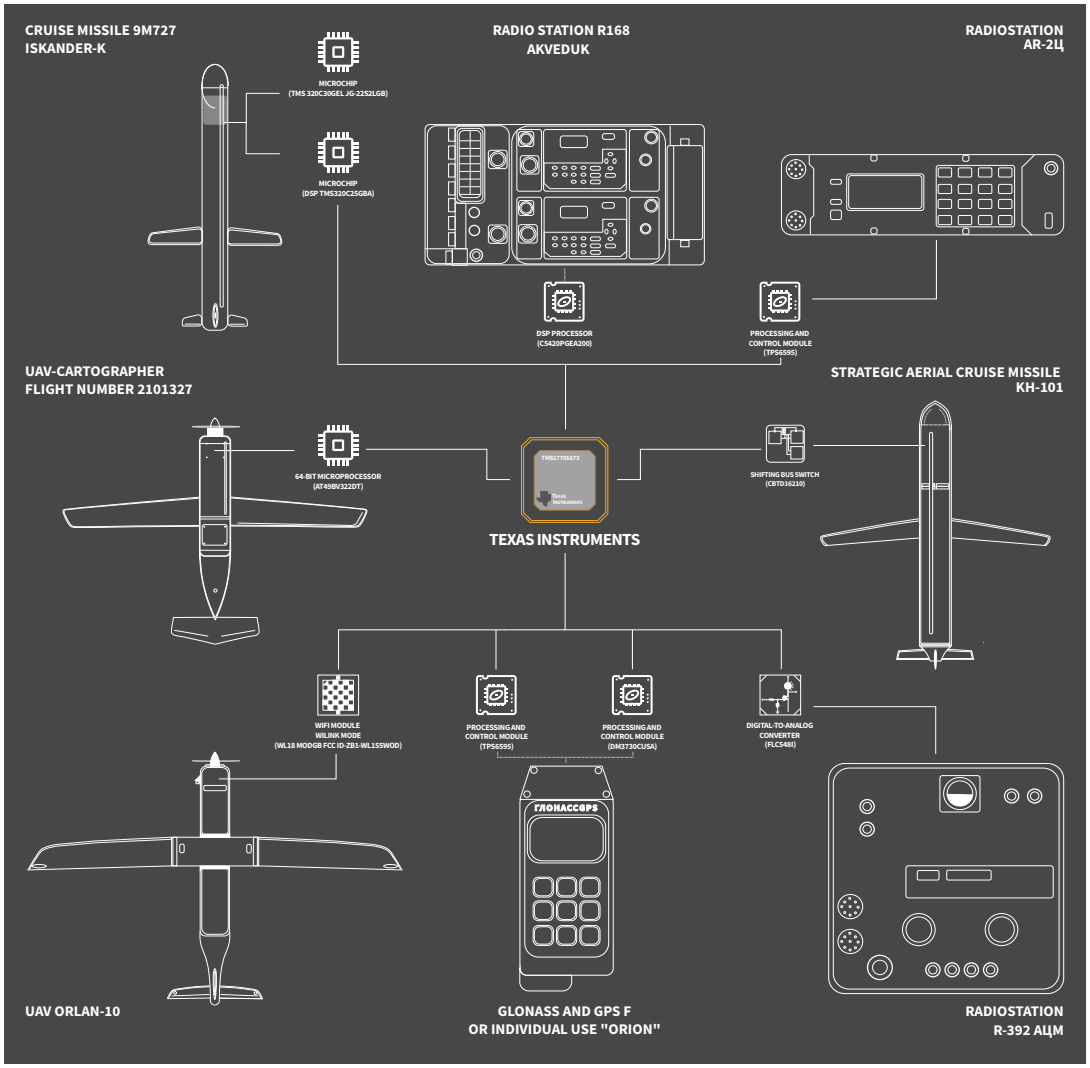
66 Texas Instruments, 'TI Fact Sheet', <https://web.archive.org/web/20160719151815/http://www.ti.com/corp/docs/company/factsheet.shtml>, accessed 19 July 2022.

67 Texas Instruments, 'Aerospace & Defense', <https://www.ti.com/applications/industrial/aerospace-defense/overview.html>, accessed 19 July 2022.

In the US, the company's military-grade and high performance components have been used in a variety of military systems, such as flight control units for aircraft, GPS receivers, radar systems, sonar systems, EW systems, smart munitions and countless others.[68] For example, the company's multicore digital signal processors are also popular for processing tasks in a range of high-performance radar systems,[69] including military synthetic aperture radars designed to collect imagery at night and through cloud.[70]

Over 50 unique components from Texas Instruments were discovered in several Russian systems, including digital signal processors found in various computing and processing modules in the 9M727 land-attack cruise missile, a CAN transceiver found in the electronic detonator of the KUB-BLA 'kamikaze' UAV, power management modules in an E95M target drone and in the Orlan-10 UAV, as well as audio codecs and converters in several of the radio sets used by the Russian Army.

Figure 9: Texas Instruments-Manufactured ECCN Components in Russian Weapons



Source: RUSI.

68 *Ibid.*

69 John McHale, 'High-Performance Radar Systems Enabled by New TI Multicore DSPs', Military Embedded Systems, 28 March 2012, <https://militaryembedded.com/radar-ew/signal-processing/high-performance-radar-systems-enabled-by-new-ti-multicore-dsps>, accessed 20 July 2022.

70 Dan Wang and Murtaza Ali, 'Multicore DSP Enhances Synthetic Aperture Radar Processing', Military Embedded Systems, 10 September 2013, <https://militaryembedded.com/radar-ew/signal-processing/multicore-aperture-radar-processing>, accessed 20 July 2022.

Other components produced by Texas Instruments were also found inside the Kh-101 ALCM, a sophisticated weapon used to strike targets deep in Ukraine, including critical infrastructure and urban population centres.[71] Some of these were in the Kh-101's processor module – a system which helps guide the missile to target – such as DS26C32ATM CMOS quad differential line receivers, which are produced to be compliant with military standards.[72]

At least 10 of the Texas Instrument components discovered in these weapon platforms are under US export controls. This includes the TMS320 C25GBA and TMS320 C30GEL digital signal processors, both present in the 9M727 GLCM.[73]

TOKYO VICE

While the US has often been 'target number one' for Russia's illicit procurement networks, other countries with sophisticated manufacturing and semiconductor industries have also been high on the Kremlin's shopping list.

In the late 1950s and early 1960s, the Japanese economic miracle of the post-war years propelled the country towards the top rankings of global economies – a transformation partly driven by the country's burgeoning semiconductor industry. But as Japanese conglomerates like Sony and Toshiba became household names, they also attracted the attention of the KGB's technical espionage teams.

In June 1971, the head of a hi-tech company in Japan operating under the Soviet codename TONDA provided his KGB handlers with two volumes of secret documents on a new microelectronic computer system to be used by US air and missile forces.[74] There were other technical intelligence coups in Japan and, in the late 1970s, Tokyo resident Oleg Guryanov told his staff that '[t]he proceeds from the operations these [Line X] officers carry out each year would cover the expenses of our entire Tokyo residency with money still left over. In fact, worldwide, technical intelligence all by itself covers all the expenses of the whole KGB foreign intelligence service'.[75]

Weapons platforms analysed for this report indicate that Japanese technology remains important for Russia's armed forces. A total of 34 unique components contained in the dataset were designed and manufactured by Japanese companies, making it the second most common country of origin outside of the US. These components came from over a dozen companies and include cameras produced by well-known companies like Panasonic and Canon, digital step attenuators produced by Fujitsu, an inertial measurement unit produced by TDK Corporation, and a model aircraft engine manufactured by Saito Seisakusho.

However, the most prevalent Japanese components were multilayer ceramic capacitors and surface mount inductors produced by Murata Manufacturing – one of Japan's oldest electronics companies. Founded in 1944, Murata primarily designs and manufactures ceramic-based passive components and solutions.[76] Unlike many other electronics firms, Murata's website kindly requests that its products are not used in either weapons of mass destruction or their conventional counterparts.[77]

71 Lorenzo Tondo, 'Russian Missiles Strike Kyiv for First Time in Three Weeks', *The Guardian*, 26 June 2022.

72 Texas Instruments, 'DS26C32ATM/NOPB - CMOS Quad Differential Line Receivers', <https://www.ti.com/product/DS26C32AT/part-details/DS26C32ATM/NOPB>, 20 July 2022.

73 ECCN 3A991.a.2 – a microprocessor or microcontroller with a clock frequency rate exceeding 25 MHz. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 – ELECTRONICS'.

74 Andrew and Mitrokhin, *The Mitrokhin Archive II*, p. 306.

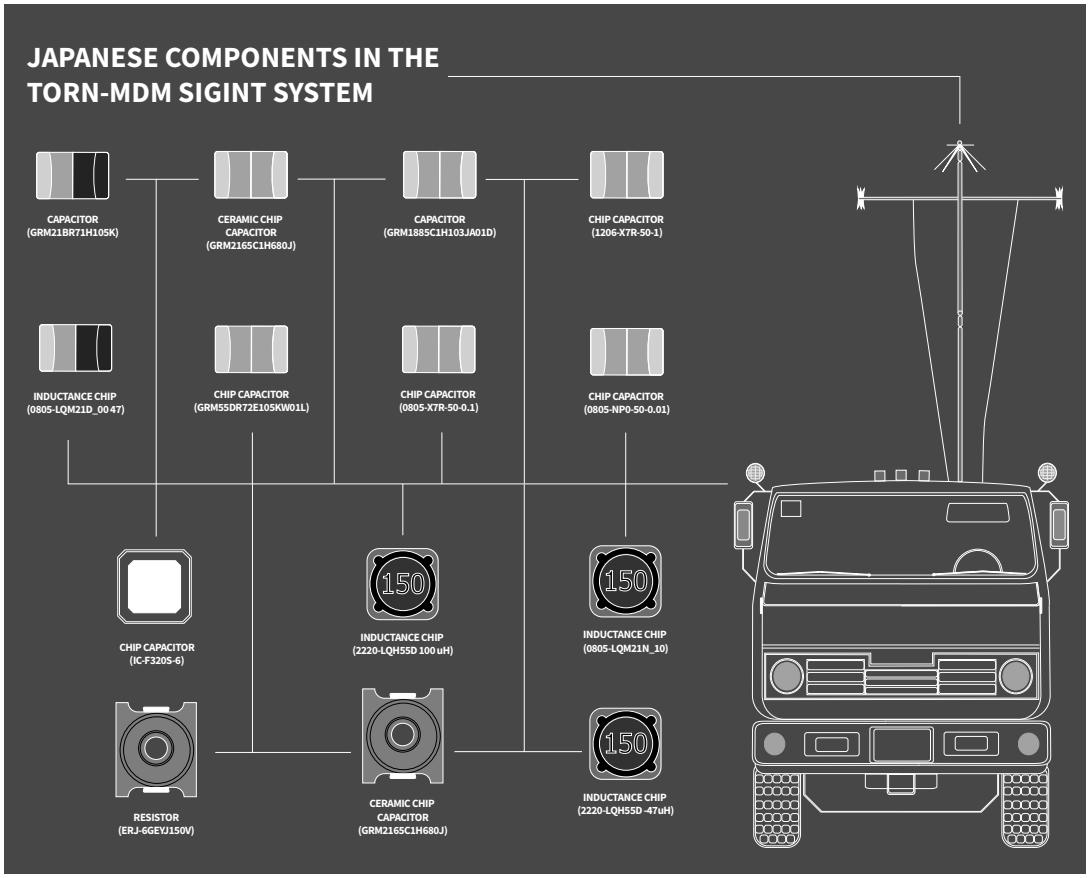
75 *Ibid.,* p. 308. Originally referenced in Stanilav Levchenko, *On the Wrong Side: My Life in the KGB* (University of Michigan: Pergamon-Brassey's International Defense Publishers: 1988), p. 104.

76 Murata Manufacturing, 'Facts and Figures', <https://corporate.murata.com/en-global/company/factsandfigures>, accessed 20 July 2022.

77 Murata Manufacturing, 'Restriction of Weapons of Mass Destruction and Conventional Weapons', <https://www.murata.com/en-global/support/militaryrestriction>, accessed 20 July 2022.

The Russians, however, appeared to have ignored this request, for several of Murata's components were found in the Torn-MDM SIGINT system and the military AR-2C radio set. The Torn-MDM SIGINT system is a relatively new platform designed to search, analyse and record radio signals, while determining the direction and location of the transmission within a radius of up to 70 km.[78]

Figure 10: Japanese Components in the Torn-MDM SIGINT System



Source: RUSI.

FROM EACH ACCORDING TO HIS ABILITY, TO EACH ACCORDING TO HIS NEEDS

Although East Asia's semiconductor industries have become an important part of Russia's military supply chain, the scientific and technological riches of the Western European countries were always coveted by Russia's special services and remain a priority target for the country's technical espionage teams.

These operations had begun in earnest even before the foundation of the Soviet Union on 28 December 1922. In 1921 or 1922, the 4th (Intelligence) Department of the Red Army General Staff – later to be renamed the GRU – dispatched Aaron and Abraham Ehrenlieb to Berlin where they established the Far Eastern Trading Company, otherwise referred to as Wostwag.[79] In a time-honoured tradition of using commercial front companies, the GRU operated Wostwag as a smoke screen for military intelligence and eventually granted the company control over Soviet arms exports.[80]

Over the course of the next century, Russia's S&T espionage and procurement operations have

78 Ukrainian Military Center, 'Ukrainian Army Captured Russian Torn-MDM SIGINT System', 17 March 2022, <https://mil.in.ua/en/news/ukrainian-army-captured-russian-torn-mdm-sigint-system/>, accessed 20 July 2022.

79 David R Stone, 'Soviet Arms Exports in the 1920s', *Journal of Contemporary History* (Vol. 48, No. 1, January 2013), pp. 57–77.

80 *Ibid.*

proved a constant thread connecting two often adversarial political and economic systems. But while the advent of the Cold War ushered in a wide-ranging embargo on technology exports to the Soviet Union,[81] the system's collapse in the early 1990s provided the Kremlin with the opportunity to legitimately purchase and integrate huge volumes of sophisticated technology into weapons systems that have been used to target Ukrainian and Syrian non-combatants and civilian infrastructure.

In fact, data analysed for this report indicates that components manufactured by European companies are prevalent in Russian military systems. The case of Catherine FC thermal sights – produced by the French company Thales – in Russian combat platforms is well documented.[82] Yet, what is less appreciated is how Russian procurement networks often target smaller, specialist European firms to acquire high-end equipment that cannot easily be sourced elsewhere.

WATCHING SWITZERLAND

Switzerland was the fourth-largest manufacturer of unique components found in Russian weapons systems, with a number of Swiss companies represented in the dataset, including STMicroelectronics and u-blox. A total of 18 unique components in the dataset were manufactured by Swiss companies.

STMicroelectronics is a Franco-Italian electronics and semiconductor manufacturer headquartered in Geneva.[83] The company primarily produces memory modules, microprocessors, transistors and microcontrollers, including the popular STM32 series.[84] Eight of these STM32 microcontrollers were recovered from a range of UAVs, including the Orlan-10, E95M, Eleron-3SV and KUB-BLA. Notably, these chips were common in several of these UAV's sub-systems, such as the flight controller, navigation and positioning system, and power supply control board.

