Research Papers

December 2025

Disrupting Russian Air Defence Production: Reclaiming the Sky

RUSI

NEXTLEVEL

RUSI Research Papers, December 2025

ISSN 2977-960X

Cover image: Courtesy of pingvin57 / AdobeStock

Get in touch

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

The Royal United Services Institute for Defence and Security
61 Whitehall, London
SW1A 2ET
United Kingdom

Follow us on

Contents

Disclaimer

This publications has been prepared by RUSI and NLI for informational purposes only (the ‘Permitted Purpose’). While all reasonable care has been taken by RUSI and NLI to ensure the accuracy of material in this paper (the ‘Information’), it has been obtained primarily from fieldwork in Ukraine and open sources and RUSI and NLI make 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 and NLI 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 or NLI include their directors, trustees and employees.

For this paper, the authors have processed company, entity and individual names recorded in Russian. 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 identification of individuals, companies, organisations or entities within this paper does not imply that they have violated the laws of any relevant jurisdiction, or any international laws or sanctions, unless clearly stated. The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

Executive Summary

Russia produces some of the most formidable air defence systems in the world and fields them in large numbers. These pose a threat to NATO air forces and to conventional deterrence in Europe. They also intercept most Ukrainian munitions targeting Russia's infrastructure and industry and therefore contribute to securing the revenue generation that underpins Russia's aggression against Ukraine.

Despite these strengths, a comprehensive analysis of the manufacturing process of Russian air defence systems demonstrates significant vulnerabilities in their production that could be exploited to disrupt their modernisation and output. This paper demonstrates that Ukraine and its international partners could:

- Prevent the modernisation of Russian microelectronics production and disrupt the purchase of critical materials used in Russia's microelectronics industry. This would significantly impact the production of command-and-control and processing units in Russia's air defence systems.
- Sanction companies involved in the supply of raw and processed materials to Russia, such as beryllium oxide ceramics, which are critical to the production of radar.
- Use export controls to prevent the shipment of Western-made measuring equipment and calibration tools for quality control and certification of air defence systems.
- Exploit software critical to the design and development of Russian air defences through cyber intrusions, to gain information to enable the compromise of air defence complexes and disrupt production processes.
- Prioritise the kinetic targeting of critical nodes within air defence production that are vulnerable to deliberate attack.
- Impose sanctions to disrupt the repair and recovery of Russian air defence facilities that have been damaged by Ukraine and rely on Western-supplied machine tools.

Considering the vulnerabilities identified in this paper, Russia's international customers for air defences should reassess the resilience of these systems to attacks, including cyberattacks, technical compromise and disruption of resupply in supply chains.

Russia is currently expending more air defence interceptors than it is producing. If the expansion of the production of interceptors can be disrupted, the damage that Ukraine can inflict against Russia over 2026 will increase – thereby augmenting other efforts to pressure Russia to desist from its armed aggression against Ukraine.

Introduction

Russia fields some of the most capable integrated air and missile defence systems (IAMDS) in the world and produces them in high volumes. These systems present a barrier to adversary air forces. With up to 80% of NATO firepower currently being air delivered,[1] these systems are of disproportionate importance in shaping the conventional balance of power in Europe. They are also critical in determining the outcome of Russia's full-scale invasion of Ukraine, because they suppress Ukraine's air force, and shield Russia's defence industry and revenue-generation infrastructure from Ukrainian strike. Russia's ability to produce and continue to improve these systems is therefore of immediate and enduring importance.

There have been many studies on the performance and doctrine of Russian air and missile defences in recent years, including several by some of the authors of this paper.[2] Rather than focusing on tactical performance and military options to overcome Russian air defences – as in past work from the authors – this paper instead seeks to outline Russia's industrial base for the production of air defences, and in particular, to map its vulnerability to deliberate disruption. The paper seeks to highlight how Russia's adversaries may degrade the quality and reliability of Russian air defences, slow the production of key systems, increase the cost of production and undermine the future development of more capable air defences.

1. Justin Bronk in oral testimony to the House of Commons Defence Select Committee, 'Modernising Defence Programme', HC 818, Response to Question 131, 17 April 2018. This percentage will since have increased owing to the gifting of large portions of NATO's conventional artillery fleets to Ukraine.
2. Justin Bronk, 'Modern Russian and Chinese Integrated Air Defence Systems: The Nature of the Threat, Growth Trajectory and Western Options', *RUSI Occasional Paper* (15 January 2020), <https://www.rusi.org/explore-our-research/publications/occasional-papers/modern-russian-and-chinese-integrated-air-defence-systems-nature-threat-growth-trajectory-and>, accessed 7 November 2025; Jack Watling, Justin Bronk and Sidharth Kaushal, 'A UK Joint Methodology for Assuring Theatre Access', *Whitehall Report*, 4-22 (19 May 2022), <https://www.rusi.org/explore-our-research/publications/whitehall-reports/uk-joint-methodology-assuring-theatre-access>, accessed 7 November 2025; Justin Bronk and Jack Watling, 'Rebalancing European Joint Fires to Deter Russia', *RUSI Occasional Paper* (15 April 2025), <https://www.rusi.org/explore-our-research/publications/occasional-papers/rebalancing-european-joint-fires-deter-russia>, accessed 7 November 2025; Michael Jonsson and Robert Dalsjö (eds), 'Beyond Bursting Bubbles – Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction', FOI, 3 July 2020, <https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4991--SE>, accessed 23 November 2025.

This paper excludes certain topics related to Russia's IAMD capabilities. First, Russia's missile defence architecture includes satellites, sub-surface sensors and strategic intelligence that are beyond the scope of this paper, which is concerned with air defence. While these missile defence elements are alluded to, they are not analysed in detail. Furthermore, Russia uses electronic warfare (EW) as a critical component of its air defences. A tactical study would need to consider these systems in detail. However, from an industrial point of view, these systems are separate and will be explored subsequently in a future paper. Again, they are referred to but not analysed in detail. The paper instead focuses on Russia's strategic air defence complexes and short-ranged air defence (SHORAD) production, and primarily the S-400 and Pantsir surface-to-air missile systems (SAMs).

This paper draws on a wide range of sources. This included the physical examination of Russian air defence systems and the deconstruction of Russian air defence interceptors, as well as interviews with operators and technical staff conducting tests on Russian air defence equipment, and interviews with individuals previously involved in the supply chain, production and design of Soviet and Russian air defences. The paper also draws on an extensive survey of open source materials produced by Russian industry and on commercially available legal, trade and financial records. In addition, the paper utilises a large body of non-public materials from Russian defence industrial enterprises. Owing to the sensitivity of some of this sourcing, the origins of these materials is often withheld.

This paper is structured into three parts. The first chapter provides a basic overview of how radar and air defence systems work, how the Russian IAMDS is structured and its impact during Russia's full-scale invasion of Ukraine. This chapter is intended to provide a basic introduction to these systems and how they function for individuals responsible for disrupting industrial targets, including officials working on sanctions, export control enforcement and intelligence who lack military expertise. The second chapter outlines the critical industrial entities involved in the production of Russian air defence systems, where they are located and how they relate to one another. The third chapter presents an indicative sample of the industrial vulnerabilities in Russian air defence production that could be exploited by its adversaries.

Introduction to Russia's Integrated Air and Missile Defences

Assessing the potential for industrial disruption to Russia's air defence production first requires an outline of how the system functions, the complexes on which it is dependent and how it is tactically employed. This chapter, therefore, outlines the constituent elements of IAMDS with a particular emphasis on SAMs and how they function, the specific structure of Russia's IAMDS and the significance of these capabilities to Russia's armed aggression against Ukraine.

Surface-to-Air Missile Systems

Air defence systems are tasked with detecting and tracking airborne threats, guiding intercepts and preventing an enemy from penetrating defended airspace and damaging friendly forces and protected objects. Air defence systems comprise sensors, command-and-control (C2) elements and interceptors.

The primary sensor type in any air defence system is radar. Although visual light, thermal and acoustic sensors are also employed, they lack the range of radar; and, in the case of optical sensors, work poorly in low light or bad weather. Radio detection and ranging work by first emitting radio waves and then receiving the reflected energy off objects to determine their location and altitude relative to the radar, measuring the distortion in frequency to determine the object's speed and direction of travel.

Radar can emit across the spectrum of radio frequencies. Different frequencies are useful for different purposes, because they interact differently with the materials they pass through, are absorbed by, or reflect off. Radars function on different wavelengths to adjust the distance the energy travels relative to the power used and the level of resolution of the tracks generated. To track many objects across a large area and at long ranges, radars will often emit a longer wavelength to maximise range for power but will produce approximations of the target's location. Once an object of interest is detected, a higher frequency and therefore shorter wavelength will be directed at it, drawing more power to cover a smaller area, but enabling the precise tracking of the object.[3]

All radars require a source of power, an oscillator to form the correct waveform, an emitting antenna, a receiving antenna and a processing unit to make sense of the returned energy. Analogue, or mechanically-scanned array radar, emit on one frequency and receive on that frequency, with the radar's antenna being physically moved to track targets. It was subsequently found that, by having multiple emitting elements on the antenna, a radar could sequence their emissions to alter the direction of its beam, without moving the antenna surface. By having several antennas in one radar, it therefore became possible to emit multiple independently steerable beams within a specific waveband – and, once a target is identified, to have one antenna track the target while the remaining antennas continued to scan. These passive electronically scanned arrays (PESA) were subsequently turned into active electronically scanned arrays (AESA), whereby every emitting element is paired with its own receiving element such that the entire radar surface can be dynamically broken up to emit multiple frequency patterns and wavelengths without the radar having to move. This enables single radars to track large numbers of targets with different characteristics simultaneously (Figure 1).[4]