Given the scale of Russia's UAV fleet and the high attrition rates associated with operating these platforms in a contested airspace, Russia's armed forces must have been able to acquire these components in significant quantities prior to the February 2022 invasion of Ukraine. Yet, several of the STM32 microcontrollers present in these systems are under US export controls.[85] Other products produced by STMicroelectronics include a PD55003 radio frequency power transistor found in an R-168 radio set and two 44-lead thin quad flat packages recovered from a Kh-101 ALCM's SN-99 satellite navigation system.

u-blox, meanwhile, is a designer and supplier of semiconductors and modules that support global navigation satellite systems (GNSS), including receivers for GPS, GLONASS, Galileo, BeiDou and QZSS.[86] Its M8 series of GNSS modules were present in the Orlan-10's GPS tracker and navigation and positioning system, as well as in the AR-2C radio set. These modules are also under US export controls.[87]

GOING DUTCH

A total of 14 components originated from Netherlands-based manufacturers, of which 10 came from NXP Semiconductors as well as two from its former subsidiary Nexperia. Despite the low number of components in the total dataset,

81 Coordinating Committee for Multilateral Export Controls (CoCom).

82 Andrew Rettman, 'French Eyes for a Russian Tiger', *euobserver*, 25 August 2015, <https://euobserver.com/investigations/129953>, accessed 20 July 2022; Oleksandr Dubilet, 'French Arms Firm Busts Sanctions to Help Russia Build Weapons', *New Voice of Ukraine*, 21 June 2022, <https://english.nv.ua/business/total-isolation-of-russia/military-thermal-imagers-for-the-russian-army-the-french-company-thales-cooperated-with-russia-aft-50247461.html>, accessed 20 July 2022.

83 LinkedIn, 'STMicroelectronics', <https://www.linkedin.com/company/stmicroelectronics/>, accessed 20 July 2022.

84 STMicroelectronics, 'Homepage', <https://www.st.com/content/st_com/en.html>, accessed 20 July 2022.

85 ECCN 3A991.a.2 – a microprocessor or microcontroller with a clock frequency rate exceeding 25 MHz. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 – ELECTRONICS'.

86 u-blox, 'We Build to Last', <https://www.u-blox.com/en/we-build-last>, accessed 20 July 2022.

87 ECCN 7A994 – navigation direction finding equipment, airborne communication equipment, aircraft inertial navigation systems and other avionic equipment. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 7 - NAVIGATION AND AVIONICS', <https://www.bis.doc.gov/index.php/documents/regulations-docs/2339-category-7-navigation-and-avionics-2/file>, accessed 20 July 2022.

NXP components were present in 10 of the 27 systems analysed.

Most prevalent were pressure sensors, such as the MPXV5004DP, MPXV5010DP and MPXV5010GP, which were found in the flight controllers of the KUB-BLA, the Orlan-10 and the E95M UAVs. The flight controller for the KUB-BLA also contained an NXP-produced microcontroller, LPC2368FBD100, an item controlled by the US.[88] Other NXP components include radio frequency transistors that were found in several of the radio sets and the GLONASS/GPS GROT-M navigation equipment. Notably, the Kh-101 ALCM's BT33 processor module contained bus transceivers produced by both NXP and Nexperia.

LONDON CALLING

As an advanced economy with an extensive defence industrial base, the UK has always been at the forefront of Russia's technical espionage operations. A large complement of the KGB's Line X officers were reportedly based in London in the 1980s and engaged in this effort, with one of their key targets being the aerospace and defence conglomerate Rolls-Royce.[89]

While only five UK-made components were discovered inside the recovered weapon systems, some of these parts are highly specialised – such as oscillators and standard crystals. These particular components were designed and produced by Golledge Electronics, which supplies frequency control products to the electronics industry.[90] Based in Southwest England, the company exports its products to over 50 countries.[91] Just like other companies described above, the company also produces a range of commercial off-the-shelf products to meet the requirements for several military standards.[92] In early March 2022, the company reported that it had ceased business in Russia on 24 February following the invasion of Ukraine.[93]

Components produced by Golledge were recovered from some of the more sophisticated Russian systems, such as the Torn-MDM and the Tor-M2 SAM system. The former contained one of the company's HC49 standard crystals, while the latter's specialised digital computing unit included a GXO-U100F oscillator. Both components are used to generate an electrical signal at a precise frequency by utilising the vibrating crystal's mechanical resonance made of piezoelectric material.[94] This is critical for use in systems like the Tor-M2 that use radar to detect and track targets and to improve the effectiveness of SIGINT and EW systems.

BERLIN STATION

While Russian espionage networks have operated from a range of European countries, Germany has also often been at the heart of Russian procurement schemes. A key target in the Cold War, East Germany was a hub for Soviet spies looking to procure Western technology. Line X agents, recruited by the Russian intelligence services in East Germany, could easily be dispatched into the Federal Republic to collect information and penetrate important German companies.[95] In 1985, an assessment claimed that West Germany was 'ineffective' at controlling illicit exports to the Soviet Union and would only act under US pressure.[96]

88 ECCN 3A991.a.2 – a microprocessor or microcontroller with a clock frequency rate exceeding 25 MHz. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 – ELECTRONICS'.

89 Office of the Secretary of Defense, 'Soviet Acquisition of Militarily Significant Western Technology: An Update', September 1985, <https://apps.dtic.mil/sti/pdfs/ADA160564.pdf>, accessed 21 July 2022.

90 Golledge Electronics, 'About Us', <https://www.golledge.com/about-us/>, accessed 20 July 2022.

91 *Ibid.*

92 Golledge Electronics, 'Mil-COTS Frequency Components for Defence and Aerospace', 28 June 2016, <https://www.golledge.com/news/using-mil-cots-for-defence-and-aerospace/>, accessed 20 July 2022.

93 Golledge Electronics, 'Golledge Have Withdrawn from Our Business in Russia', 11 March 2022, <https://www.golledge.com/news/russian-business-withdrawal-aid-for-ukraine/>, accessed 20 July 2022.

94 Sluiceairfair.com, 'What is the Principle of Piezoelectric Oscillator?', 31 August 2020, <https://www.sluiceartfair.com/2020/popular-lifehacks/what-is-the-principle-of-piezoelectric-oscillator/>, accessed 21 July 2022.

95 Office of the Secretary of Defense, 'Soviet Acquisition of Militarily Significant Western Technology: An Update'.

96 Daniel Salisbury, 'Countering a Technological Berlin Tunnel: North Korean Operatives, Helicopters and Intelligence in the Cold War Illicit Arms Trade, 1981-1986', *Intelligence and National Security* (2022).

That same year, US authorities pursued a large and complex Soviet microelectronic procurement network as part of Operation *Exodus*, a customs-led attempt to stem the flow of critical technology to Russia. Directed by a German national named Richard Mueller, the network aimed to 'divert sophisticated computer equipment' to improve the Soviet Union's manufacturing capabilities for military-grade semiconductors.[96] In the mid-1980s, US customs identified Mueller as one of the world's most wanted arms smugglers.[97]

But there were other high-profile proliferation agents working from German soil. Babeck Seroush, an Iranian with an office in Cologne and Moscow,[98] was indicted in 1984 by a US court for exporting 143 semiconductors for use in missile guidance systems and night vision equipment to North Korea.[99] Only two years before, Seroush, who was also alleged to have been recruited by the KGB,[100] was implicated in a case involving the diversion of electronic components to the Soviet Union.[101]

At the time, Vladimir Putin himself and Sergey Chemezov – the current head of Russia's largest defence conglomerate – were both KGB officers based in Dresden.[102] A grainy photo taken in the 1980s shows them together in Dresden as young men.[103] As Putin rose to power, Chemezov followed, and in 2007 Putin placed his old colleague at the helm of Rostec (State Corporation for Assistance to Development, Production and Export of Advanced Technology Industrial Product 'Rostec'), a post he still holds today.[104]

Figure 11: Putin and Chemezov, Reportedly Taken in 2021

Source: Kremlin.ru.

96 Ruth Marcus, '"Entrepreneurs" of War', *Washington Post*, 10 August 1985.

97 *Ibid.*

98 Ellan Cates, 'A West German Exporter Has Been Charged with Conspiracy…', *UPI*, 5 November 1984, <https://www.upi.com/Archives/1984/11/05/A-West-German-exporter-has-been-charged-with-conspiracy/3117468478800/>, accessed 20 July 2022.

99 *Ibid.*

100 Salisbury, 'Countering a Technological Berlin Tunnel'.

101 *AP News*, 'Exec Charged with Conspiring to Ship Computer Boards to Soviet Union', 25 April 1985.

102 *The Economist*, 'The Making of a Neo-KGB State', 23 August 2007.

103 Rob Lee (@RALee85), 'Sergei Chemezov and Vladimir Putin in Dresden in the 1980s and today', Twitter, 20 July 2021, <https://twitter.com/ralee85/status/1417560713862828035?lang=en>, accessed 20 July 2022.

104 Rostec, 'Sergey Chemezov Reports to President of Russia on Rostec 2021 Performance', 18 May 2022, <https://rostec.ru/en/news/sergey-chemezov-reports-to-president-of-russia-on-rostec-2021-performance-/>, accessed 20 July 2022.

In recent years, Germany has continued to be a target both for S&T espionage and procurement networks looking to lay their hands on sophisticated technology. In May 2021, a German national was arrested for shipping dual-use goods to a company operated by Russia's intelligence services.[105] Barely a month later, German authorities arrested a Russian scientist for stealing aeronautical secrets and missile technology from research centres in Augsburg.[106]

RUSI found 10 components produced by German companies in seven of the systems. The most common were filters and surface mount inductors that were manufactured by EPCOS AG and found in several sub-systems of the Torn-MDM SIGINT system. EPCOS AG was originally formed in 1999 from Siemens Matsushita Components, a joint venture between Germany's Siemens and Japan's Matsushita.[107] The company was later purchased by Japan's TDK Corporation in 2009 and renamed to TDK Electronics AG.[108] The company's product catalogue includes capacitors, ceramic components, EMC filters, inductors, radio frequency modules and others.[109]

Meanwhile, both the Eleron-3SV and KUB-BLA UAVs were discovered using air blades produced by Graupner GmbH and Aero Naut, respectively. However, a US export-controlled item was recovered from one Russian weapon system. This was a Würth Elektronik GmbH-manufactured LAN transformer[110] found in a special computing module in the R-330BMV EW system.

105 *AP News*, 'Germany Arrests Businessman Over Dual-Use Exports to Russia', 18 May 2021.

106 Matthias von Hein, 'Russian Scientist Stands Trial for Espionage in Germany', *DW*, 17 February 2022.

107 Gerhard Fasol, 'TDK Acquires Passive Electronic Component Maker EPCOS', Europe-Japan, 31 July 2008, <https://eu-japan.com/2008/07/tdk-epcos/>, accessed 20 July 2022.

108 Interference Technology, 'EPCOS AG Changes Its Name to TDK Electronics AG', 5 October 2018, <https://interferencetechnology.com/epcos-ag-changes-its-name-to-tdk-electronics-ag%E2%80%AF/>, accessed 20 July 2022.

109 TDK Corporation, 'Acquisition of EPCOS AG – Becoming the Global Leader in the Electronic Components Industry', 2009, <https://www.tdk.com/ir/ir_library/annual/web/lib20405.pdf>, accessed 20 July 2022.

110 ECCN 3A991.b.2.a – a microwave monolithic integrated circuit power amplifier rated for operation at frequencies exceeding 2.7 GHz and up to and including 6.8 GHz with a fractional bandwidth greater than 15%. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 – ELECTRONICS'.

An Inside Look at Russian Missiles

'[C]ombat operations during military conflicts in the near future will feature struggles between advanced technologies, with the most critical of those being aerospace attack weapons as well as air and missile defense systems', noted Yan Novikov, director general of Russian state-owned defence contractor Almaz-Antey, on 6 December 2021.[111]

In the opening hours of the invasion, the Russian armed forces aimed to disrupt and neutralise Ukrainian air defences and C4ISR[112] systems, firing salvos of cruise and ballistic missiles at a range of facilities.[113] Later, the target list was expanded to include military infrastructure including barracks housing foreign fighters, rail infrastructure to disrupt Western supply lines, fuel depots, arms factories, and even civilian targets such as hospitals and shopping centres.

The Russian armed forces have an extensive arsenal of these weapons, reportedly expending over 2,000 missiles by the beginning of May.[114] These have included the Kh-101 ALCM, used by the Russian Air Force to strike targets from the safety of Russian air space,[115] while the Russian ground forces have deployed 9M720 and 9M727 Iskander ballistic and cruise missiles often fired from Russian territory.[116]

While many of these systems were destroyed in the process of hitting their targets, several have been recovered and later disassembled, providing an unparalleled insight into their construction.

111 Yan Novikov, 'Almaz-Antey Director: Air and Space Capabilities Will Decide Tomorrow's Conflicts', *DefenseNews*, 6 December 2021.

112 Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR)

113 Justin Bronk, 'The Mysterious Case of the Missing Russian Air Force', *RUSI Commentary*, 28 February 2022.

114 US Department of Defense, 'Senior Defense Official Holds a Background Briefing', transcript, 2 May 2022, <https://www.defense.gov/News/Transcripts/Transcript/Article/3017053/senior-defense-official-holds-a-background-briefing/>, accessed 20 July 2022.

115 *NBC News*, '2 Reported Killed as Russian Missiles Strike Kyiv for First Time in Weeks', 26 June 2022.

116 *Kyiv Independent*, 'General Staff: Russia Deploys Iskander Missile Launchers to Belgorod Oblast', 22 May 2022.

02

These weapons integrate a wide array of subsystems and point to complex networks of manufacturers involved in the production of their constituent parts. But while the branches of these networks may be expansive, they often trace back to the same roots: Russia's state-owned principal defence conglomerates Rostec and Almaz-Antey (OAO Concern VKO 'Almaz-Antey'), both targeted by Western countries for their central role in supplying the Russian armed forces.

Established in 2007, Rostec has been headed by Putin confidant Chemezov since its inception.[117] Almaz-Antey, meanwhile, was created by presidential decree in 2002 and is led by Yan Novikov. Between 2014 and 2016, however, the company's board of directors was also headed by Chemezov.[118]

Together, these sprawling organisations operate a bewildering array of research institutes, design bureaus, manufacturing plants and companies that feed into the design, development and production of Russian missiles and other military systems.

THE ISKANDER 9M727

The 9M727 is a Russian medium-range GLCM that flies at low altitudes to evade radar and reduce the risk of interception.[119] In order to navigate to its target and make course corrections mid-flight, the missile contains a number of sensors and internal computer systems designed to translate external signals into digital inputs.

Figure 12: Images of the 9M727 Cruise Missile

Source: RUSI.

117 *Reuters*, 'Putin Ally Chemezov Says Russia Will Be the Victor', 10 March 2022.

118 Almaz-Antey, 'History', <http://www.almaz-antey.ru/en/istoriya/>, accessed 21 July 2022.

119 CSIS Missile Defense Project, '9M729 (SSC-8)', last updated 31 March 2022, <https://missilethreat.csis.org/missile/ssc-8-novator-9m729/>, accessed 21 July 2022.

Two of the missile's most important signal processing systems are the Zarya and Baget-62-04 computers, which process radar and television guidance (TGM) data, respectively. One of the missile's most important sensors is a system attached to its fuselage that processes GPS and GLONASS signals – the SN-99 (CH-99).

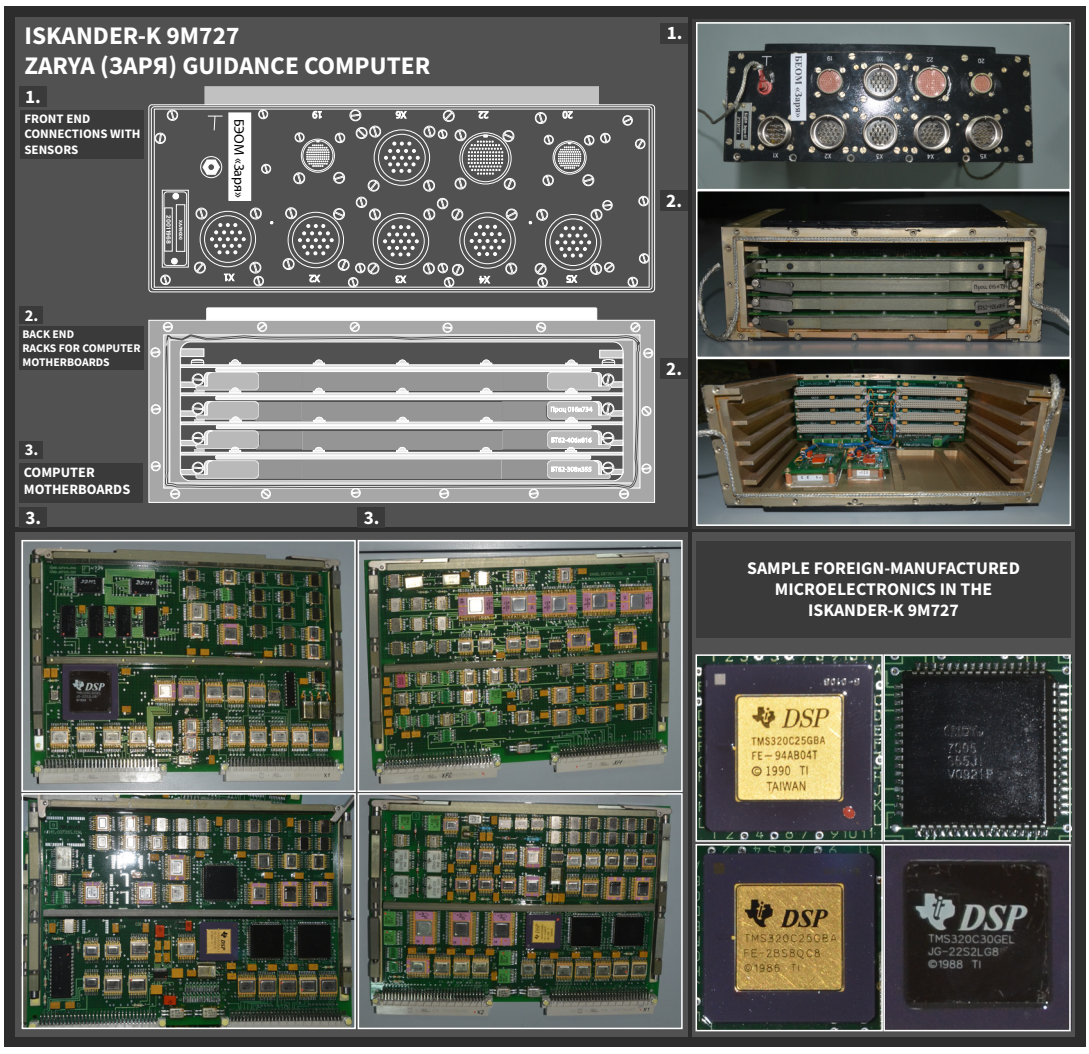
A study of the constituent parts of these systems reveals the extensive use of Western-produced components in their construction, while their Russian-based manufacturing chains often ultimately lead back to Rostec and Almaz-Antey.

ZARYA RADAR PROCESSING COMPUTER

The Zarya computer sits at the front end of the 9M727 missile and is fitted within an all-metal chassis and secured within a locking metal retainer. The robust construction is designed to protect the computer from vibration and shocks that could disrupt its operation as the missile launches and navigates to its target. The metal chassis also protects the computer from electromagnetic interference, as does the presence of a braided metal gasket that seals the computer when installed inside the 9M727 fuselage.

The Zarya is passively cooled, meaning that no fans or air vents are required to manage temperatures. This provides the electronics with some resistance to water damage and to vibrations that could interfere with its operations if the system relied on an alternative, active cooling mechanism.

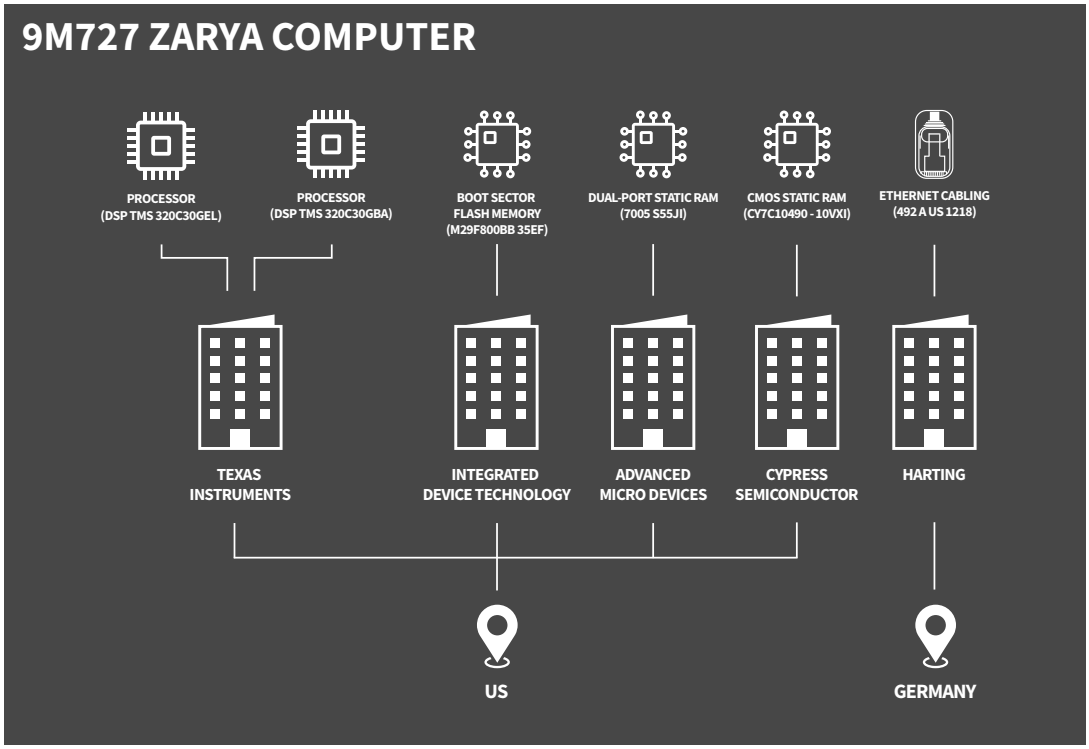
Figure 13: Disassembly of the Zarya Computer



Source: RUSI.

At least some of the models of the Zarya computers appear to have historically been manufactured by entities linked to the production of Russian military systems and – ultimately – to Almaz-Antey.[120] However, despite this, the Zarya computer recovered from the 9M727 contained several Western-sourced components, including digital signal processors, flash memory modules, static RAM modules, and ethernet cabling that originated from US and German companies.

Figure 14: Western Components in the Zarya Computer



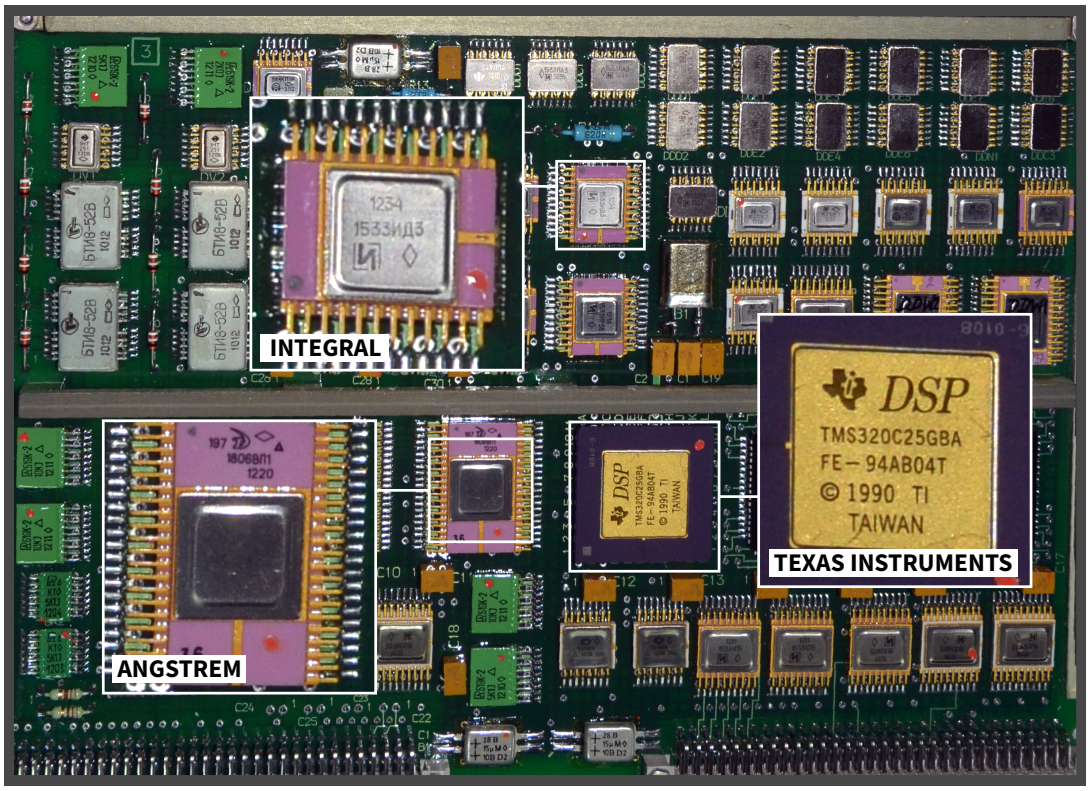
Source: RUSI.

120 A document attributed to A.N. Shishkov of the Moscow Aviation Institute notes that, in the early 1990s, a series of Zarya models was produced by an 'NII Priborostroeniya' in Moscow. A H Shishkov, 'Lekcija Mikroprocessory' ['Microprocessor Lecture'], Moscow Aviation Institute, p. 38, <http://frela-mk.narod.ru/olderfiles/1/Lekcciya_3_4_Mikroproccessory.pdf>, accessed 28 July 2022. This may refer to either the V.V. Tikhomirov Scientific Research Institute of Instrument Design (NIIP) (Nauchno-izsledovatel'skij institut priborostroenniya imeni V.V. Tikhomirova) or the State Research Institute of Instrument Design (GosNIIP) (Gosudarstvennyj nauchno-izsledovatel'skij institut priborostroeniya). Both entities have been involved in the production of military technology. See V.V. Tikhomirov Scientific Research Institute of Instrument Design, 'Eksportnaya produkciya' ['Export Production'], <https://www.niip.ru/catalog/eksportnaya-produktsiya>, accessed 26 July 2022; *Army Recognition*, 'Russia Has More SSC-8 Cruise Missiles Than Expected, with Conflictual Range', 11 February 2019, <https://www.armyrecognition.com/february_2019_global_defense_security_army_news_industry/russia_has_more_ssc-8_cruise_missiles_than_expected_with_conflictual_range.html>, accessed 28 July 2022; Russian Strategic Nuclear Forces, 'Cruise Missiles and INF - What About 9M729?', 23 June 2015, <https://webcache.googleusercontent.com/search?q=cache:kGNi1MZkOSIJ:https://russianforces.org/blog/2015/06/cruise_missiles_and_inf_-_what.shtml+&cd=2&hl=en&ct=clnk&gl=de>, accessed 28 July 2022. At the time of writing, NIIP was controlled by Almaz-Antey and Rostec. See Oruzhiye Rossii [Russian Weaponry], 'Nauchno-izsledovatel'skij institut priborostroenniya imeni V.V. Tikhomirova, AO' ['V.V. Tikhomirov Scientific Research Institute of Instrument Design, JSC'], <https://www.arms-expo.ru/armament/ members/625/83161/>, accessed 21 July 2022. GosNIIP was part of Almaz-Antey as recently as 2018 and still prominently features the Almaz-Antey logo on its webpage. See GosNIIP, 'Akcionernoye obschestvo "Gosudarstvennyj nauchno-izsledovatel'skij institut priborostroeniya"' ['Joint Stock Company "State Research Institute of Instrument Design"'], <http://www.gosniip.ru/>, accessed 28 July 2022; Vladimir Medvedev, 'Frontovyje aviacionnye pribory i ih sozdateli' ['Front-line Aviation Instruments and Their Creators'], *Nacional'naya oborona* [*National Defence*], 27 February 2018, <https://2009-2020.oborona.ru/includes/periodics/defense/2018/0227/122323529/print.shtml>, accessed 28 July 2022.

Notably, the core processing on the Zarya system appears to be performed by a Texas Instruments digital signalling processor. These processors are used for manipulating streams of data in repetitive ways, and could perform the filtering, manipulation and conversion of data collected by the missile's onboard sensors.

The digital signalling processing chips used in the Zarya are the Texas Instruments TMS320 series, initially released in 1983, but which have had various revisions since. The boards inspected by RUSI in the 9M727 have both the C25 and C30 variants present, the latter being capable of up to 50 million operations per second – likely to be the top of the available market at the time of construction. The microchips are dated to 1988 and 1990, which indicates the system was likely designed and constructed in the late 1980s into the early 1990s. The digital signalling processors also appear to be coupled with other Western-sourced memory chips produced by either Integrated Device Technology or Cypress Semiconductor.

Figure 15: Angstrem and Integral Microchip on the Zarya Circuit Boards



Source: RUSI.

The metal-packaged integrated circuit devices visible in the system are primarily of Soviet origin, which can be determined by the logos on the domestic manufactured chips produced by Angstrem and Integral. Up until the fall of the Soviet Union, Angstrem and Integral, alongside Moscow-based PAO Mikron,[121] were the country's principal entities producing integrated circuits.

Angstrem was founded in 1963 under the auspices of the Leningrad-based Scientific Research Institute of Fine Mechanics and developed the first domestically produced 'Tropa' series of microchips.[122] The company has since produced over 2,000 types of microchips and semiconductor devices for use in missile guidance systems, space and aviation technology, personal computers and

121 Mikron's history dates back to the late 1950s and can be traced to the Voronezh Plant of Semiconductor Devices (Voronezhskij zavod poluprovodnikovyh priborov), which later became VZPP-Mikron. Mikron has historically produced components for use in military systems. See Mikron, 'Mikron History', <https://en.mikron.ru/company/history/>, accessed 30 June 2022.