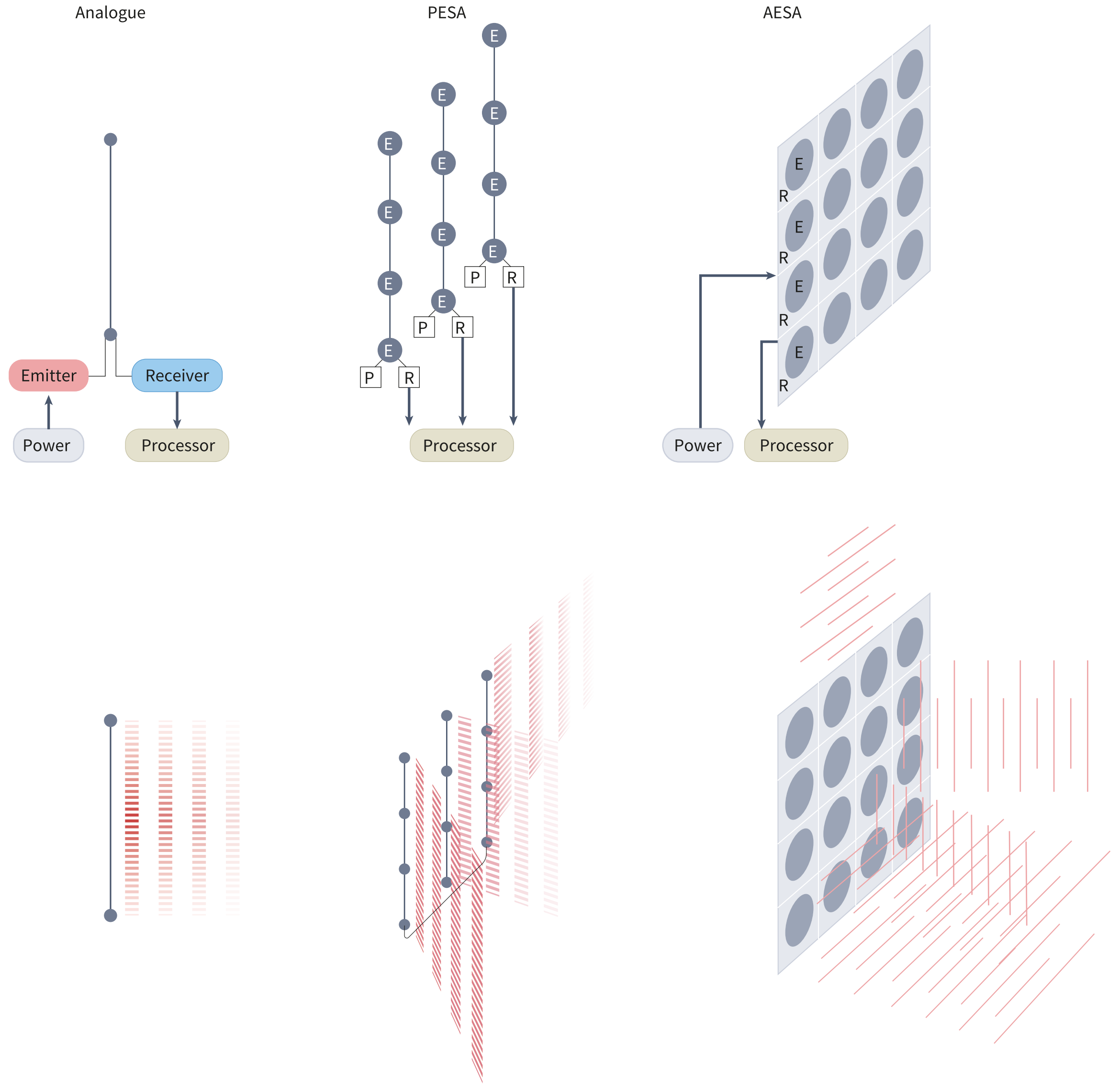
To achieve reasonable fidelity, radar must generally emit energy and function within line of sight. For ground-based radar, the view is limited by the horizon (Figure 2). Lower-fidelity tracking can be achieved by bouncing specific frequencies off the ionosphere or through passive sensing, whereby the radar receives energy that has been emitted from elsewhere or is part of the background environment and reflected off the target. Because an active radar must send out and receive the reflected signal to achieve a detection, whereas someone looking for the radar only needs to receive its emission, a radar can generally be detected at a distance that is 50% greater than the radar itself can detect objects.[5] Passive radars do not have this vulnerability but instead have a variable level of effectiveness, depending on the background electromagnetic activity in the environment.[6]

An IAMDS uses multiple kinds of radars, sometimes supported by thermal, electro-optical and acoustic sensors to detect, classify and track aerial threats. To do this, the system needs a library of known objects against which to compare a target's radar cross-section and a significant processing capability to make sense of the signals it

3. Merrill I Skolnik, *Introduction to Radar Systems* (London: McGraw Hill, 1981).
4. Carlo Kopp, 'Evolution of AESA Radar Technology', *Microwave Journal*, 14 August 2012, <https://www.microwavejournal.com/articles/17992-evolution-of-aesa-radar-technology>, accessed 12 October 2025.
5. MIT Lincoln Laboratory, 'Introduction to Radar Systems: Radar Range Equation', July 2018, <https://www.ll.mit.edu/sites/default/files/outreach/doc/2018-07/lecture%202.pdf>, accessed 22 November 2025.
6. NASA, 'Remote Sensing Fundamentals', <https://gpm.nasa.gov/image-gallery/active-and-passive-remote-sensing-diagram>, accessed 12 October 2025.

receives. Precisely because IAMDS require multiple types of radar to be effective and must thereafter pass their tracks to an interceptor that can engage or shoot down aerial targets, they must move data around a geographic area. They are therefore dependent on low-latency communications.

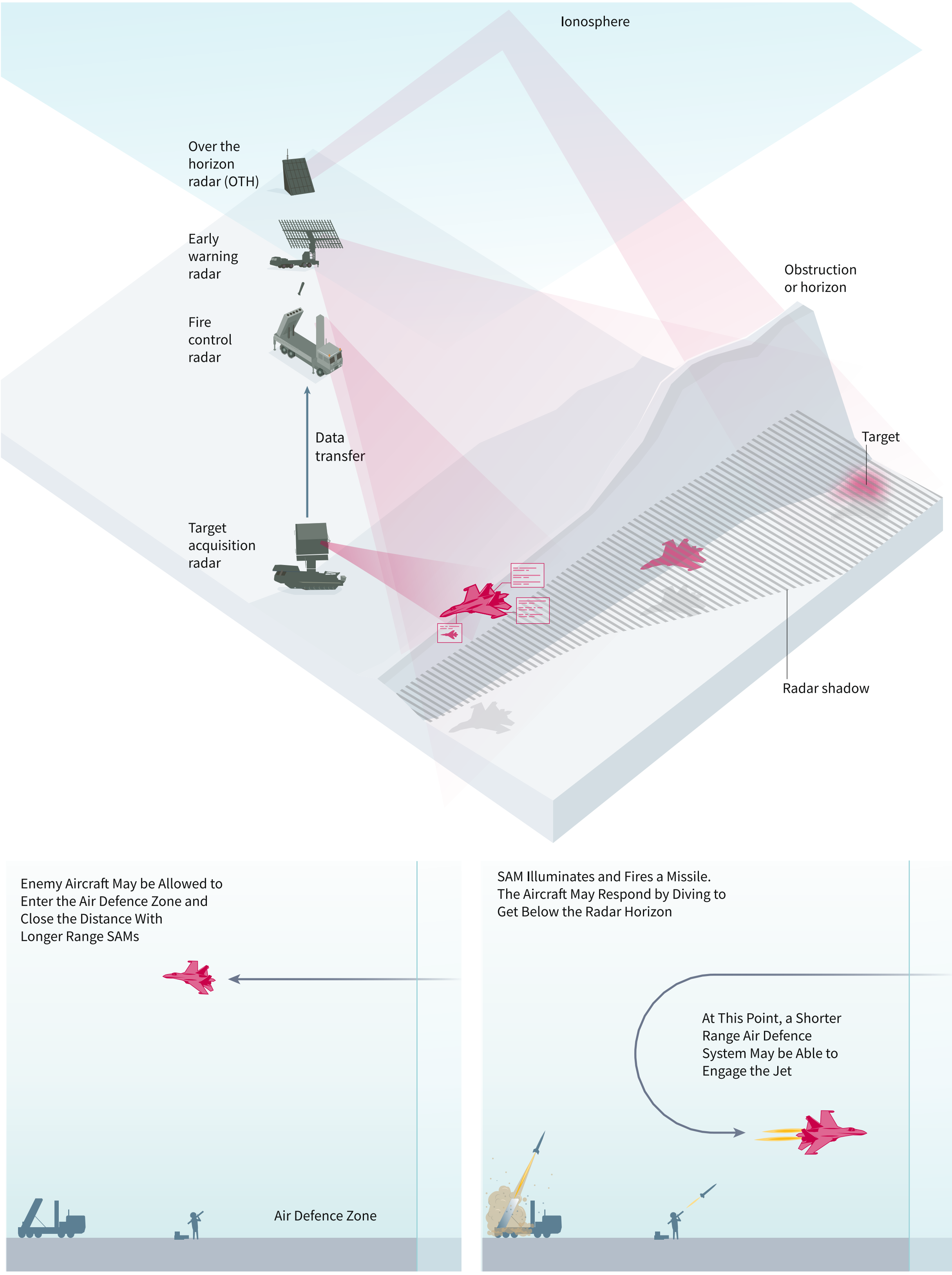
Figure 1: The Evolution of Radar



Source: The authors and Alex Whitworth.

Just as an air defence system needs multiple kinds of radar to accurately detect, classify and engage threats, it also needs multiple kinds of interceptor. This is primarily because different threats vary by speed, attack profile and cost. An interceptor that can defeat a ballistic missile travelling at hypersonic speeds, for example, can hit a powered bomb such as a Shaheed-136, but one such interceptor may cost the same as up to a hundred Shaheeds. Conversely, an interceptor UAV that can hit a Shaheed-136 will lack the acceleration, engagement ceiling or terminal effect necessary to intercept a ballistic

Figure 2: Detection Layers Within an IAMDS



Source: The authors and Alex Whitworth.

missile. A cannon, meanwhile, may be able to track a cruise missile and shoot it down, but will lack the range to hit an aircraft at high altitude.