122 Angstrem, 'Katalog produkcii' ['Product Catalogue'], 2022, <https://tinyurl.com/6mcp38rp>, accessed 21 July 2022.

micro-calculators, among other applications.[123]

In 2018, over 91% of Angstrem's overall sales were of products with military applications; for sales on the domestic market, that number was over 96%.[124] Angstrem is a majority shareholder in AO Angstrem-T, whose assets were blocked by the Office of Foreign Assets Control (OFAC) on 22 February 2022.[125]

Integral, meanwhile, is a Belarus-based producer of integrated systems, discrete semiconductor devices and information display systems, including – according to the company's webpage – for integration into specialised equipment deployed in extreme conditions.[126] Integral began production in the 1960s but was sanctioned by OFAC on 24 February 2022 in relation to the Russian invasion of Ukraine.[127]

BAGET COMPUTING MACHINE

Another of the computers found inside the Iskander-K 9M727 is the Baget-62-04 – a television guidance processing system that is primarily used in the terminal phase to ensure pinpoint accuracy. The Baget family of computers is described in a recent article by a researcher from the Scientific Research Institute for System Analysis of the Russian Academy of Sciences (SRISA RAS) as high-performance devices for signal processing.[128]

Like the Zarya computer, the Baget-62-04's electronics are encased within a specialised system designed to protect them from high-destructive load factors and electromagnetic interference. The Baget-62-04 also contains a range of Western-manufactured components including microprocessors, FPGAs, SRAM chips, crystal oscillators, connecting sockets and a range of others.

123 *Ibid.*

124 Angstrem, 'Godovoj otchet Akcionernogo obschestva 'Angstrem' za 2018 god' ['Yearly Report of Joint-Stock Company "Angstrem" for the Year 2018'], report confirmed by the company general director and head chief accountant on 28 June 2019, p. 7. Accessed at *Interfax,* 'AO 'Angstrem' ['JSC 'Angstrem'], Centr Raskrytiya Korporativnoj Informacii [Corporate Information Discovery Centre], <https://www.e-disclosure.ru/portal/files.aspx?id=3782&type=2&attempt=1> , accessed 1 July 2022.

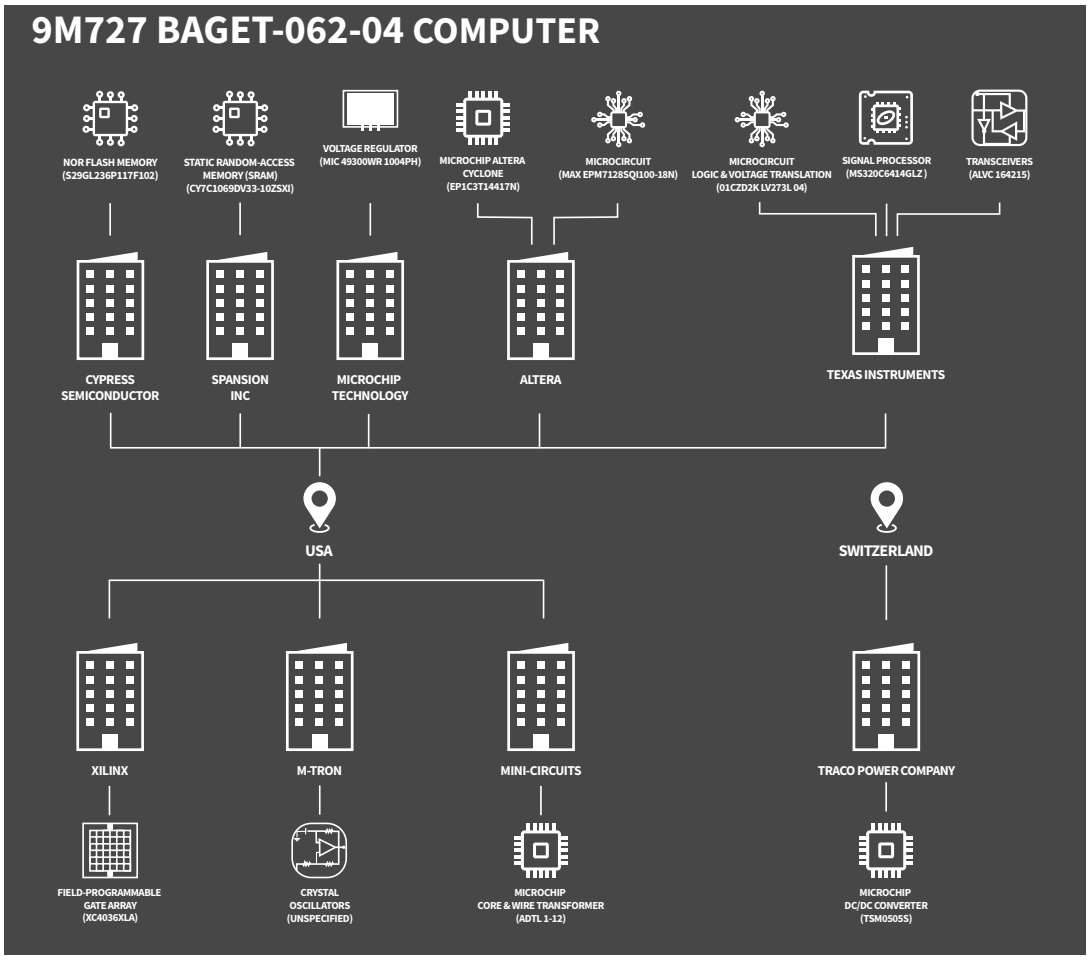
125 US Department of the Treasury, 'U.S. Treasury Imposes Immediate Economic Costs in Response to Actions in the Donetsk and Luhansk Regions', press release, 22 February 2022, <https://home.treasury.gov/news/press-releases/jy0602>, accessed 21 July 2022.

126 Integral, 'Produkciya' ['Products'], <https://integral.by/ru/products>, accessed 20 July 2022.

127 US Department of the Treasury, 'U.S. Treasury Imposes Immediate Economic Costs in Response to Actions in the Donetsk and Luhansk Regions'.

128 Antonov A A and A A Krasnyuk, 'The Internal Structure of Microprocessors for Industrial Control and Data Processing Systems', *IOP Conference Series: Materials Science and Engineering* (No. 1061, 2021).

Figure 16: Western Components in the Baget-62-04



Source: RUSI.

The Baget series traces its lineage back to Russian government efforts – following the collapse of the Soviet Union – to domestically manufacture computers and components for military applications to reduce reliance on foreign suppliers.[129] A 2017 brochure published by the Russian manufacturers shows that a possible descendant of the Baget 64-02 is intended for use as an onboard control system in aviation complexes as well as in ground- and air-based high-precision weapons complexes.[130]

Co-authored by the AO Design Bureau 'Korund-M' (KB Korund-M) and Russia's SRISA RAS, the brochure advertises a range of Baget computers and domestically manufactured microchips designed for military applications.

129 AO Konstruktorskoe b'uro (KB) Korund-M (JSC Design Bureau (DB) Korund-M) and Federal'noe gosudarstvennoe uchrezhdeniye Federal'nyj nauchnyj centr nauchno-izsledovatel'skij institute sistemnyh izsledovanij rossijskoj akademii nauk [Federal State Institution 'Scientific Research Institute for Systems Analysis of the Russian Academy of Sciences (FSI FSC SRISA RAS)], 'Perspektivnye EVM semejstva Baget' ['Prospective Computers of the Baget Family'], 2017, pp. 2–3.

130 *Ibid.*

Figure 17: Modern Baget Computer Systems Advertised by KB Korund-M and SRISA RAS

Source: Korund-M and SRISA RAS Brochure.

KB Korund-M, which seems to be a design bureau of SRISA RAS,[131] notes on its webpage that its products have been deployed in Russian military systems, including the Iskander missile complex, and that it continues to produce computers with military applications and to conduct R&D related to the computing needs of the Russian Ministry of Defence.[132] SRISA RAS was sanctioned by OFAC on 2 August 2022.[133] KB Korund-M is not sanctioned by Western governments.[134]

The Baget-62-04 is also named in the annual reports of AO Serpukhov Metallist Plant, which claim that the company produced 222 Baget-62-04 computers for the Iskander-M missile in 2013, with plans to produce 269 Baget-62-03 computers the following year.[135] The plant's annual reports continued to reference involvement in the production of Baget

131 One of the company's founders is Vladimir Betelin, who is also the scientific director at SRISA RAS. See Federal Government Institution Scientific Research Institute for Systems Analysis of the Russian Academy of Sciences, 'Betelin Vladimir Borisovich', <https://www.niisi.ru/betelin.htm>, accessed 25 July 2022. In Russian federal tax documents dated 24 July 2020, Betelin is listed as the general director and principal shareholder of AO KB Korund-M. Russian federal tax documents dated 4 December 2021 also listed Betelin as the director of Autonomous Non-Commercial Organisation Design Bureau Korund-M, while SRISA RAS was listed as a shareholder of the company. Russian federal tax documents dated 16 June 2022 still list Betelin as director of the company, but make no mention of SRISA RAS. Russia Federal Tax Registry documents can be accessed through Sayari Labs, <https://sayari.com/>, accessed 22 July 2022.

132 Konstruktorskoye B'uro Korund-M [Design Bureau Korund-M], 'O "Korund-M"' ['About "Korund-M"'], <https://kbkorund.ru/about>, accessed 26 July 2022.

133 US Department of State, 'Imposing Additional Costs on Russia for Its Continued War Against Ukraine', fact sheet, 2 August 2022, <https://www.state.gov/imposing-additional-costs-on-russia-for-its-continued-war-against-ukraine/>, accessed 2 August 2022.

134 It appears that some models of the Baget – namely, the Baget-53 computers – have also been manufactured by Ramenskoye Instrument-Making Design Bureau [Ramenskoye 'Priborostroitel'noye konstruktorskoye b'uro']. See Open Joint-Stock Company 'Ramenskoye Instrument-Making Design Bureau' (OJSC 'RIDB'), 'Katalog produkcii elektronnogo napravleniya "OAO Ramenskoye Priborostroitel'noye Konstruktorskoye B'uro"' ['Electronic Product Catalogue of the OJSC "Ramenskoye Instrument-Making Design Bureau"'], 2013, p. 14, <https://mniirip.ru/sites/default/files/articles/katalog_elektronnogo_napravleniya_rpkb.pdf>, accessed 20 July 2022.

135 'Godovoj otchet Otkrytogo akcionnernogo obschestva "Serpukhovskij zavod 'Metallist'" za 2013 god' ['Annual Report of the Open Joint Stock Company "Serpukhov Plant 'Metallist'" for the Year 2013'], 2014, p. 16. Accessed at *Interfax*, 'AO Serpukhovskij Zavod "Metallist"' ['JSC "Serpukhov Plant 'Metallist'"'], Centr Raskrytiya Korporativnoj Informacii [Corporate Information Discovery Centre], <https://www.e-disclosure.ru/portal/files.aspx?id=23097&type=2>, accessed 1 July 2022.

computers as recently as the 2020 report, published in 2021.[136] The 2021 annual report, released in June 2022, makes no reference to the Baget computers.[137]

Established in November 1943 by the federal defence committee of the Soviet Union, the Serpukhov Metallist Plant is a sprawling facility that has been historically involved in the production of Soviet and Russian military technology,[138] and has reportedly continued to produce critical military components until more recently.[139] As of December 2021, the plant was owned by JSC NPO High Precision Systems (AO 'NPO Vysokotochnye Kompleksy') of Rostec.[140]

NPO High Precision Systems is a Russian state-owned holding company sanctioned by the US Treasury in March 2022. According to the US Treasury, some of the missile systems produced by NPO High Precision Systems – including Iskanders – were brought to the Russia–Ukraine border in advance of the February 2022 invasion.[141]

GUIDANCE SYSTEMS

For nearly two decades, Russian military doctrine has relied on the use of long- and medium-range cruise missiles to strike at key critical military infrastructure deep inside an opponent's territory. In order to ensure these weapons hit their targets, the Russian armed forces have developed advanced inertial and navigation sensors to direct the missile while manoeuvring at low altitude to avoid air defences. One of the critical sensors found on both the 9M727 and the Kh-101 air-launched cruise missile is the GLONASS and GPS guidance unit SN-99 (CH-99).

136 See, for example, 'Godovoj otchet Otkrytogo akcionnernogo obschestva "Serpukhovskij zavod 'Metallist' za 2020 god"' ['Annual Report of the Open Joint Stock Company "Serpukhov Plant 'Metallist' for the Year 2020"'], 2021, pp. 16, 31. Accessed at *Interfax*, 'AO Serpukhovskij Zavod "Metallist"' ['JSC "Serpukhov Plant 'Metallist'"'], Centr Raskrytiya Korporativnoj Informacii [Corporate Information Discovery Centre], <https://www.e-disclosure.ru/portal/files.aspx?id=23097&type=2>, accessed 1 July 2022.

137 'Godovoj otchet Otkrytogo akcionnernogo obschestva "Serpukhovskij zavod 'Metallist' za 2021 god"' ['Annual Report of the Open Joint Stock Company "Serpukhov Plant 'Metallist'" for the Year 2021'], 2022. Accessed at *Interfax,* 'AO Serpukhovskij Zavod "Metallist"' ['JSC "Serpukhov Plant 'Metallist'"'], Centr Raskrytiya Korporativnoj Informacii [Corporate Information Discovery Centre], <https://www.e-disclosure.ru/portal/files.aspx?id=23097&type=2>, accessed 28 July 2022.

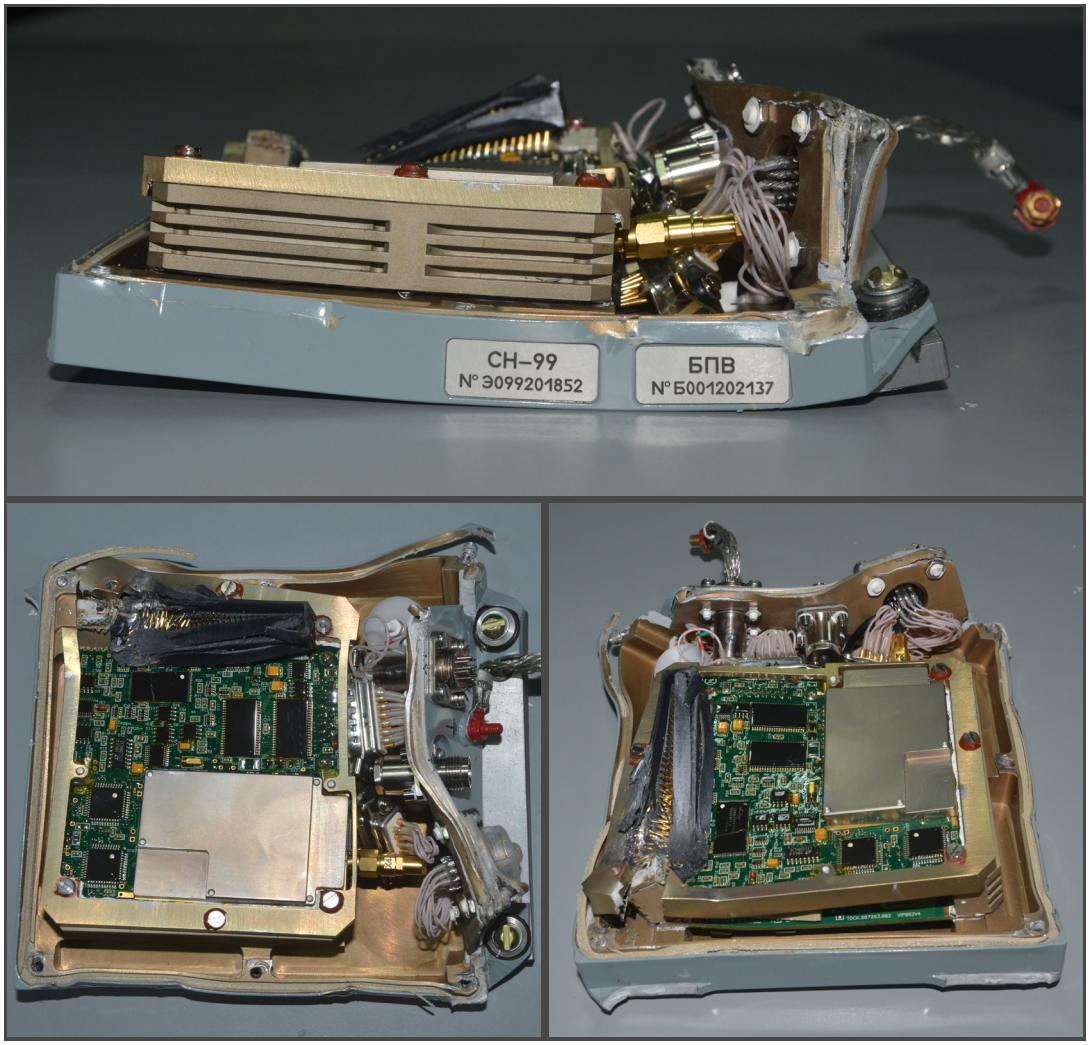
138 Oleg Falichev, '"Metallist": pricel'noe razvitie' ['"Metallist": Targeted Development'], *Voyenno-promyshlennyj kur'jer* [*Military-Industrial Courier*], 6 November 2018, <https://vpk-news.ru/articles/46107>, accessed 21 July 2022.