Air defence missiles – comprising the bulk of interceptors – must each feature a motor, control surfaces to alter course, a fuze, a warhead and a sensor fit that allows it to be guided to its target. Sensors may be thermal, as with Man Portable Air Defence Systems (MANPADS). They may also be electro-optical. Most involve radar, either on the missile's nose, or on the ground, with the track passed via a communications link to the missile. Any single logic of engagement can generally be defeated tactically. A missile dependent on guidance from a radar can have its target engagement radar jammed or struck or the target may pass below the horizon so that the radar loses lock. A missile with an active seeker can see its target vary direction such that it burns speed by altering course and thereby runs out of range to reach its target. A missile that is guided by the ground radar with periodic updates so that it minimises course changes, only to go active and use its own radar to track the target when in close proximity, will maximise its manoeuvrability and speed in the terminal phase and so maintain range. These systems are expensive and complex to operate, however.

Coordinating and running such a complex, geographically dispersed, and essential system (that must also avoid shooting down friendly munitions, drones and aircraft) requires well-trained and practised operators. It is dependent on low-latency communications between these various elements and software support that allows the system to identify and keep track of all the objects it can detect. Design bureaus and labs are not only relevant to the construction of air defence systems; the scientists and technicians of the design bureaus are an integral and ongoing part of IAMDS operations. As new air threats emerge with different characteristics, and as the enemy develops EW techniques to interfere with radars, ongoing work to update and upgrade air defence systems will be required to maintain their performance.

An integrated air and missile defence system is a collection of complementary components. If properly designed, it is not the case that the compromise of a single component collapses the system. However, as with all interlocking systems, once a component is compromised, gaps start to emerge in an otherwise resilient structure. These gaps can be exploited. Disruptions to an IAMDS cannot be achieved by targeting one element, but multiple effects can compound until the system loses its coherence.

Integrated Air and Missile Defence System

As far back as the 1970s, the Soviet Union acknowledged that it would struggle to keep pace with advances in NATO aircraft construction. The precision revolution in warfare that followed further convinced the Soviets, and thereafter the Russian Federation, that it needed an asymmetric counter to NATO airpower, because NATO airpower offered the Alliance an advantage and yet was also a dependence.[7] Combined with a persistent anxiety about nuclear bombers in the 1950s and cruise missiles in subsequent decades, given its large size, the Soviet Union (and thereafter the Russian Federation) invested disproportionately in IAMD. The result is one of the densest, most sophisticated and most integrated air defence networks in the world. Before considering how it can be disrupted, it is necessary to describe its constituent parts.

Ballistic Missile Defence

At the heart of the Russian IAMDS are the components responsible for countering nuclear threats. These include strategic intelligence collection against nuclear strike forces; early-warning radar such as 77Ya6-M Voronezh-M, 77Ya6-DM Voronezh-DM and older Daryal; and satellites for tracking missiles, including the US-KMO, US-K and Oko early-warning constellation. The primary ballistic missile defence (BMD) system is the A-135 protecting Moscow, which is managed with the Don-2N AESA radar, paired with 53T6 nuclear-armed interceptors.

Russia is currently significantly upgrading its BMD capabilities through the delivery of the A-235 missile defence system for Moscow, using a hit-to-kill interceptor rather than a nuclear-armed interceptor, and the S-500 system. The S-500 is a mobile system with significant commonality with Russian air defence systems (discussed later), but is equipped with the 77N6 and 77N6-N1 missiles for engaging ballistic missiles and satellites, respectively.[8]

Strategic SAMs

Beneath the BMD system are the strategic SAMs of the Russian Aerospace Forces (VKS) and ground forces. The role of these systems is to provide situational awareness and C2 for the integrated air defence network, and to hold at-risk enemy aircraft at long range, including enabling aircraft (such as tankers).

Russia's strategic SAMs are derivatives of the S-300 family. Newer variants of the S-300 are still in widespread service, especially tracked variants for protecting ground forces during manoeuvres, although the S-400 is the most modern system. These SAMs all comprise the same groupings of equipment with similar roles. This paper outlines the components of the S-400 system, although there are analogue systems for the S-300 and S-350 that perform the same functions, albeit with less range and effectiveness.

7. Mary FitzGerald, 'Marshal Ogarkov and the New Revolution in Soviet Military Affairs', Center for Naval Analysis, January 1987, <https://apps.dtic.mil/sti/tr/pdf/ADA187009.pdf>, accessed 7 November 2025.
8. Jacob Mezey, 'Russian and Chinese Strategic Missile Defence: Doctrine, Capabilities, and Development', Atlantic Council, 10 September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russian-and-chinese-strategic-missile-defense-doctrine-capabilities-and-development/>, accessed 12 October 2025.

Contributing to Russia's mobile strategic SAMs are over-the-horizon (OTH) radar, such as the static Kontayner 29B6 and Resonance-N, able to monitor the approach of aircraft significantly beyond Russia's borders. Strategic SAM brigades are supported by several radar optimised for tracking different kinds of targets. VKS A-50U Beriev airborne early warning and control (AWACs) aircraft offer the strategic SAMs coverage from a wide area look-down radar to maintain situational awareness over the horizon of ground based radars. Wide-area air surveillance radar, such as the 12A6 Sopka-2, also help maintain coverage over large areas.[9]

In addition to the fixed radar installations described above are a range of radar, which are organic to the mobile air defence formations that collectively ensure effective radar coverage:

- The NEBO-M: A wide area surveillance radar optimised for detecting low-observable targets.
- The 48Ya6-K1 Podlet: Used as an approach detection radar, used to track targets at low altitude.
- The 96L6E: An AESA surveillance and target acquisition radar optimised for the detection of objects moving at a high altitude, including ballistic missiles.
- The 91N6 radar: An S-Band surveillance and tracking radar used for long-range target tracks.

Collectively, these radars provide the S-400 system with significant range and coverage against various threats. Because they are long-range systems, they can sit well behind the defensive layers of air defences to watch for approaching threats. The data from these various radars is fused through the S-400 C2 system and then pushed to batteries.[10]

The heart of the S-400 battery is the 92N6 engagement radar. This hardened system, which is difficult to jam, can manage engagements against a large number of simultaneous tracks. It will provide track data to the battery command vehicle,

9. For a comprehensive overview, see: Tom Withington, 'Russian IADS Redux Part-1: Resonating with Resonance', *ARMADA International*, 2 March 2023, <https://www.armadainternational.com/2023/03/russian-air-defence-systems-part-1-resonance-radar/>, accessed 7 November 2025; Tom Withington, 'Russian IADS Redux Part-2: Hilltop View', *ARMADA International*, 5 April 2023, <https://www.armadainternational.com/2023/04/russian-air-defence-analysis-part-2/>, accessed 7 November 2025; Tom Withington, 'Russian IADS Redux Part-3: Strategic Skywatchers', *ARMADA International*, 4 May 2023, <https://www.armadainternational.com/2023/05/russian-air-defence-analysis-part-3/>, accessed 7 November 2025; Tom Withington, 'Russian IADS Redux Part-4: Missing Link', *ARMADA International*, 8 June 2023, <https://www.armadainternational.com/2023/06/russian-air-force-tactical-communications/>, accessed 7 November 2025; Tom Withington, 'Russian IADS Redux Part-5: Reset Password?', *ARMADA International*, 6 July 2023, <https://www.armadainternational.com/2023/07/russian-air-force-iff-radar/>, accessed 10 November 2025.
10. Ministry of Defence, Development Concepts and Doctrine Centre, 'Joint Air Defence: Joint Warfare Publication 3-63', July 2003, <https://assets.publishing.service.gov.uk/media/5c814432e5274a2a5d70cd2c/archive_doctrine_uk_joint_air_defence_jwp_3_63.pdf>, accessed 12 October 2025.

which will then assign the battery's transporter erector launchers (TELs) to engage the relevant targets. The S-400 has canisterised interceptors, so that a vehicle can carry multiple types of interceptor. The most long-range and capable is the 40N6, which has an active seeker and engages with a lofted trajectory, coming down against its targets so that they cannot dive to avoid being hit. The 48N6 is a shorter-ranged missile with a more traditional trajectory but is significantly cheaper. The system is also armed with the 9M96 missile, which is substantially shorter-ranged but can be carried in larger numbers.[11]

Tactical SAMs

Russia's strategic SAMs are highly effective but not optimised for protecting manoeuvring forces. Strategic SAMs for defending territory are fielded by the VKS, while ground forces use strategic SAMs to protect critical nodes. To protect the manoeuvre units themselves from air attack, Russia fields tactical SAMs that can keep up with the units.

The core system fulfilling this role is the Buk-M3. The Buk battalion comprises a command vehicle, responsible for directing the battalion's engagements but also capable of receiving feeds from strategic SAMs and the VKS to maintain a common air picture. The battalion also has a dedicated surveillance and target acquisition radar. This vehicle pair coordinate and direct six transporter erector launcher and radar (TELAR) vehicles with their own engagement radar and three TELs.

As tracked vehicles, these air defence platforms can move quickly over rough terrain and, while having less range than the strategic SAMs, can use the situational awareness from a higher echelon to avoid illuminating until the enemy is well within their engagement envelope. The system is also optimised to set up and collapse quickly.

Short-Ranged Air Defence

Although highly effective, the large Russian SAMs are not optimised for engaging low-flying cruise missiles, attack helicopters or UAVs. Moreover, while capable of shooting down munitions, the strategic SAMs risk being saturated. For this reason, the Russians also invest in large numbers of SHORAD systems that act as 'goalkeepers', moving with S-400 and Buk units, or sitting on the perimeter of key sites to engage with what breaks through the integrated air defence system.[12]

The primary SHORAD systems in Russian service are the 9K330 Tor-M2 and 96K6 Pantsir-S2. The Tor is a tracked SAM with a rapid set up and target acquisition capability,

11. Bronk, 'Modern Russian and Chinese Integrated Air Defence Systems'.
12. Lester Grau and Charles Bartles, *The Russian Way of War* (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), p. 271.

optimised for short-range and low-altitude engagements against fast or fleeting targets (such as cruise missiles and helicopters). It can also defeat a range of munitions.