139 *Serpukhovskie Vesti*, 'Serpuhovskomu zavodu Metallist ispolnyaetsya 75 let' ['The Serpukhov "Metallist" Plant Turns 75'], 13 August 2018, <http://inserpuhov.ru/novosti/proizvodstvo/serpuhovskomu-zavodu-metallist-ispolnyaetsya-75-let>, accessed 20 July 2022.

140 Serpukhov Plant Metallist, 'Glavnaya' ['Main'], archived version of the webpage captured 26 December 2021, <https://web.archive.org/web/20211226064918/http://www.szmetallist.ru/>, accessed 21 July 2022.

141 US Department of the Treasury, 'U.S. Treasury Sanctions Russia's Defense-Industrial Base, the Russian Duma and Its Members, and Sberbank CEO', press release, 24 March 2022, <https://home.treasury.gov/news/press-releases/jy0677>, accessed 21 July 2022.

Figure 18: Images of the SN-99 (CH-99) GLONASS and GPS Guidance System



Source: RUSI.

This unit is produced by the Design Bureau of Navigational Systems (AO KB NAVIS),[142] a manufacturer of GLONASS, GPS and GALILEO navigational systems used by the Russian military.[143] Russian-language corporate records[144] and periodicals also claim that KB Korund-M, the aforementioned SRISA RAS design bureau, established KB NAVIS.[145] Like KB Korund-M,

142 Konstruktorskoye B'uro Navigacionnyh Sistem Navis [Design Bureau of Navigational Systems Navis], 'SN-99 Navigacionnaya apparatura dlya vysokodinamichnyh ob'ektov GLONASS/GPS/SBAS' ['SN-99 – Navigational Equipment for GLONASS/GPS/SBAS High Dynamic Objects'], <https://navis.ru/assets/files/SN-99---korrekt_NEW.pdf>, accessed 21 July 2022.

143 'Nekommercheskaya organizaciya Associaciya razrabotchikov, proizvoditelei i potrebitelei oborudovaniya i prilozhenij na osnove global'nyh navigacionnyh sputnikovyh sistem GLONASS/GNSS-Forum' ['Non-Commercial Organisation the Association of Developers, Producers and Consumers of Equipment and Applications on the Basis of the Global Satellite Navigation Systems "GLONASS/GNSS-Forum"'], 'Analiticheskij otchet po itogam izsledovaniya sostoianiya i perspektiv razvitiya rynka navigacionnyh, svyazanyh i navigacionno-sviazannyh modulej, a takzhe ocenki vliyanniya na razvitie rossijskogo i mezhdunarodnogo rynka "Avtonet"' ['Analytical Report on the Findings of the Study of the State and Development Perspectives of the Market for Navigation, Network and Navigational-Network Modules, As Well As the Impact Assessment of the Development of the Russian and International "Autonet" Market'], 2019, <https://tinyurl.com/yckfrxwx>, p. 189, accessed 15 July 2022.

144 See Russian Federal Tax Register, document dated 9 July 2020 taken from Sayari Labs, <https://sayari.com/>, accessed 10 July 2022.

145 A A Shanin et al., 'Apparatura Sputnikovyh Navigacionnyh Sistem GLONASS i GPS Konstruktorskogo B'uro Navigacionnyh

KB NAVIS has not been sanctioned by Western governments despite its provision of critical technology to the country's missile programme.

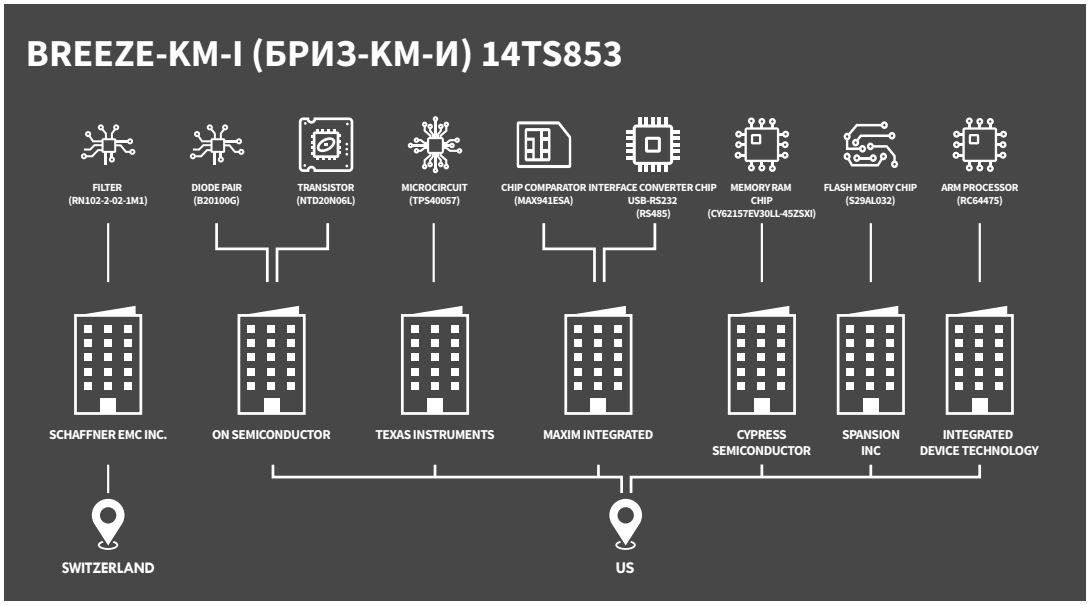
Notably, the SN-99 (CH-99) systems contain several Western-made components such as a 32-megabit flash memory chip made by Spansion and a 12-bit A/D converter manufactured by Linear Technology Corporation. While an A/D converter in the 12-bit range is no longer considered exceptional by modern standards, it is still a critical component for tactical cruise and ballistic missiles and was likely considered top-of-the-line when this SN-99 system was assembled.

MULTIPLE PRODUCTS

KB NAVIS, however, appears to manufacture several pieces of equipment for the Russian military. Another of these is a handheld navigational and positional system used by the country's special operations forces (SOF) named Breeze-KM-I.[146] These types of devices are commonly employed by SOF and forward reconnaissance personnel to accurately pinpoint their own position and estimate coordinates for precision artillery and air strikes on the enemy's location.

When disassembled, the Breeze-KM-I contains a number of Western-manufactured microelectronics including a high-performance 64-bit microprocessor, SRAM chips, transceivers and amplifiers.

Figure 19: Components in the Breeze-KM-I



Source: RUSI.

One of these components is a high-performance CMOS static RAM chip (CY62157EV30LL-45ZSXI) originally produced by US-based Cypress Semiconductor. The component is a high-speed, ultra-low-power memory chip[147] that is classified as a dual-use good for export purposes.[148]

Sistem' ['Equipment for Satellite Navigation Systems GLONASS and GPS of the Design Bureau of Navigation Systems'], Navigation and Hydrography, State Research Navigation-Hydrography Institute, Russian Federation Ministry of Defence, December 2001, p. 173.

146 NAVIS, 'Breeze-KM-I Individual'naya navigacionnaya apparatura GLONASS/GPS/SBAS' ['Breeze-KM-I Individual Navigational GLONASS/GPS/SBAS Equipment'], <https://navis.ru>, accessed 23 June 2022.

147 Infineon Technologies, 'CY62157EV30 MoBL 8-Mbit (512K × 16) Static RAM', data sheet, 28 February 2020, <https://www.infineon.com/dgdl/Infineon-CY62157EV30_MoBL_8-Mbit_(512_K_16)_Static_RAM-DataSheet-v20_00-EN.pdf?fileId=8ac78c8c7d0d8da4017d0ebe669131ef>, accessed 21 July 2022.

148 ECCN 3A991.b.2.a – static random-access memory (SRAM) with a storage capacity exceeding 1 Mbit per package. See Bureau of Industry and Security of the US Department of Commerce, 'Commerce Control List: CATEGORY 3 -

Russian trade records and import declarations show that, between 2017 and 2021, KB NAVIS imported large volumes of electronics, integrated circuits and other electronic components manufactured by US companies such as Analog Devices, Texas Instruments and Linear Technology.[149] However, while most of its shipments were of US-manufactured goods, the vast majority of these were shipped through Switzerland, Israel, China and Malaysia.[150]

Notably, over 90% of these were moved to KB NAVIS by Switzerland-based NVS Technologies AG, both of which are part of the NAVIS group of companies.[151]

The CEO of NVS Technologies – a Russian national named Vasiliy Engelsberg[152] – is also the co-founder of KB NAVIS[153] and of the wider NAVIS group of companies.[154] Notably, fellow KB NAVIS co-founder Valery Babakov[155] has also served as the chief designer of consumer navigational equipment at Almaz-Antey.[156] In a 2008 piece on the commercialisation of GLONASS co-authored with Engelsberg, Babakov noted that the NAVIS Group was the main supplier of GLONASS receivers in Russia. He also explained that NVS Technologies was established 'as part of the process of integration of our technologies into the worldwide GNSS market'.[157]

While KB Navis appears to produce items for several civilian applications, a 2019 Russian-language industry report claimed that over 70% of the institute's contracts were with the Russian Ministry of Defence.[158] At the time, these apparently amounted to over 3.5 billion roubles, or $55 million at the time. Hence, it appears possible that many of the Western-sourced components imported by KB NAVIS found their way into the kinds of Russian weapons systems assessed for this report.

ELECTRONICS'.

149 Trade data supplied by third-party commercial provider.

150 *Ibid.*

151 'Nekommercheskaya organizaciya Associaciya razrabotchikov, proizvoditelei i potrebitelei oborudovaniya i prilozhenij na osnove global'nyh navigacionnyh sputnikovyh sistem GLONASS/GNSS-Forum' ['Non-Commercial Organisation of the Association of Developers, Producers and Consumers of Equipment and Applications on the Basis of the Global Satellite Navigation Systems "GLONASS/GNSS-Forum"'], 'Analiticheskij otchet po itogam izsledovaniya sostoianiya i perspektiv razvitiya rynka navigacionnyh, svyazanyh i navigacionno-sviazannyh modulej, a takzhe ocenki vliyanniya na razvitie rossijskogo I mezhdunarodnogo rynka "Avtonet"' ['Analytical Report on the Findings of the Study of the State and Development Perspectives of the Market for Navigation, Network and Navigational-Network Modules, As Well As the Impact Assessment of the Development of the Russian and International "Autonet" Market'], pp. 187, 160.

152 LinkedIn, 'Vasily Engelsberg', <https://ch.linkedin.com/in/vasily-engelsberg-3b637b16>, accessed 21 July 2022.

153 Polina Jeremenko, 'Soshel s orbity' ['Left Orbit'], *Moskovskiye Novosti* [*Moscow News*], 7 April 2011, <https://www.mn.ru/politics/68113>, accessed 3 July 2022.

154 *PravoRU*, 'Sobstvenniku postavschika Minoborony otkazali v iske na sovladel'ca' ['Owner of a Ministry of Defence Supplier Has Been Denied a Claim Against the Co-Owner'], 10 November 2017, <https://pravo.ru/news/view/145748/>, accessed 3 July 2022.

155 *Ibid.*

156 *Novosti navigacii*, '5th International Satellite Navigation Forum', (No. 2, 2011), p. 51, <https://internavigation.ru/wp-content/uploads/2019/07/nn2011_02.pdf#page=51>, accessed 12 July 2022.

157 Vasiliy Engelsberg, Ivan Petrovski and Valery Babakov, 'Expert Advice: GLONASS Business Prospects', *GPS World*, 1 March 2008, <https://www.gpsworld.com/gnss-systemglonassexpert-advice-glonass-business-prospects-4215/>, accessed 21 July 2022.

158 According to this document, KB NAVIS had concluded 106 contracts with the Russian federal government, valued at 5.1 billion roubles. Twenty of those contracts – amounting to 3.6 billion roubles or 72.6% of the company's business – were with the Russian Ministry of Defence. See 'Nekommercheskaya organizaciya Associaciya razrabotchikov, proizvoditelei i potrebitelei oborudovaniya i prilozhenij na osnove global'nyh navigacionnyh sputnikovyh sistem GLONASS/GNSS-Forum' ['Non-Commercial Organisation of the Association of Developers, Producers and Consumers of Equipment and Applications on the Basis of the Global Satellite Navigation Systems "GLONASS/GNSS-Forum"'], 'Analiticheskij otchet po itogam izsledovaniya sostoianiya i perspektiv razvitiya rynka navigacionnyh, svyazanyh i navigacionno-sviazannyh modulej, a takzhe ocenki vliyanniya na razvitie rossijskogo I mezhdunarodnogo rynka "Avtonet"' ['Analytical Report on the Findings of the Study of the State and Development Perspectives of the Market for Navigation, Network and Navigational-Network Modules, As Well As the Impact Assessment of the Development of the Russian and International "Autonet" Market'], p. 189.

THE KH-101 CRUISE MISSILE

The Kh-101 ALCM has been expended in significant numbers in Ukraine. The missile has been used to attack a variety of targets, including railway infrastructure[159] and urban centres.[160] It is noteworthy that the design has been mooted since the 1980s and its entry into service slowed by a lack of state funding, which pushed its development into the 2000s.[161]

Introduced into service in 2012, the missile was developed as a long-range, standoff cruise missile with a range of up to 2,800 km to carry either conventional warheads – such as high explosive, fragmentation, submunitions – or even a 250-kt nuclear warhead. Being launched from an aircraft, the missile does not require the use of a booster to gain initial velocity and reportedly can cruise at an altitude of 6,000 metres at Mach 0.58.[162] In addition, the missile can fly to a target at an altitude of 30–60 metres at a maximum speed of Mach 0.78.[163]

The missile uses a range of systems and sensors for midcourse navigation, including inertial, GLONASS and GPS satellite data.[164] These latter signals are received and processed by the same SN-99 (CH-99) unit fitted on to the 9M727 cruise missile. The electro-optical correction system uses a stored terrain map to carry out terrain comparison updates.[165] In its terminal phase, the Kh-101 makes use of a TV imaging infrared seeker.[166]

159 Ministry of Defence (@DefenceHQ), '(2/6) In the early hours of 5 June, Russian Kh-101 air-launched cruise missiles struck rail infrastructure in Kyiv, likely in an attempt disrupt the supply of Western military equipment to frontline Ukrainian units', Twitter, 6 June 2022, <https://twitter.com/DefenceHQ/status/1533682058463268864>, accessed 21 July 2022.

160 *NBC News*, '2 Reported Killed as Russian Missiles Strike Kyiv for First Time in Weeks'.

161 Robin Hewson, 'Details Emerge of Russia's Latest Cruise Missiles', *Jane's Defence Weekly*, October 2007, <https://web.archive.org/web/20080225163154/http://www.janes.com/news/defence/systems/jdw/jdw071022_1_n.shtml>, accessed 21 July 2022.

162 CSIS Missile Defense Project, 'Kh-101 / Kh-102', 31 July 2021, <https://missilethreat.csis.org/missile/kh-101-kh-102/>, accessed 21 July 2022.

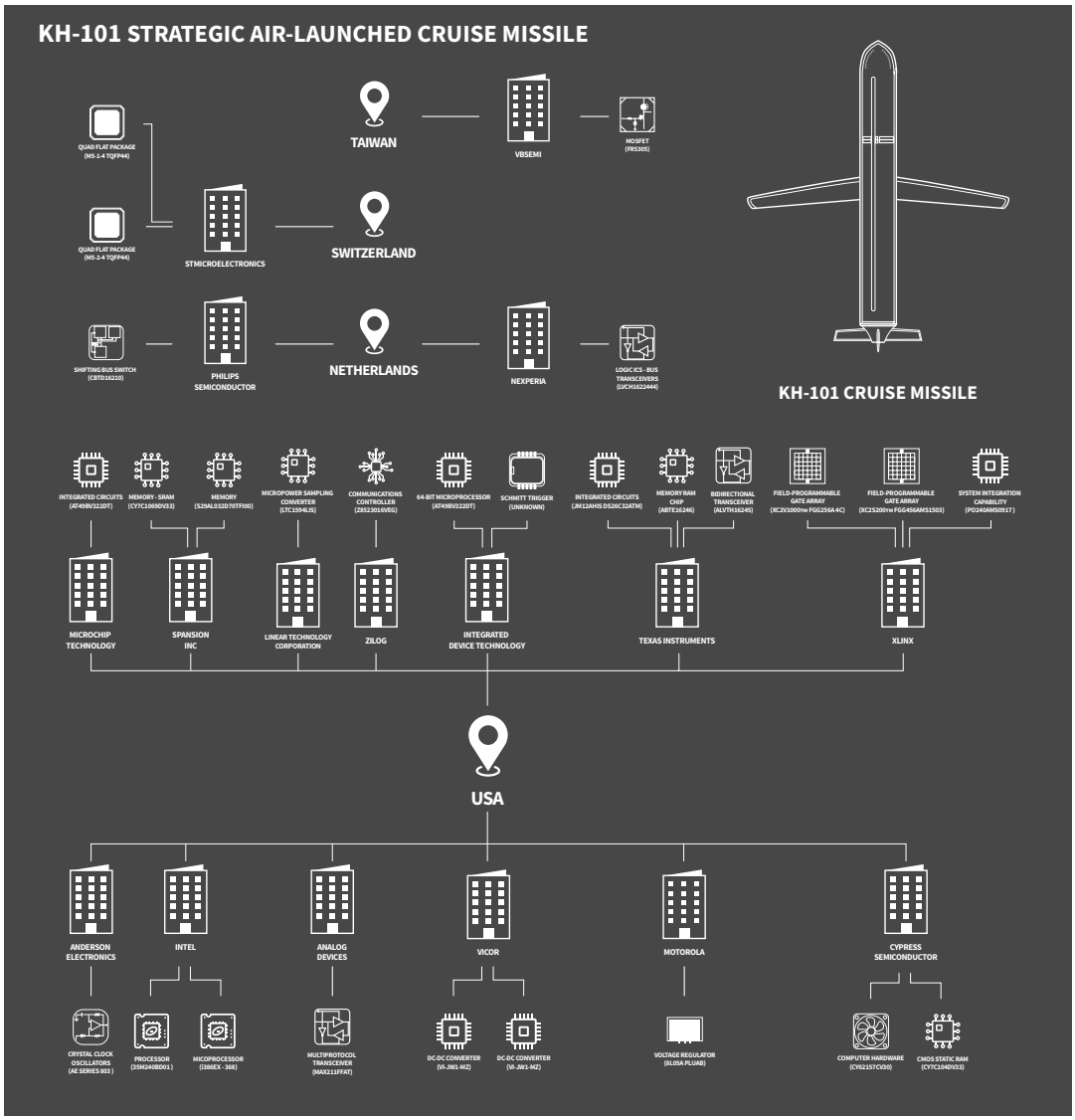
163 *Ibid.*

164 *Ibid.*

165 *Ibid.*

166 *Ibid.*

Figure 20: Western Components in the Kh-101



Source: RUSI.

An intact Kh-101 that was recovered reveals that the missile has at least six sub-systems – such as satellite navigation systems and a receiver unit, a processor module and a computing unit. All these systems contain extensive numbers of Western-produced microelectronics. For instance, the BT33-202 processor module contains at least a dozen microelectronic components – including CMOS SRAM modules, FPGAs, RS-232 and bus transceivers – produced by a range of companies based in the US and the Netherlands. Notably, it also includes Texas Instruments-manufactured CMOS quad differential line receivers, capable of balanced and unbalanced digital data transmission while maintaining low-power characteristics. Texas Instruments states that this component is manufactured to US Mil-Std-883C specification, yet the product is classified as EAR99.[167]

167 Texas Instruments, 'DS26C32ATM/NOPB - CMOS Quad Differential Line Receivers', <https://www.ti.com/product/DS26C32AT/part-details/DS26C32ATM/NOPB>, accessed 21 July 2022.

Open Circuit: Component Flows Into Russia

Despite years of increasingly stringent sanctions and export controls designed to curtail the Russian military's access to critical components, Russian shipment-level trade records and import declarations filed between 2017 and 2021 provide some insight into how these components have moved into the country.[168]

Using these records and a tool named the Altana Atlas, the research team screened billions of harmonised trade records for Russian imports of semiconductors and semiconductor-related inputs that could have found their way into Russian weapons platforms deployed to Ukraine.[169]

This dataset was then checked for entities that could have acted as conduits for components entering Russia's military–industrial complex, a process which identified dozens of military importers and other companies with close links to the country's defence industry.

A GLOBAL SUPPLY CHAIN: RUSSIAN SEMICONDUCTOR IMPORTS

Russia is a large importer of semiconductors and microelectronics used in commercial, industrial and military systems. In order to better understand these flows, the research team searched for all instances from 2017–22 where Russian companies imported goods under a range of HS codes corresponding to microelectronics and microelectronic-related goods.[170]

168 Trade data provided by Altana Trade Atlas (https://altana.ai/atlas/) and a third-party commercial data provider.

169 Altana Trade Atlas, <https://altana.ai/atlas/>.

170 HS Codes, or Harmonised System Codes, are standardised codes used to denote categories of goods in international trade. HS Codes represent goods categories, not specific products. Up to the sixth digit, they are standardised internationally – after which they are modified by individual countries for their own record-keeping purposes. For our sample, we included HS codes '854239' (electronic integrated circuits; parts thereof), '854129' (unmounted chips, dice and wafers), '854110' (diodes, other than photosensitive or light-emitting diodes), '854231' (processors and controllers, whether or not combined with memories, converters, logic circuits, amplifiers, clock and timing circuits, or other circuits) and '381800' (chemical elements doped for use in electronics, in the form of discs, wafers or similar forms).

03

This query generated nearly one million semiconductor-related imports into Russia during this time period.[171] In total, 5,597 distinct companies appeared as importers. Among these companies, there was significant variety – from large, multi-input wholesale goods processors to specialised electronics manufacturers, and from local affiliates of Western multinationals simply conducting intra-firm trade to companies specialised in dealing with Russia's military–industrial complex. The Altana Atlas returned transactions in everything from semiconductors destined for simple desktop computers to highly specialised components of the precise types found on the battlefields of Ukraine.[172]

Unsurprisingly, the top importers by number of overall transactions tended to be wholesale importers sourcing a wide variety of electronic components from around the world.

Figure 21: Top Russian Importers

IMPORTER	NUMBER OF SEMICONDUCTOR-RELATED TRANSACTIONS	
OOO BELIV	100,313	GERMANY – 8,544 MALAYSIA – 7,403 CHINA – 7,213 PHILIPPINES – 4,037 US – 3,880
KOMPONENT	34,252	US – 12,884 MALAYSIA – 3,088 CHINA – 2,732 HONG KONG SAR – 1,943 THAILAND – 1,850
BALTELEKTRON	32,377	US – 9,025 UK – 5,357 HONG KONG SAR – 3,931 CHINA – 2,635 MALAYSIA – 2,449
WEST-OST	29,115	GERMANY – 6,018 HONG KONG SAR – 4,830 CHINA – 4,763 MALAYSIA – 2,085 TAIWAN – 1,389
SPETSVOLTAZH	28,843	CHINA – 6,576 FINLAND – 5,637 US – 3,449 MALAYSIA – 2,654 TAIWAN – 2,241

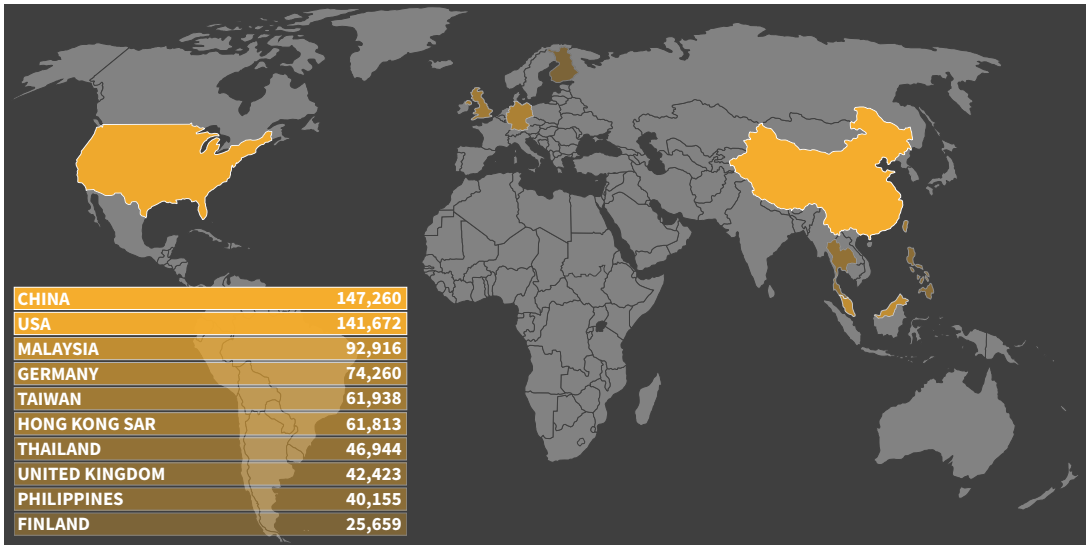
Sources: Altana Atlas; RUSI.

171 Altana Trade Atlas.

172 *Ibid.*

Electronic goods were sourced from a wide variety of countries and jurisdictions. While prominent semiconductor export jurisdictions such as China, the US, Germany, Taiwan, Hong Kong and the UK were among the top 10 suppliers, a significant volume of transactions came from countries, such as Malaysia and Thailand, where a number of large multinational semiconductor manufacturers have manufacturing plants and facilities where assembled integrated circuits are tested before being shipped to customers and distributors.[173]

Figure 22: Top 10 Semiconductor and Microelectronic Exporters to Russia



Sources: Altana Atlas; RUSI.

However, closer investigation indicates that some of these transactions, particularly those from countries without robust semiconductor and electronics industries, are often unlikely to represent deliveries from manufacturers. There are generally two explanations for these types of transactions: return shipments; and transshipment.

Return shipments are often identifiable by examining the nature of the counterparties involved in the transaction. For instance, the Altana Atlas showcases several transactions in semiconductor-related goods from Algeria to Russia during the period studied. Detailed transaction data shows that all these shipments, however, are for non-light-emitting diodes and integrated circuits from the Algerian Ministry of Defence to 'PAO Kompaniya Sukhoi' and 'PAO Kompaniya Irkut' – two well-known Russian defence contractors.[174]

As the Algerian military operates defence systems manufactured by these two corporations,[175] it is highly likely that, rather than transactions of finished microelectronics manufactured by the Algerian Ministry of Defence, these transactions represent return shipments of faulty, surplus or otherwise unneeded components. Similar dynamics were observed for other companies

173 *Ibid.*

174 Sukhoi is a well-known military brand and was recently merged into the United Aircraft Corporation which was sanctioned by the UK on 24 February 2022. See Foreign, Commonwealth and Development Office, 'Foreign Secretary Imposes UK's Most Punishing Sanctions to Inflict Maximum and Lasting Pain on Russia', press release, 24 February 2022, <https://www.gov.uk/government/news/foreign-secretary-imposes-uks-most-punishing-sanctions-to-inflict-maximum-and-lasting-pain-on-russia>, accessed 21 July 2022. The many subsidiaries and affiliated companies of Kompaniya Irkut are listed in US Treasury designations. See US Department of the Treasury, 'Russia-Related Designations and Designations Updates; Issuance of Russia-Related General Licenses and Related Frequently Asked Questions', press release, 28 June 2022, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220628>, accessed 21 July 2022.

175 *Times Aerospace*, 'Algeria to Get 14 SU-57 Fighters from Russia', <https://www.timesaerospace.aero/news/defence/algeria-to-get-14-su-57-fighters-from-russia>, accessed 10 July 2022.

based in countries lacking robust electronic manufacturing industries, but which still had sent shipments to Russia.

Transshipment through third countries is a more important, but difficult, case. Microelectronic third-party distributors and wholesalers often operate from intermediary jurisdictions such as Hong Kong, meaning that components bound for Russia are sometimes legitimately supplied through trading entities domiciled outside of Russia itself. However, third countries are also often exploited by procurement agents looking to move sensitive and controlled goods by obscuring the real exporter or end user.[176] Russia's clandestine procurement networks and those acting on their behalf often base their operations in jurisdictions with large microelectronic trading industries and laxer controls. As recently as 28 June 2022, for example, OFAC sanctioned three individuals and a Hong Kong company named EMC Sud Limited it alleged were part of a covert procurement network linked to the FSB. One of these individuals, former FSB agent Alexander Kokorev, was allegedly covertly procuring electronics from the US, Japan and Europe to benefit Russia's defence industrial base.[177]

Detecting transshipment patterns is challenging, in large part because it requires multi-tier visibility of goods moving from an origin country, through a transit country, and finally to a destination country. Though hard to see, tools such as the Altana Atlas can shed some visibility on multi-stage value chains to see potential cases of transshipment.