The Pantsir-S2 is an air defence module with organic target acquisition and engagement radar, anti-aircraft cannon and modular missile canisters that can be mounted on a range of vehicle chassis or emplaced. Although it has had a lower probability of kill (Pk) than Tor, it is cheaper and has been periodically improved. Beyond this, the Russians are experimenting with a wide range of counter-UAV systems. These SHORAD systems present a pervasive 'pop-up' threat over Russian forces, as they can draw on radar tracks from higher echelons to then ambush overflying aircraft. Russia also distributes large numbers of MANPADS to its ground forces and has significant legacy stocks of both towed and self-propelled anti-aircraft artillery systems.

It is important to briefly cover who the operators of Russian SAMs are. Unlike the bulk of personnel in line units, SAM operators are overwhelmingly contract soldiers with significant technical and tactical training. Russian air defence systems have withstood modest damage during the full-scale invasion of Ukraine, enabling the force to steadily build experience.

At the same time, the war has shown the dependence of the operators on operational integration to make the right decisions. When isolated, under pressure from multiple threats, faced with uncertainty as to the performance of their equipment, or simply exhausted, operators have made important errors, including shooting down friendly aircraft and even a civilian airliner.[13] Understanding declining operator performance and their degree of confidence in their equipment is beyond the scope of this paper, but remains critical to effectively disrupting Russia's IAMDS.

Impact of Russian Air Defence During its Invasion of Ukraine

Ukraine's persistent strikes on Russian territory over the course of the war have created a popular perception that Russian air defences are not very effective. This is misleading. Russian air defences have imposed significant constraints on Ukraine's military, shielded the Russian military and industry from the bulk of attempts to strike them in depth and improved substantially over the course of the war. Russia has also avoided using some parts of its air defence systems that are most concerning for NATO. At the same time,

13. *Sky News*, 'Putin Admits Russia Shot Down Azerbaijani Passenger Jet, Killing 38', 9 October 2025, <https://news.sky.com/story/putin-admits-russia-shot-down-azerbaijani-passenger-jet-killing-38-13447588>, accessed 7 November 2025.

Russian air defences can be penetrated and destroyed. They are not insurmountable but are a major obstacle to efficiently striking Russian forces and territory.

In the first few days of the war, Russian air defenders were under orders to treat all aircraft and other aerial vehicles as friendly. The result was embarrassing, as Ukrainian UAVs and aircraft struck Russian columns. Russian air defences quickly transitioned to protecting key nodes, and losses of Ukrainian aircraft increased immediately. This incentivised the Armed Forces of Ukraine (AFU) to keep aircraft low – below 250 ft. The general rule became that only low-altitude flying was survivable within 80 km of the frontline.[14] Nevertheless, one Ukrainian aircraft was shot down by Russian air defences at a range of 150 km while flying below 50 ft. Ukrainian aircraft can still launch sorties when conditions are favourable or when air defences have been distracted or displaced.[15] Nevertheless, they are heavily constrained and are now dependent on stand-off weapons to deliver strikes. Russian air defences – beyond constraining Ukrainian air operations – continue to destroy Ukrainian aircraft on a semi-regular basis.[16] For a short period, Ukraine had some success using AGM-88 high-speed anti-radiation missiles (HARMs) to strike Russian air defence radar, thereby creating gaps in their defences. Russian SAM operators, however, rapidly learned to turn off their radar – or, in more densely defended sectors, to simply shoot down the HARMs on approach.[17]

The Ukrainians delivered a second shock to Russian forces when precision ground-based fires entered their arsenal in June and July 2022. Guided multiple launch rocket systems (GMLRS), and later, army tactical missile systems (ATACMS), inflicted substantial losses on the Russians when first employed. Nevertheless, over time, Russian air defences learned how to track and engage these munitions effectively and the rate of successful hits dropped from close to 70% with GMLRS in 2022, to around 30% in 2023 and 2024, and often close to 8% in 2025.[18] For attacks on components of the air defence system, it has been found that up to 10 ATACMS must be committed to destroy one radar.[19] These overall percentages conceal a crucial contextual detail: with the right combination of strike systems, good intelligence and EW, hit rates can be brought back up. But this slowed the pace of Ukrainian strikes, removed many targets from consideration, and therefore had second-order consequences for Ukrainian options that are harder to quantify.[20] Another aspect of Russian improvement was the efficiency of their engagements. When ATACMS first came into theatre, for example, the number of S-400 interceptors that the Russians would fire to defeat them was

14. Author interviews with Ukrainian air force pilots, Ukraine, August and October 2022.
15. Dag Henriksen and Justin Bronk (eds.), *The Air War in Ukraine: The First Year of Conflict* (Abingdon: Routledge, 2024).
16. Author engagements with Ukrainian air force, Ukraine, 2025.
17. Author interviews, Ukrainian air force personnel, Ukraine, March 2023.
18. Data supplied by the Armed Forces of Ukraine (AFU), Ukraine, August 2025.
19. Author interviews, Ukrainian officers involved in deep strikes, Ukraine, August 2025.
20. Data supplied by the AFU, Ukraine, January, March, June and August 2025.

disproportionate. Over time, the integration of the Russian system has improved, with far more effective matching of appropriate interceptors to targets.

Russia similarly struggled to prepare for Ukraine's long-range strike campaign on its territory, which is ironic considering how publicly Ukrainian officials discussed it.[21] Russia has continued to take hits around oil refineries, military-industrial sites and logistics hubs as Ukraine has scaled the production of a wide range of long-range strike systems.[22] The regular images of fires in Russia have caused a perception that Russian air defences are failing to protect the territory.

The reality is more complex. There are a lot of targets in Russia, and they are geographically dispersed, meaning that they cannot all be defended. Ukraine has, over time, become quite adept at attacking targets that lack air defence and has prioritised targets where flammable or sensitive materials will allow small numbers of munitions with limited payloads to cause cascading damage to a facility. This leaves large numbers of targets that the Russians have decided to defend, and that, consequently, Ukraine has struggled to hit. When Ukraine has attacked more protected targets, the results have been consistent. Out of a salvo of 100–150 UAVs, costing between $20,000 and $80,000 each, around 10 will get to their target, where their small payload often causes negligible damage that can quickly be repaired.[23] The overall success rate of Ukrainian strikes has been that less than 10% of munitions have reached a target, and fewer still have delivered an effect.[24] Successful strikes on hardened targets have often required Ukraine to fire over 100 UAVs on one attack vector to exhaust the air defences in a sector, and only then fire cruise missiles or larger UAVs to deliver damage. Even where Storm Shadow or other prestige weapons are used by Ukraine, the improvements in Russian munitions matching have meant that they often intercept over 50% of these munitions, even when they are part of a complex salvo.[25]

Russia's air defences, therefore, have absorbed many resources from Ukraine, and have made large numbers of high-value targets unreachable. On several occasions, Ukraine has lined up complex attacks and gamed the air defence system to get munitions on target. Such techniques are rarely repeatable; nevertheless, as more is known about how the Russian systems function, vulnerabilities can be found and exploited. Moreover, while the cost of the UAVs is not inconsequential, neither is the price of interceptors. Russia's ability to resupply its launchers, and thus the industrial

21. Ukrainian campaigning for suitable munitions was conducted with the slogan, 'kill the archer, not the arrow', see Illia Kabachinskyi, 'Kill the Archer, Not the Arrow: Ukrainians Urgently Seek US Approval to Strike Back at Russia', *United 24*, 3 September 2025, <https://united24media.com/war-in-ukraine/kill-the-archer-not-the-arrow-ukrainians-urgently-seek-us-approval-to-strike-back-at-russia-2090>, accessed 23 November 2025.
22. Tom Balmforth et al., 'Inside Ukraine's drone campaign to blitz Russia's energy industry', *Reuters*, 16 October 2025.
23. Author interviews with Ukrainian officers, Kyiv, October 2025.
24. Data supplied by the AFU, Ukraine, October 2025.
25. Author interviews with Ukrainian officers responsible for strike operations, Ukraine, August 2025.

production of air defence interceptors, is ultimately critical to Ukraine's ability to expand the rate of damage it can inflict.[26]

A final consideration is that Russia has suffered attrition of air defence equipment during the invasion of Ukraine but has also withheld some of its more capable systems: 40N6 long-range air defence missiles have not been used, and 48N6 missiles have been fired sparingly. Russian air defence interceptors are currently being fired faster than they can be produced,[27] but this is overwhelmingly concentrated in older or obsolete platforms such as 9K33 Osa and SHORAD systems, especially Pantsir.

Russia is now trying to significantly increase the production of interceptors for Pantsir to overcome this shortfall. Russia has experienced losses of some higher-echelon radar, but at a rate that has allowed their replenishment. The combination, therefore, of Russia's expanding production of air defences, the limited attrition of systems over the course of the war, and their improvement as they confront Western systems means that they remain a major obstacle to NATO airpower and especially European airpower.

Russia's ability to continue to improve and expand its air defences, relative to Europe's ability to build munitions suitable for suppressing or destroying air defences, is both a critical metric in the conventional balance of forces in Europe and sets the context for the feasibility of long-term security guarantees for Ukraine. This question, therefore, cuts to the heart of both Ukraine's future and the assurance of European security. The next chapter, in turn, maps how Russia produces its air defences.

26. Author interviews with Ukrainian officers overseeing the long-range strike campaign, Ukraine, 2022–25.
27. Author interviews with Ukrainian intelligence officers, Ukraine, August 2025.

Mapping Russia's Air Defence Industrial Ecosystem

To evaluate the resilience and capacity of Russian air defence production, it is necessary to map the ecosystem of companies involved and their role. Like most critical defence projects in Russia, the air defence enterprise revolves around a single, central industrial entity which manages the contracting of subordinate entities for the design, assembly, subsystem manufacture and supply of raw materials to deliver the project. This hub-and-spoke approach, whereby a core company manages the interactions throughout the supply chain and lifecycle for a system, means that the centre holds all critical data on timelines for delivery and development. Nevertheless, beneath this monolithic structure are a very large number of subordinate entities.

In the case of S-400 and much of the remainder of Russia's air defence network, the enterprise is subsumed within the Almaz-Antey concern. This chapter breaks down the corporate structure for the production of S-400 missiles, radar, C2 systems and SHORAD to the second, and in some cases third, tier of the supply chain.

Missiles

Design of 40N6 and 48N6 missiles, along with other interceptors for the S-400 Complex, is carried out by the Joint Stock Company (JSC) Machine-Building Engineering Office Fakel named after academic P D Grushin (hereafter called Fakel), based in Khimki, Moscow Oblast.[28] The missiles are ultimately assembled, and the supply chains for their sub-components contracted and managed, by the Moscow-based MMZ Avangard.[29]

28. « АО МКБ «Факел» имени академика П. Д. Грушина » ['JSC MKB "Fakel", Named After P D Grushin'], <https://www.mkbfakel.ru/>, accessed 22 September 2025.
29. « Московский машиностроительний завод «Авангард» » ['MMZ "Avangard"'], <https://www.mmzavangard.ru/>, accessed 12 October 2025.

MMZ Avangard, however, sits at the heart of a multi-tier supply chain with suppliers responsible for the delivery of the missile engines, bodies, navigational subsystems, communications, seeker heads, canisters and payloads.

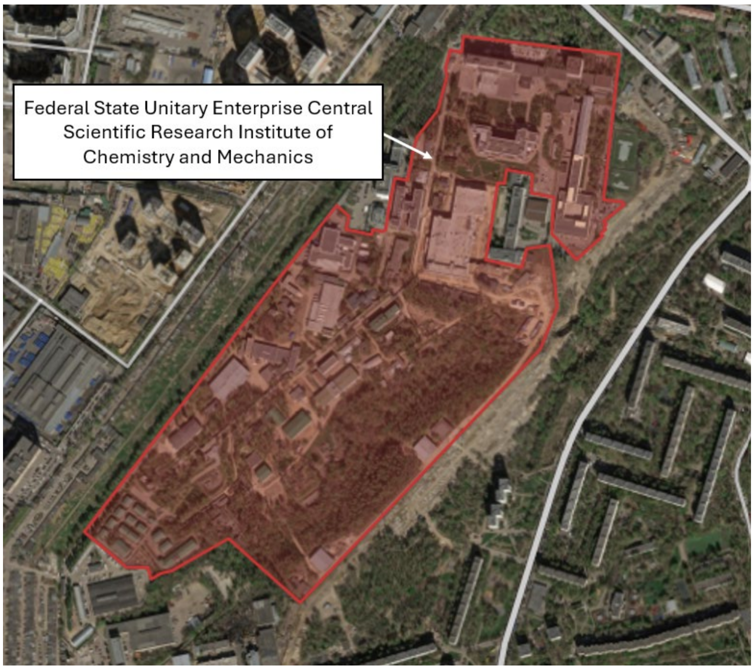
The missile engines for Russia's air defence interceptors are produced by Kamensky Combine, with its primary production site located in Kamensk-Shakhtinsky in Rostov Oblast,[30] and at the Samara-based Salyut JSC.[31] These factories receive materials from the Soyuz Federal Center of Dual Technologies (FSUE), located in Dzerzhinsky, Moscow Oblast,[32] and additional raw materials from the Anozit Federal State Enterprise in Kuibyshev, Novosibirsk Region – the likeliest material being ammonium perchlorate, since Anozit is its only supplier in Russia.[33]

The missile casings are manufactured by JSC KUMZ, with its main production site at Kamensk-Uralsky in Sverdlovsk,[34] while critical components of the launch mechanism are made by Gidroagregat of Pavlovo, Nizhny Novgorod Oblast.[35] Composite materials for the missile body are supplied by the Obninsk Research and Production Enterprise 'Technology' named after A G Romashin.[36] DPO Plastik of Dzerzhinsk fabricates the launch canisters for all Russian tube-launched military systems, from MANPADS to the massive cylinders for 40N6 and 48N6 air defence interceptors.[37]

The production of warheads for Russia's air defence interceptors are concentrated at the Federal State Unitary Enterprise Central Scientific Research Institute of Chemistry and Mechanics in Moscow.[38] Triggers for the warheads are supplied by IMPULS, with its main facility in Moscow (Figure 3).[39] The Moscow-based institute is an instructive example of Russia's defence industrial enterprises. The institute presents itself as being engaged in research, with a narrow frontage and a low profile. Financial documents, however, show that the large factory complex behind its façade delivers over $61 million of product to MMZ Avangard and is responsible for large-scale production of munitions.[40]

30. « ФКП «Комбинат "Каменский» » ['FKP "Kamensky" Combine'], « О компании » ['About the Company'], <https://www.fkpkk.ru/company>, accessed 12 October 2025.
31. « АО «Салют» » ['JSC "Saylut"'], <https://www.ao-salut.ru/>, accessed 12 October 2025.
32. Rusprofile, « АО «ФЦДТ» Союз » ['JSC FSDT "Soyuz"'], <https://www.rusprofile.ru/id/1245000132937>, accessed 12 October 2025.
33. « ФКП «Анозит» » ['FPK "Anozit"'], <https://www.anozit.ru>, accessed 12 October 2025.
34. « КУМЗ » ['KUMZ'], <https://www.kumz.ru/>, accessed 12 October 2025.
35. « АО «Гидроагрегат» », ['JSC "Gidroagregat"'], <http://www.gidroagregat-nn.ru/>, accessed 12 October 2025.
36. « АО "Обнинское НПП «Технология» имени А. Г. Ромашина» » ['JSC Obninskoye NPP "Technology", Named After A G Romashina'], <https://www.technologiya.ru>, accessed 11 November 2025.
37. « АО ДПО «Пластик» » ['JSC DPO "Plastic"'], <https://dplast.ru>, accessed 11 November 2025.
38. « ГНЦ РФ ФГУП «Центральный научно-исследовательский институт химии и механики» » [GNC RF FSUE "Central Scientific Research Institute of Chemistry and Mechanics"'], <https://cniihm.ru>, accessed 12 October 2025.
39. « ПАО НПП «ИМПУЛЬС» » ['PJSC NPO "IMPULS"'], <https://impuls.ru/>, accessed 12 October 2025.
40. According to 2024/25 financial data reviewed by the authors.

Figure 3: Warhead Production Site



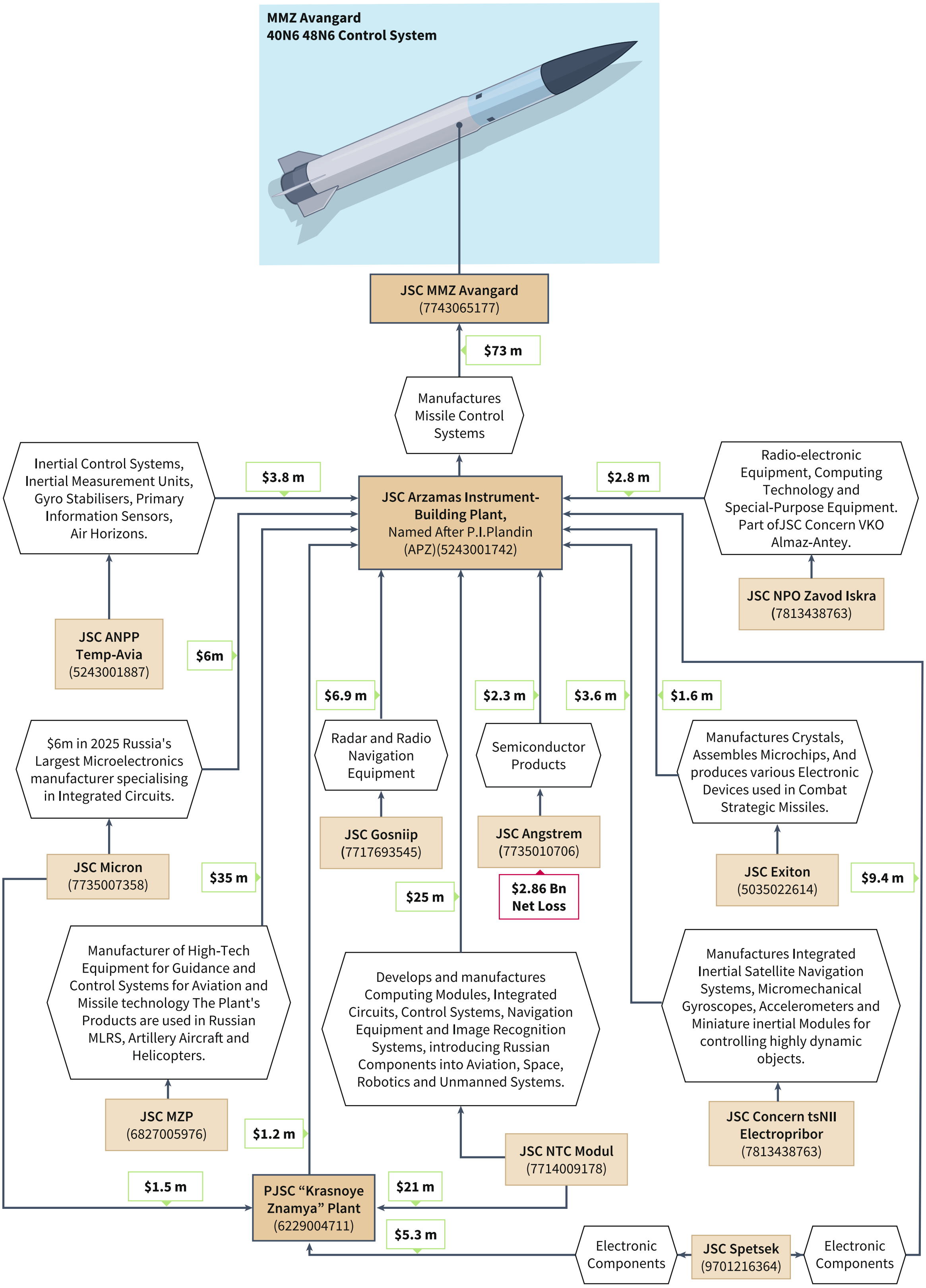
Source: Produced using Felt mapping tools, <https://felt.com/>, accessed 22 November 2025.

Beyond the motor, casing and warhead, air defence interceptors include complex electronics to manage the missile control surfaces, communications suites to receive updates from supporting radar and homing heads to track the target and determine the appropriate point to detonate. All must be resilient on a platform under immense G-loads, as the missile aggressively accelerates and manoeuvres.