For instance, SP Semiconductors Private Limited, a semiconductor manufacturer based in New Delhi, India, sent Infineon-branded integrated circuits to King-Pai Technology (HK) Co Ltd (金派科技(香港)有限公司) on 9 June 2021. Later in the same month, King-Pai sent multiple transactions with similar goods descriptions to several Russian companies active in the military-industrial space, including Trade-Component[178] and Radiant Electronic Components, both first sanctioned by the US Treasury in 2021,[179] and Radioavtomatika, first sanctioned in 2022.[180] All companies have documented histories of providing microelectronics to the Russian military.[181] King-Pai Technology was added to BIS's Entity List in late June 2022 for providing support to Russia's military and defence industry.[182] Hong Kong corporate records for the company name its sole director and shareholder as a Chinese national named Yao Jinbiao (姚金标). An archived version of the company's website states that the company operates overseas offices in Moscow, Russia, and Ho Chi Minh City, Vietnam.[183] Yao Jinbiao also appears to operate another Hong Kong company using the 'Kingpai' name, one directly – Kingpai Technology International Co Ltd (金派科技國際有限公司) – while the similarly named Kingpai Technology Group Co Ltd (金派科技集團有限公司) is operated by an individual with the same surname as Yao.[184]

176 Daniel Salisbury, 'Exploring the Use of "Third Countries" in Proliferation Networks: The Case of Malaysia', *European Journal of International Security* (Vol. 4, No. 1, February 2019).

177 US Department of the Treasury, 'U.S. Treasury Sanctions Nearly 100 Targets in Putin's War Machine, Prohibits Russian Gold Imports', press release, 28 June 2022, <https://home.treasury.gov/news/press-releases/jy0838>, accessed 22 July 2022.

178 Altana Trade Atlas, <https://altana.ai/atlas/>.

179 Bureau of Industry and Security of the US Department of Commerce, 'Addition of Certain Entities to the Entity List; Revision of Existing Entry on the Entity List; Removal of Entity From the Unverified List; and Addition of Entity to the Military End-User (MEU) List', 12 July 2021, <https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list>, accessed 22 July 2022.

180 US Department of the Treasury, ''Russia-Related Designations; Issuance of Russia-Related General License', press release, 3 March 2022, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220303>, accessed 22 July 2022.

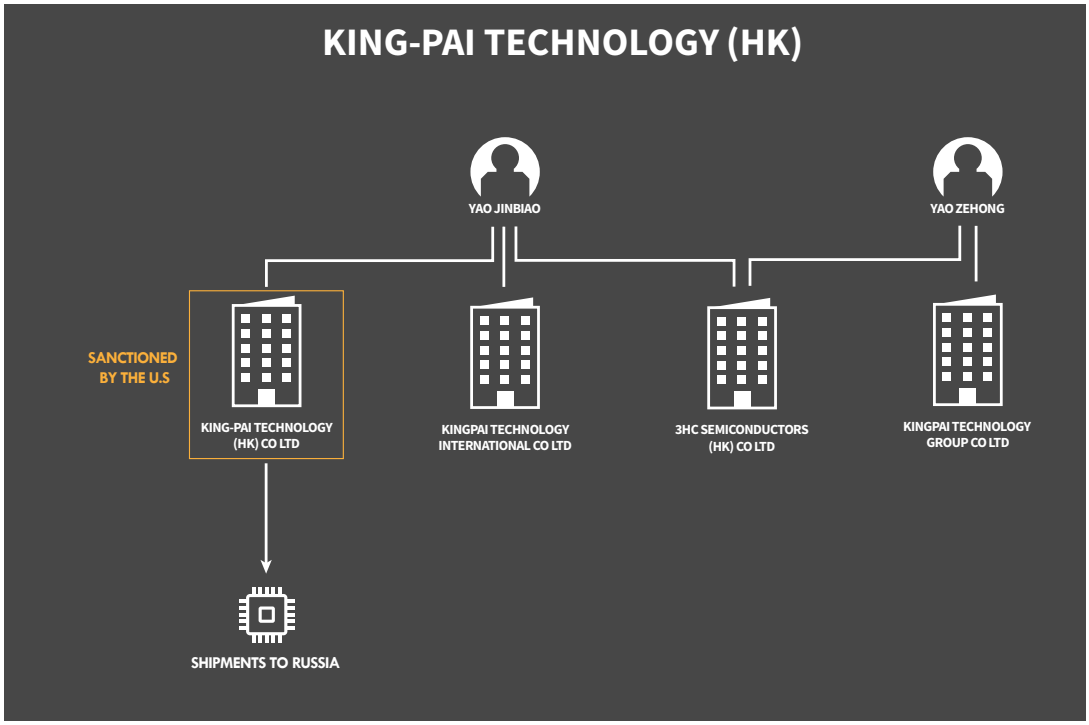
181 Alexandra Alper, 'U.S. Accuses Five Firms in China of Supporting Russia's Military', *Reuters*, 29 June 2022.

182 Bureau of Industry and Security of the U.S. Department of Commerce, 'Supplement No. 4 to Part 744 - ENTITY LIST', 28 June 2022, <https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file>, accessed 22 July 2022.

183 King-Pai Technology (HK), 'Contact Us', <https://www.king-pai.com/contact.asp>, accessed 22 July 2022.

184 Hong Kong Companies Registry, available at <www.icris.cr.gov.hk>.

Figure 23: Companies of the King-Pai Network



Sources: US Bureau of Industry and Security; Hong Kong Companies Registry; Qichacha; Altana Trade Atlas; RUSI.

A director search for Yao Jinbiao reveals that he operates a network of companies involved in the sale of microelectronics, centered on a Shenzhen-based company named 3HC Semiconductors Co Ltd (深圳市三合成科技有限公司).[185] According to the Altana Atlas, 3HC's export history largely mirrors that of King-Pai, with trade records showing several transactions in microelectronics and related goods to sanctioned entities such as Radioavtomatika and Trade-Component.[186]

ZEROING IN ON THE BATTLEFIELD

It is also possible to look more closely at shipments of the precise goods and components that have been found on the battlefield within Russian weapons systems.

The research team used the Altana Atlas to search for all transactions into Russia matching a sample of 204 specific semiconductor serial numbers taken directly from disassembled Russian weapons systems. In total, this resulted in 2,744 matching shipments to 286 unique recipients in Russia.[187]

Many semiconductors have multiple applications, meaning that even a shipment featuring the precise type of semiconductor found in a Russian weapons system may have been destined for civilian use. Several of these shipments likely represent benign uses of semiconductors of the type which, it so happens, were also used in Russian weapons. Indeed, the Altana Atlas shows several instances of intra-firm trading by Western companies sending semiconductors to their Russian subsidiaries. In these cases, the likelihood of intentional diversion to the military is low.[188]

Other importers, however, pose a higher risk. For instance, ZAO Radiotekhkomplekt (RTKT), a company with a long history of supplying to the military, appears in the database as a recipient of the precise types of semiconductors found in Russian weapons, including those manufactured

185 Qichacha [企查查], '3hc Semiconductors Co.,limited' ['深圳市三合成科技有限公司'], <https://www.qcc.com/firm/535b9127d06edbbba894ca64b6ae41b6.html>, accessed 22 July 2022.

186 Altana Trade Atlas, <https://altana.ai/atlas/>.

187 *Ibid.*

188 *Ibid.*

by firms such as TE Connectivity, Microchip Technology, Analog Devices' subsidiary Linear Technology and many others.[189] Founded in 1997, the company supplies a range of Russian enterprises, research institutes and design bureaus with electronic components.[190] Meanwhile, an archived version of the RTKT webpage notes that the company has been certified since 2000 for the provision of certain kinds of electronic components to the military,[191] and claimed that the US-designated[192] Russian helicopter manufacturer Kumertau Aviation Production Enterprise (AKA AO KUMAPP) was one of its customers up to at least 2020.[193] The page also identifies a range of Western technology companies for whom RTKT acts as a supplier, including Texas Instruments, Cypress Semiconductor, Golledge and others,[194] whose parts are often found in Russian weapons systems.

Meanwhile, several other companies which also appear as receivers of the precise components recovered on the battlefield in Ukraine have already been targeted by a range of Western sanctions, including Rosoboronexport and Uralvagonzavod.[195]

TRACING SANCTIONED ENTITIES

In addition to focusing on proven instances of semiconductors ending up on the battlefield, we can trace supply links to entities that have been publicly sanctioned by the US and its allies for involvement in tech transfers on behalf of the Russian military. Many of these sanctions have been applied recently, meaning that historical transactions shown in the Altana Atlas may not have been illegal at the time that they took place. However, even if a transaction was legitimate at the time it was conducted, the trading activities of these companies can provide some insights into the nature of their procurement networks.

Returning to the original sample of 5,597 companies importing microelectronics into Russia, the research team found records for over 40 companies that either appear directly on US and international sanctions or export control lists, or that are 50% owned by companies that do (and which are therefore sanctioned by operation of law).[196]

Within the sample, denied parties that received semiconductor-related imports included companies which were sanctioned precisely for their procurement of electronics for the Russian military, including Npo Elektronnye Sistemy, Radioavtomatika, Publichnoe Aktsionernoe Obshchestvo Oplot and many others. According to the Altana Atlas, transactions to parties denied either outright or by law have continued as recently as September 2021 – which may indicate potential sanctions violations or due diligence failures by counterparties.[197]

By examining a given company's import history in more detail, one can begin to understand how a given entity is likely to have acted as a conduit for these goods to enter into Russian military systems. For instance, the Altana Atlas reveals more than 2,500 individual trade transactions between PAO Mikron and 148 distinct senders from 33 countries and jurisdictions, including the US, the UK, Germany, the Netherlands and Taiwan.

189 *Ibid.*

190 Radiotekhkomplekt, 'Homepage', <http://web.archive.org/web/20161219070553/https://www.rtkt.ru/eng/>, accessed 22 July 2022.

191 US Department of the Treasury, 'U.S. Treasury Sanctions Russia's Defense-Industrial Base, the Russian Duma and Its Members, and Sberbank CEO', press release, 24 March 2022, <https://home.treasury.gov/news/press-releases/jy0677>, accessed 22 July 2022.

192 Radiotekhkomplekt, 'About'.

193 *Ibid.*

194 Radiotekhkomplekt, 'Manufacturers', <https://www.rtkt.ru/eng/manufacturers/>, accessed 22 July 2022.

195 US Department of the Treasury, 'Ukraine-/Russia-Related Designations and Identification Update; Syria Designations; Kingpin Act Designations; Issuance of Ukraine-/Russia-Related General Licenses 12 and 13; Publication of New FAQs and Updated FAQ', press release, 6 April 2018, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20180406>, accessed 22 July 2022.

196 US Department of the Treasury, 'Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists', 28 June 2022, <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>, accessed 22 July 2022.

197 Altana Trade Atlas, <https://altana.ai/atlas/>.

As noted earlier, Mikron had been one of the key producers of integrated circuits in the Soviet Union and it still markets itself as the leading producer and exporter of microelectronics in Russia.[198] In 2016, the company was reportedly contracted to produce electronic components for Russian space launch vehicles.[199] Mikron has been sanctioned by the US Treasury in relation to the Russian invasion of Ukraine.[200]

Nearly all the 2,500 transactions referenced were for semiconductor-related manufacturing equipment or components. This included a transaction between Mikron and an Irish firm for parts of lasers included in the ASML-produced Twinscan XT:1060k lithography laser system, designed for the production of integrated circuits.[201] Another transaction originating from a company in the UK referenced 'Silicon, doped, cleaned, single-crystal, in the form of plates, polished, for use in microelectronics'.[202] While these transactions may or may not have been in violation of sanctions at the time they were conducted, they do raise the possibility of leakage to the military–industrial complex in Russia – and ultimately to the battlefield in Ukraine.

HONG KONG CHIP SHOPS

In June 2022, BIS added several non-Russian companies to its Entity List for supporting Russia's military and defence industrial base,[203] effectively denying them the ability to import and re-import even EAR99-classified goods from the US.

Among these was a Hong Kong-based company named Sinno Electronics Co Ltd (信諾電子科技有限公司; AKA Xinnuo Electronic Technology), which operates from several addresses in Hong Kong[204] and Shenzhen, in mainland China.[205] The company is owned and operated by three Chinese nationals named Peng Minbo (彭敏波; AKA Betty Peng), Lin Qing (林青; AKA Becky Lin), and Hong Junxu (洪俊旭; AKA Billy Hong; AKA 阿旭).[206]

Sinno has an extensive online presence with shop fronts[207] and an English-language-only website,[208] which advertises products made by Analog Devices, Texas Instruments and many other manufacturers.[209] The company appears to have attended ExpoElectronica in Moscow since at least 2013,[210] and most recently in 2021.[211] During the coronavirus pandemic, the company even

198 Mezhdunarodnyj Ob'yedinnenyj Biographicheskij Centr [International United Biographical Centre], 'Nacional'noe dostoyaniye, OAO "NIIME i Mikron"' ['National Treasure, OJSC "NIIME and Mikron"'], <http://www.biograph.ru/index.php/nationdestiny/5269-mikron>, accessed 25 July 2022; Mikron, 'Mikron History', <https://en.mikron.ru/company/history/>, accessed 30 June 2022; Mikron, <https://en.mikron.ru/>, accessed 30 June 2022.

199 *Zelenograd Infoportal*, '"Mikron" zaimetsya proizvodstvom elementov noveyshey sistemy upravleniya dlya raket-nositelej' ['"Mikron" Will Undertake the Production of Elements for the Newest Space Launch Vehicle Control System'], 7 December 2016, <https://www.netall.ru/society/news/983044.html>, accessed 25 July 2022.

200 US Department of the Treasury, 'Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War', 31 March 2022, <https://home.treasury.gov/news/press-releases/jy0692>, accessed 27 July 2022.

201 Altana Trade Atlas, <https://altana.ai/atlas/>.

202 *Ibid.*

203 Bureau of Industry and Security of the US Department of Commerce, 'Addition of Entities, Revision and Correction of Entries, and Removal of Entities from the Entity List', 30 June 2022, <https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3043-public-display-version-of-entity-list-rule-on-public-display-and-effetive-6-28-22-scheduled/file>, accessed 22 July 2022.

204 Sinno Electronics, 'Contact Us', <http://www.sinnoelec.com/contact.aspx>, accessed 22 July 2022.

205 Bureau of Industry and Security of the US Department of Commerce, 'Federal Register / Vol. 87, No. 125', 30 June 2022, <https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2022/3053-87-fr-38920-entity-list-rule-effective-6-28-22-published-6-30-22/file>, accessed 22 July 2022.

206 Hong Kong Companies Registry, <www.icris.cr.gov.hk>.

207 Hong Kong Inventory, 'Sinno Electronics Co., Limited', <http://hksinno.hkinventory.com/Shop/Page_CompanyProfile.asp>, accessed 22 July 2022.