The missile control systems on S-400 missiles (Figure 4) are assembled by JSC Arzamas Instrument-Building Plant Named After P I Plandin[41] and located in Arzamas, Nizhny Novgorod Oblast, which sold some $72 million of product to MMZ Avangard in 2024.[42] The plant receives inertial control systems built by NPP Temp-Avia JSC and located in the same city;[43] control elements – including hydraulic and pneumatic mechanisms – from Gidroagregat of Pavlovo, Nizhny Novgorod Oblast;[44] and radar and navigation subsystems from the State Research Institute of Instrument Engineering JSC (Gosniip) in Moscow.[45]

41. « АО «Арзамасский приборостроителный завод имени П. И. Пландина» » [‘JSC Arzamas Instrument-Making Plant Named After P I Plandin’], <https://www.aoapz.ru>, accessed 12 October 2025.
42. According to 2024/25 financial data reviewed by the authors.
43. « АО Арзамасское НПП «ТЕМП-АВИЯ» » [‘JSC Arzamas NPO “TEMP-AVIA”’], <https://temp-avia.ru/>, accessed 12 October 2025.
44. « АО «Гидроагрегат» » [‘JSC “Gidroagregat”’], <http://www.gidroagregat-nn.ru/>, accessed 12 October 2025.
45. « АО Государственный научно-исследовательский институт приборостроения» [‘JSC State Research Institute of Instrument Engineering’], <http://www.gosniip.ru/>, accessed 12 October 2025.

Figure 4: Missile Control Systems Supply Chain



Source: Authors and Alex Whitworth; amounts based on financial records for 2024 seen by the authors.

S-400 interceptors also use computing modules supplied by JSC NTS Modul of Moscow,[46] guidance subsystems from MZP JSC in Michurinsk, Tambov Oblast[47] and satellite navigation subsystems from Concern TsNII Elektropribor JSC.[48] Beneath each of these second-tier suppliers are third-tier manufacturers of microelectronic components, raw and processed materials and machine tooling.

MZP JSC, for example, is supplied by JSC Scientific Production Complex Elara Named After G A Ilyenko (hereafter JSC Elara),[49] in Cheboksary in the Chuvash Republic. This complex is supplied by ZPP from Nizhny Novgorod, Testpribor and DZRD.[50] In many cases, specialist electronic manufacturers sell to multiple subsystems' producers in the missile supply chain. JSC Elara, for example, also sells integrated flight control modules to TVEL (the Rosatom subsidiary), which also contributes to missile production.[51]

The homing heads for S-400 interceptors are assembled by PJSC Krasnoye Znamya Plant in Ryazan,[52] which sold $480 million of products to MMZ Avangard in 2024.[53] Behind these systems is a complex ecosystem of manufacturers and subsystems, including:

- Vacuum microwave devices from Moscow-based Pluton JSC.[54]
- Radio transceivers and receivers from Salyut JSC in Nizhny Novgorod.[55]
- Circuit boards from the Mariyskiy Machine-Building Plant JSC in Yoshkar-Ola, Republic of Mari El.[56]
- Radio-electronic equipment from Saturn JSC in Omsk.[57]
- Converters and amplifiers from the JSC Experimental Design Bureau of Microelectronics (JSC OKB-MEL) in Kaluga.[58]
- Microchips and processors from the NTC Modul Scientific and Technical Centre of Moscow.[59]

Each of these companies draws on several producers of general electrical components.

46. « АО НТЦ «Модуль» » ['JSC STC "Modul"'], <https://module.ru/company>, accessed 12 October 2025.
47. « АО «Московский завод полиметаллов» » ['JSC "Moscow Polymetal Factory"'], <https://mzp.tvel.ru/>, accessed 12 October 2025.
48. « ПАО «Электроприбор» » ['PJSC "Electropribor"'], <https://www.elektmb.ru/>, accessed 12 October 2025.
49. « АО «ЭЛАРА» » ['JSC "Elara"'], <https://www.elara.ru>, accessed 12 October 2025.
50. «АО « ТЕСТПРИБОР" [JSC "Testpribor"'], <https://test-expert.ru>, accessed 11 November 2025; « ОАО «Донский завод радиодеталей» » [PJSC "Don Factory of Radio Components"'], <https://alunddzrd.ru>, accessed 11 November 2025.
51. « АО «Московский завод полиметаллов» » [JSC "Moscow Polymetal Factory"'].
52. « ПАО завод «Красное знамя» » ['PJSC "Krasnoe Znamya Plant"'], <https://www.kznamya.ru/>, accessed 12 October 2025.
53. According to 2024/25 financial data reviewed by the authors.
54. « АО «Плутон» » ['JSC "Pluton"'], « Магазин » ['Shop'], <https://aopluton.ru/shop/>, accessed 12 October 2025.
55. « АО «Салют» » ['JSC "Salyut"'], <https://www.ao-salut.ru/>, accessed 12 October 2025.
56. « АО «Марийский машиностроительный завод» » ['JSC "Mariskiy Machine-Building Factory"'] <https://marimmz.ru/>, accessed 12 October 2025.
57. « ПАО «Сатурн» » ['PJSC "Saturn"'], <https://saturn-omsk.ru>, accessed 11 November 2025.
58. « АО «Опытно-конструкторское бюро микроэлектроники» » ['JSC "Experimental Design Bureau of Microelectronics"'], « О нас » ['About Us'], <https://okbmel.ru/about/>, accessed 12 October 2025.
59. « АО НТЦ «Модуль» » ['JSC STC "Modul"'], <https://module.ru>, accessed 12 October 2025.

Saturn JSC is one of the largest suppliers to Krasnoye Znamya, having sold $172 million of product in 2024 and itself receiving components from Pluton and Modul,[60] high frequency diodes from JSC Optron, located in Moscow;[61] microelectronic components from Tomsk-based Mikran;[62] and Zavod Iskra in Ulyanovsk (Figure 5).[63]

If Saturn JSC is significant by market value, entities such as JSC Scientific and Production Enterprise ISTOK Named After A I Shokin (hereafter JSC ISTOK)[64] – selling $39 million of complex microwave components, according to 2024 financial records, to the S-400 production process – are important for the research and development they carry out on behalf of Krasnoye Znamya, MMZ Avangard and, ultimately, Almaz Antey.[65] Beneath all of these enterprises are also wholesalers of microelectronics, foremost among which is JSC Spetselectroncomplex of Moscow.[66]

Short-Ranged Air Defence

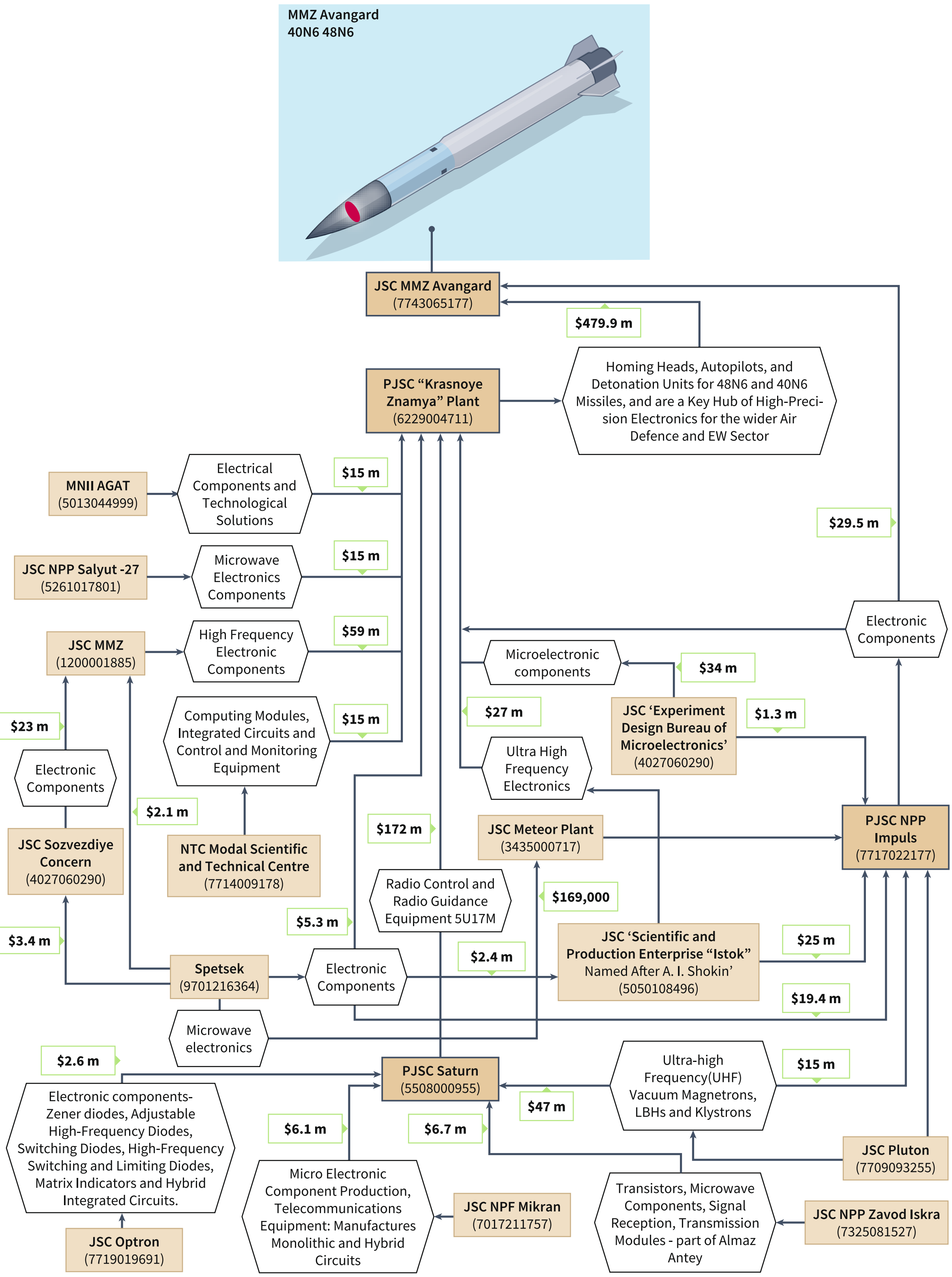
Whereas strategic SAM systems comprise multiple radar, command vehicles and missile types, SHORAD systems integrate all functions onto individual platforms. The production of these systems therefore deserves examination, as it is a distinct supply chain that determines the ability to provide layered protection to more capable systems. The most widespread SHORAD system used by Russia today is the Pantsir, produced by the KBP in Tula, which oversees the programming and assembly of the system (Figure 6). Assembly is also conducted at a nearby subsidiary of KBP, PJSC Shcheglovsky Val.[67]

The Pantsir uses two radars: the 2RL80 search radar and the 1RS2-1 missile guidance radar. The search radar is produced by the JSC Central Design Bureau of Automation (TsKBA) in Tula, which sold $744 million in products to KBP in 2024.[68] TsKBA draws on several companies for sub-components, including:

- Moscow-based NPO PKRV,[69] which supplies the central processing unit 1VS1 and mathematical software for missile guidance.

60. According to 2024/25 financial data reviewed by the authors.
61. « АО «Оптрон» » ['JSC "Optron"'], « Акционерам» ['For Shareholders'], <https://www.optron.ru/about/shareholder/>, accessed 12 October 2025.
62. « АО НПФ «Микран» » ['JSC NPF "Mikran"'], <https://www.micran.ru>, accessed 12 October 2025.
63. « АО НПП «Завод Искра» » ['JSC NPO "Zavod Iskra"'], <https://zavod-iskra.ru>, accessed 12 October 2025.
64. « Продукция НПП « Исток» » ['NPO "Istok" Products'], « АО "НПП «Исток» имени Шокина» » ['JSC NPO "Istok", Named After Shokin'], <https://istokmw.ru/products/>, accessed 12 October 2025.
65. According to 2024/25 financial data reviewed by the authors.
66. « АО «Спецэлектронкомплект» » ['JSC "Spetselectroncomplex"'], <https://www.s-ekomplekt.ru/>, accessed 12 October 2025.
67. « АО «Щегловский вал» » ['JSC "Shcheglovsky Val"'], <https://ros-bm.ru/factories/factory-167/>, accessed 12 October 2025.
68. According to 2024/25 financial data reviewed by the authors.
69. « НПО ПКРВ » ['NPO PKRV'], <https://npo-pkrv.ru/>, accessed 12 October 2025.

Figure 5: The Missile Homing Head Supply Chain



Source: The Authors and Alex Whitworth; sales figures from 2024 financial records seen by the authors.

- Rezonans, which supplies phased array antennas, emitters and phase shifters.[70]
- LLC Zavod RUSNIT, which supplies phased arrays, emitters, beam control modules, impulse modulators and heat exchangers.[71]
- Radis Ltd, which supplies amplifier modules and reference frequency synthesisers.[72]
- NPP ISTOK, which supplies synthesisers and five channel radio receivers.[73]

The engagement radar is produced in-house by KBP, where the same companies appear across the supply chain.

The Pantsir also uses the 10ES1 Guidance Module, incorporating a 1TPP1 electro-optical sensor and the 1PN80 Sagem Infrared Sensor, assembled by NPO GIPO in Kazan.[74] NPO GIPO assembled $108 million of product delivered to KBP in 2024.[75] NPO GIPO's main suppliers include the Optika Grupp,[76] JSC RTKT,[77] JSC Germanii,[78] MTG LLC[79] and NAO NPTS SPS.[80] Historically, NPO GIPO has relied on French electro-optical sensors and there are indications that it still uses stockpiled components that were obtained before 2022.

The Pantsir uses several classes of missile - the most common are the 57-E6 and the TKB-1055. Currently, the latter is the highest priority for Russian industry, being cheaper and better suited to engaging UAVs, although the Russians are exploring a third missile that is supposedly easier to produce. The TKB-1055 is produced by KBP in Tula; TulaTochMash is the main subcontractor,[81] with $333 million of product supplied to KBP in 2024.[82]

The TKB-1055, as with all air defence interceptors, still requires a motor, casing, flight controls, navigation modules, communications link, seeker and warhead. Elements of these systems are provided to TulaTochMash by JSC Rybinsk Instrument-Making

70. « ООО «Резонанс» » ['"Rezonans" LLC'], <https://antennas.spb.ru/>, accessed 12 October 2025.
71. « ООО «Завод Руснит» » ['"Zavod Rusnit" LLC'], <https://zavodrusnit.ru/>, accessed 12 October 2025.
72. « Радис Лтд » ['Radis Ltd'], <https://www.radis.ru>, accessed 12 October 2025.
73. « АО НПП «Исток» имени Шокина» » ['JSC NPO "Istok", Named After Shokin'], « Продукция НПП «Исток» » ['NPO "Istok" Products'], <https://istokmw.ru/products/>, accessed 12 October 2025.
74. « АО «НПО ГИПО» » ['JSC "NPO GIPO"'], <https://www.rusprofile.ru/id/4829223>, accessed 11 November 2025.
75. According to 2024/25 financial data reviewed by the authors.
76. « ООО ОЦ «Оптика» С-3» » ['Industry Centre "Optika" S-3 LLC'], <https://www.rusprofile.ru/id/1237800063302>, accessed 11 November 2025.
77. « АО Радиотехкомплект » ['JSC Radiotekhkomplekt'], <https://www.rtkt.ru>, accessed 12 October 2025.
78. « АО Германий » ['JSC Germanii'], <https://www.krasgermanium.com/>, accessed 12 October 2025.
79. « ООО МТГ » [MTG LLC], <https://mtg.group>, accessed 11 November 2025.
80. « НАО НЦП «Специализированные приборы и системы» » ['NJSC NPTS "Specialised Devices and Systems"'], <https://sps.moscow/>, accessed 12 October 2025.
81. « АО Тулаточмаш » ['JSC TulaTochMash'], <https://tulatochmash.ru/>, accessed 12 October 2025.
82. According to 2024/25 financial data reviewed by the authors.

Plant,[83] NPO PKRV,[84] Zavod Komponent,[85] DPO Plastik and PJSC Elektropribor.[86] Pantsir's 30mm cannon are produced by TulaMashZavod, with $169 million worth supplied to KBP in 2024,[87] although the Russians appear to be moving away from cannon-based solutions for SHORAD.

Other critical elements of the Pantsir include its communications, processing and power units. These include the 12Sh6 communications system, with subsystems including the ShS2 Identification Friend-or-Foe (IFF) system, the ShS10 Fibre Optic Communications System and the ShS50 Radio Modem. The Pantsir also uses the 1NA1 navigation module, the 1VS1 (NPO PKRV) Central Processing Unit and the 2E62 Power Module. The primary supplier for the communications systems is JSC Sozvezdiye Concern, based in Voronezh, which supplied $139 million of product to KBP in 2024.[88] Sozvezdiye Concern is supplied by JSC Elektrosignal,[89] JSC TZ Oktyabr, JSC Almaz, JSC Ryazanskiy Radiozavod[90] and Vnii Signal,[91] among others.

Translating the outputs of the processing unit into the alignment of the combat module requires a complex array of servos and gyroscopic motors. For Pantsir, these are supplied by Serpukhovsky Plant Metallist[92] in Serpukhov in Moscow Oblast, which supplied KBP with $252 million of product in 2024.[93] The plant's suppliers include MZ Saphir, NPP SER LLC, NPO Orion, NPP ISTOK and KB Zvezda LLC,[94] among others. Generally, Pantsir is mounted on Kamaz trucks, but the system is in fact a module that can be dismounted from the vehicle or affixed to other platforms, such that the chassis should not really be considered part of the Pantsir.

83. « АО «Рыбинский завод приборостроения» » ['JSC "Rybinsk Instrument Making Plant"'], <https://rzp.su>, accessed 12 October 2025.
84. « НПО ПКРВ » ['NPO PKRV'], <https://npo-pkrv.ru/>, accessed 12 October 2025.
85. « АО Завод «Компонент» » ['JSC Zavod "Komponent"'], <https://zavodkomponent.ru/>, accessed 12 October 2025.
86. «ПАО Тамбовский завод «Электроприбор» [PJSC "Electropribor"'], <https://elektmb.ru/>, accessed 12 October 2025.
87. According to 2024/25 financial data reviewed by the authors.
88. According to 2024/25 financial data reviewed by the authors.
89. « АО Электросигнал » ['JSC Electrosignal'], <https://elektrosignal.ru/>, accessed 12 October 2025.
90. « АО «Рязанский Радиозавод» » ['JSC "Ryazanskiy Radiozavod"'], <https://radiozavod.ru/>, accessed 12 October 2025.
91. « АО ВНИИ «Сигнал» » ['JSC VNII "Signal"'], <https://www.vniisignal.ru/>, accessed 12 October 2025.
92. « АО Серпуховский завод «Металлист» » ['JSC Serpuhovsky Factory "Metallist"'], <https://www.szmetallist.ru/>, accessed 12 October 2025.
93. According to 2024/25 financial data reviewed by the authors.
94. « ФГУП Электромеханический завод «Звезда» » ['KB "Zvezda" Electromechanical Factory'], <https://www.zvezdasp.ru>, accessed 12 October 2025.