208 Sinno Electronics, 'Homepage', <http://www.sinnoelec.com/index.aspx>, accessed 22 July 2022.

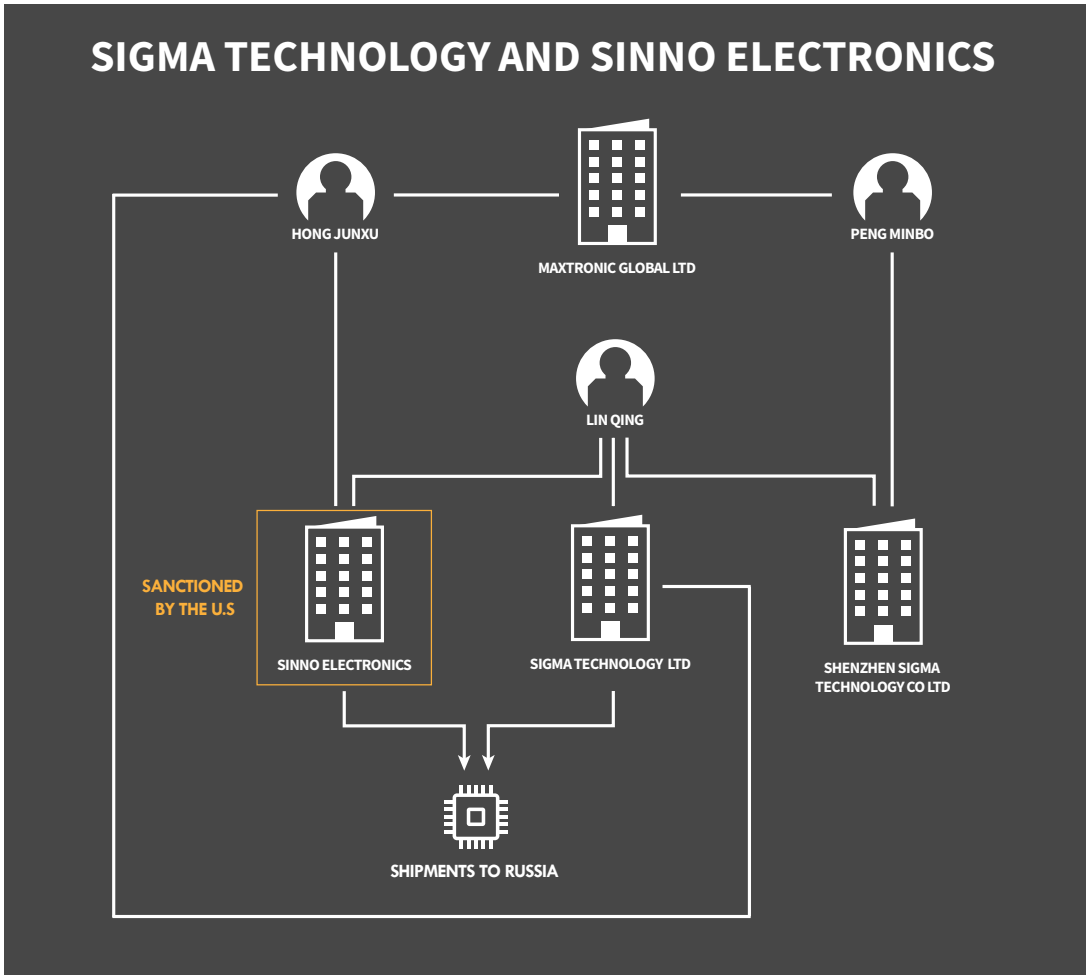
209 Sinno Electronics, 'Product', <http://www.sinnoelec.com/product.aspx>, accessed 22 July 2022.

210 Hong Kong Inventory, 'Expo Electronica Apr 10-12, 2013 Moscow', <https://www.hkinventory.com/public/UpcomingEventDetail.asp?id=173>, accessed 22 July 2022.

211 ExpoElectronica, 'ExpoElectronica and ElectronTechExpo Will Bring Together Leading Manufacturers, Suppliers and

sponsored a 2020 webinar on 'Russian-Chinese cooperation in the field of high technologies'.[212]

Figure 24: Sinno and Sigma Network



Sources: US Bureau of Industry and Security; Hong Kong Companies Registry; Qichacha; Altana Trade Atlas; RUSI.

An online shop front for Sinno Electronics provides an up-to-date inventory of its components.[213] Out of a total of 43 components readily available, 20 are listed as export controlled by BIS. Notably, many of these controlled components are produced by major microelectronics manufacturers such as NXP, Texas Instruments and STMicroelectronics. In fact, one of these components, produced by STMicroelectronics, is an STM32F103VCT6 microcontroller,[214] the very same model that was recovered from an Orlan-10 UAV used by the Russian Army in Ukraine.

Trade records and import declarations show that between 2017 and 2021, Sinno was exporting large volumes of semiconductors and microelectronics to a wide variety of Russian companies.[215] One of these, the Moscow-based OOO Trade-Component,

Customers in Live Interaction', press release, 6 April 2021, <https://expoelectronica.ru/Articles/press-release-en-ee-2021>, accessed 22 July 2022.

212 ExpoElectronica, 'Russian-Chinese Cooperation', <https://expoelectronica.ru/Page/russia-china-forum>, accessed 22 July 2022.

213 Hong Kong Inventory, 'Sinno Electronics Co., Limited', <http://hksinno.hkinventory.com/Shop/Page_Inventory.asp>, accessed 22 July 2022.

214 *Ibid.*

215 Trade data supplied by third-party commercial provider.

was sanctioned by the US government on 12 July 2021 for allegedly being 'involved in the procurement of U.S.-origin electronic components likely in furtherance of Russian military programs'.[216]

Sinno's shipments to OOO Trade-Component appear to have stopped in June 2021, when the Hong Kong vendor shipped over $100,000 worth of electronic integrated circuits branded as Analog Devices to Moscow.[217]

However, Hong Kong corporate records reveal that Becky Lin and Billy Hong have another locally registered company named Sigma Technology Limited (希舸電子技術有限公司)[218] that has been shipping large volumes of microelectronics and related goods to Russia.[219] According to trade records filed between April 2018 and June 2021, the company shipped over $3 million worth of goods to Russia, more than seven times than that shipped to Russia by sister company Sinno Electronics in the same period.[220]

Incorporated only two months after Russia's invasion of Crimea in 2014,[221] Sigma Technology only appears to have shipped goods to a small number of customers. One of these is RTKT, mentioned above, which received hundreds of shipments of microelectronics from Sigma between February 2017 and December 2021.[222] Curiously, while trade records for Sinno Electronics did not report any shipments of STMicroelectrionics-branded components to Russia between 2017 and 2021, Sigma had made at least 35 shipments of components from that brand to RTKT in the same period.[223]

Notably, Sigma also shipped microelectronics to other military suppliers, such as AO Radiopriborsnab,[224] an electronic-component supplier that forms part of the sanctioned (and ultimately Rostec-owned) Concern Radio-Electronic Technologies (Concern Radioelektronnye technologii, or 'CRET').

216 Bureau of Industry and Security of the US Department of Commerce, 'Addition of Certain Entities to the Entity List; Revision of Existing Entry on the Entity List; Removal of Entity from the Unverified List; and Addition of Entity to the Military End-User (MEU) List', Federal Register, 12 July 2021, <https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list>, accessed 10 July 2022.

217 Trade data supplied by third-party commercial provider.

218 Hong Kong Companies Registry, <www.icris.cr.gov.hk>.

219 Trade data supplied by third-party commercial provider.

220 *Ibid.*

221 Hong Kong Companies Registry, <www.icris.cr.gov.hk>.

222 Trade data supplied by third-party commercial provider.

223 *Ibid.*

224 Altana Trade Atlas, <https://altana.ai/atlas/>.

Conclusion

In the wake of Russia's invasion of Ukraine and the imposition of international sanctions, the Russian Presidential Administration established a committee to examine how the Russian defence industry could sustain production of critical military systems. Several laboratories of the Russian Academy of Sciences and major state-owned military enterprises were tasked with examining whether they could manufacture components in Russia, whether they could substitute components now sanctioned for alternative components manufactured in countries where supply would remain accessible, or whether it would be necessary to evade sanctions. The results of these studies were not encouraging. In order for Russian weapons to use foreign-sourced components, it is necessary for the manufacturer to justify to the Russian Ministry of Defence why the specific component must be used. The manufacturer must explain why it cannot be made in Russia economically, why an alternative component from a friendly country cannot be substituted and why the introduction of the component does not compromise the security of the device. For military communication systems, the specific architecture must also be approved by the FSB, which is responsible for assuring the security of Russian encryption. In short, the vast majority of foreign-made components identified in Russian weapons systems detailed in this report are for the most part critical to the viability of these systems.

Historically, Russian special services have had significant success in maintaining the supply of Western microelectronics. They obtained a high volume of components during the Cold War and expanded their procurement of these goods significantly after Cold War sanctions were lifted. In many cases, the Russian military has procured up to a decade's worth of components for critical systems in advance, precisely to safeguard production against sanctions. It is evident, however, that they have not achieved this for all the components identified in this report. Given that Russia had amassed an arsenal of complex weapons that posed a major threat to international security and has demonstrated in Ukraine that the Russian government has no inhibitions about using these weapons for the purpose of aggressive war, including to deliberately target civilians, the future strength of sanctions and enforcement is vital if Russia is not to rebuild its stockpiles.

Much of Russia's procurement of Western microelectronics for military purposes involved the use of false end-user certificates, front companies and transshipments. Mapping and

closing down these networks is a first step in constraining the Russian defence industry, but as Russia restructures its procurement architecture, abuses the Vienna Convention to move components procured under false pretences, and seeks to corrupt or infiltrate regulatory bodies, preventing the future transfer of such components to Russia will require significant and sustained vigilance. It is also evident – given the widespread use of third countries for transshipment of the onward selling of components – that constraining Russian defence industries will require significant international cooperation.

It is also important to grapple with the unintended consequences of the severing of access to critical components for Russia's complex weapons. Many states had depended on Russia as an arms supplier. The assurance of those arms remains critical to their national security. For countries like India, which sources 45% of its defence imports from Russia,[225] a loss of access to Russian equipment constitutes a security threat. This may encourage countries in this position to facilitate the evasion of sanctions. Alternatively, since few countries in this position have large microelectronic industries, it could be a catalyst to alter their suppliers. This presents opportunities for the Western alliance if it can bring constructive proposals to these states, while avoiding an exploitative approach to foreign military sales. It could also significantly sour relations with several powerful countries if no constructive proposals are forthcoming while Western sanctions undermine national security.

Russia's military power has been sustained by a silicon lifeline; one that runs from the US, through the UK, the Netherlands, Germany, Switzerland and France, to Taiwan, South Korea and Japan. Without that lifeline, the Russian military will be destined to employ increasingly obsolescent technology, without the means to deliver precision or efficiency on the battlefield. This may see Russia become increasingly dependent on China for its armaments, or revert to a more rapid escalation to tactical nuclear use in conflict, given the unfavourable dynamics that it must confront in conventional operations. The critical question this report puts before Western policymakers is whether this silicon lifeline is to be cut, and whether states are prepared to exploit the opportunities that severing it creates.

AUTHORS

James Byrne is the Director of Open Source Intelligence and Analysis (OSIA) at RUSI.

Gary Somerville is a Research Fellow in OSIA at RUSI.

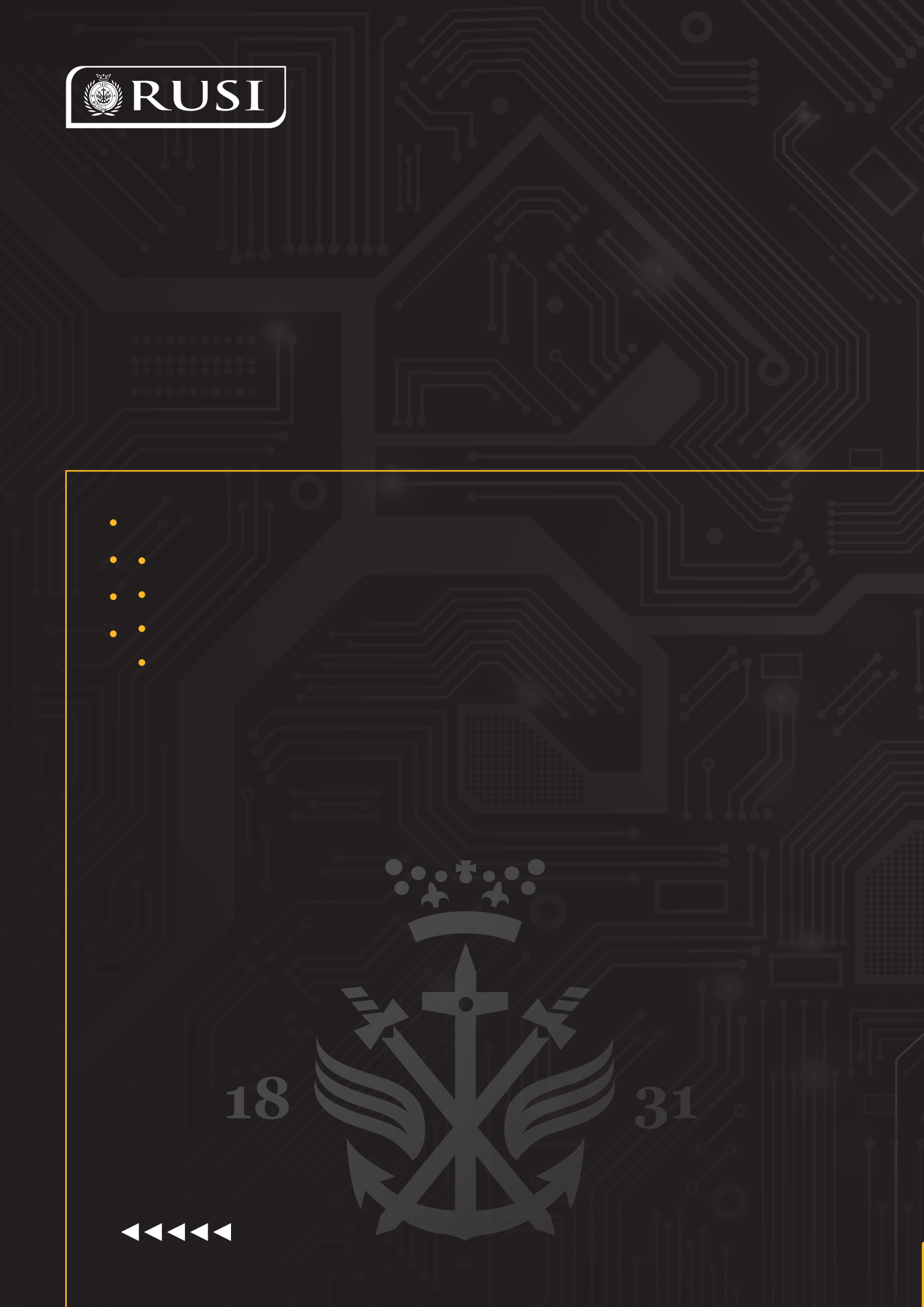
Joseph Byrne is a Research Fellow in OSIA at RUSI.

Jack Watling is Senior Research Fellow for Land Warfare at RUSI.

Nick Reynolds is a Research Analyst for Land Warfare at RUSI.

Jane Baker is an independent consultant.

225 *Economic Times*, 'Russia's Share of Arms Import to India Fell from 69% in 2012-17 to 46% in 2017-21: Report', 15 March 2022, <https://economictimes.indiatimes.com/news/defence/russias-share-of-arms-import-to-india-fell-from-69-in-2012-17-to-46-in-2017-21-report/articleshow/90218483.cms>, accessed 10 July 2022.


RUSI
18
31