Radar and Command and Control

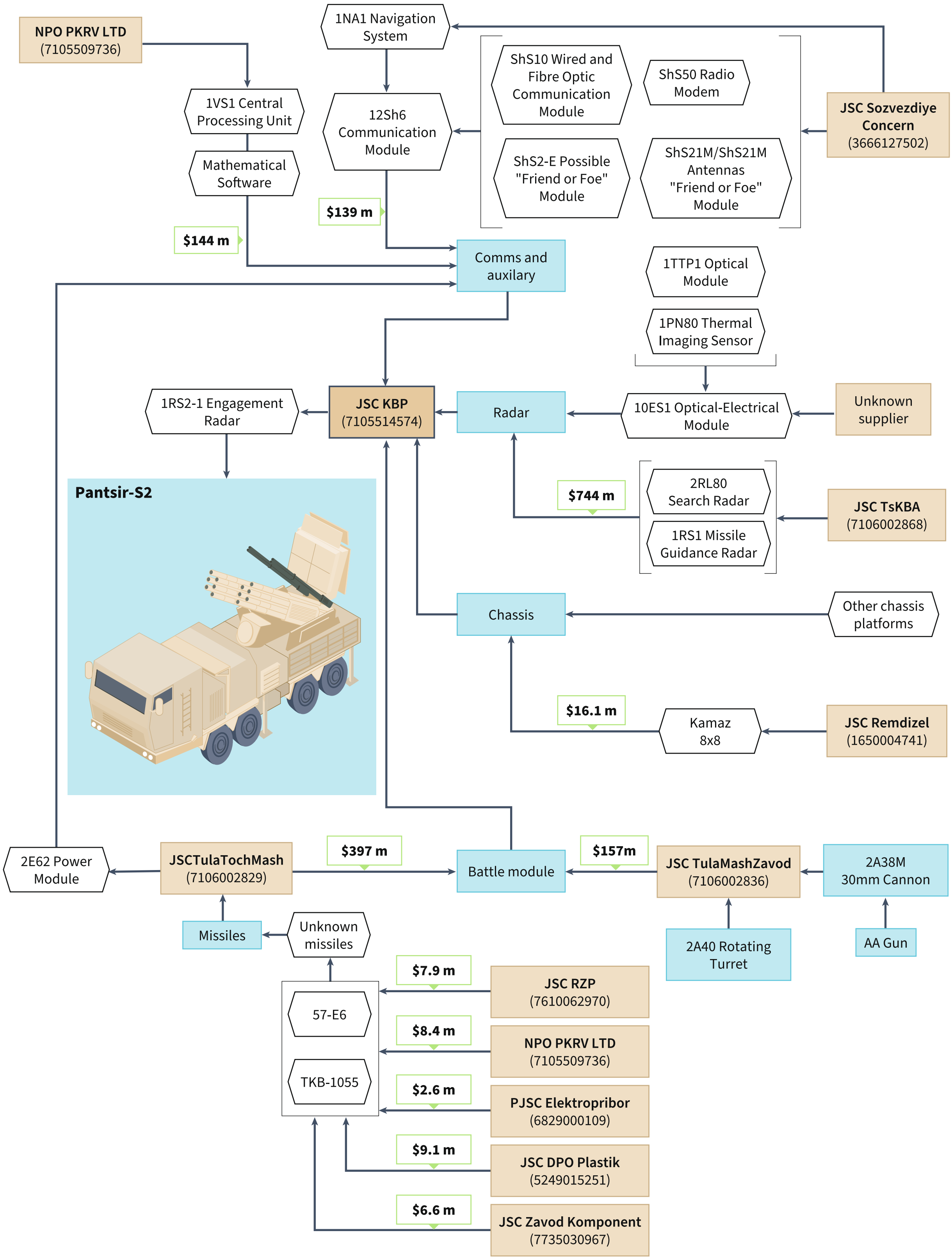
Whereas missile production is subcontracted to MMZ Avangard, Almaz Antey retains a much closer relationship with its radar producers. The most important radar in the S-400 complex is arguably the 92N6 Gravestone radar (Figure 7), which is developed by PJSC NPO Almaz,[95] a unit within Almaz Antey, headquartered in Moscow. Along with research and development within Almaz Antey's Experimental Production Division, NPO Almaz oversees the assembly of the different functional modules for the radar at its affiliates JSC Nizhegorodskiy Zavod 70-Letiya Pobedy (NZ 70-Letiya Pobedy),[96] JSC Obukhovskiy Plant[97] and JSC Mariyskiy Machine-Building Plant.[98] NPO Almaz also produces the 96L6 Cheese Board radar, critical for both the S-400 and S-500 systems.

According to financial data for 2024–25, NPO Almaz delivered some $675 million of systems to Almaz Antey in 2024.[99] Although much of the assembly is carried out in-house, there are still complex subsystems supplied to NPO Almaz. These include the Tuf-M Communications Suite, produced by Kontsern Sozvezdiye in Voronezh[100] and the 40V6M Universal Mast, to which radar systems are affixed, produced by Tyazhmash.[101]

The 91N6 Bigbird Radar, used in both the S-400 and S-500 complexes, is produced by JSC NPO NIIP NZIK in Novosibirsk.[102] Among its critical suppliers is JSC NPP Toriy in Moscow, which produces klystrons,[103] the vacuum tubes critical to generating radio-waves. NZIK also procures microwave components from JSC Svetlana-Elektronpribor,[104] Gallium Arsenide-based amplifiers from CJSC NPP Planeta Argall,[105] resistors from JSC Almaz, semiconductor components from VZPP-S,[106] and pin diodes from Optron.

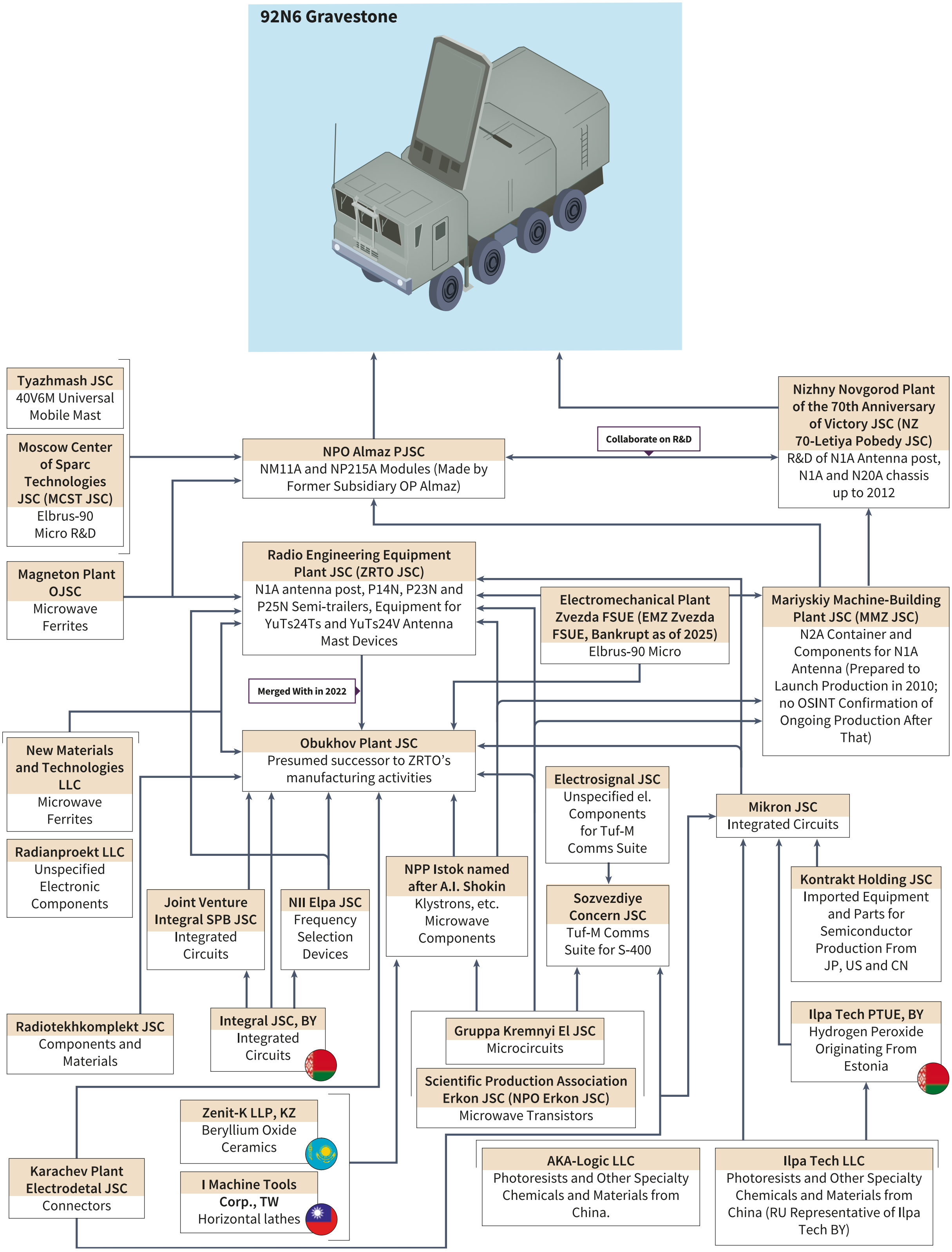
95. « ПАО Научно-производственное объединение «Алмаз» имени академика А А Расплетина» » ['PJSC NPO "Almaz"'], <https://www.raspletin.com/>, accessed 12 October 2025.
96. « АО Нижегородский завод 70-летия Победы » ['JSC Nizhny Novgorod Factory of the 70th Anniversary of Victory'], <https://www.nzslp.ru/>, accessed 12 October 2025.
97. « АО Научно-производственное объединение Северо-Западный региональный центр Концерна ВКО «Алмаз-Антей – Обуховский завод» » ['JSC Research and Production Association North-West Regional Centre of the "Almaz-Antey Air and Space Defence Concern – Obukhovskiy Plant"'], <https://www.goz.ru>, accessed 12 October 2025.
98. « АО Марийский машиностроительный завод » ['JSC Mariyskiy Machine-Building Plant'], <https://www.marimmz.ru/>, accessed 12 October 2025.
99. According to 2024/25 financial data reviewed by the authors.
100. « АО Концерн «Созвездие» » ['JSC Kontsern "Sozvezdiye"'], <https://ros-bm.ru/factories/factory-20/>, accessed 12 October 2025.
101. « Тяжмаш » ['Tyazhmash'], <https://tyazhmash.com/>, accessed 12 October 2025.
102. « Научно-исследовательский институт измерительных приборов – Новосибирский завод имени Коминтерна » ['JSC Scientific and Research Institute of Measurement Instrumentation – Komintern Novosibirsk Plant'], <https://www.нииип-нзик.рф/>, accessed 12 October 2025.
103. « АО "НПП «Торий» » ['JSC NPP "Toriy"'], <https://www.toriy.ru>, accessed 12 October 2025.
104. « АО «Светлана-Электроприбор» » ['JSC "Svetlana-Elektronpribor"'], <https://www.svetlana-ep.ru>, accessed 12 October 2025.
105. « ЗАО «НПП «Планета-Аргалл» » ['CJSC NPP "Planeta-Argall"'], <https://argall.nov.ru>, accessed 12 October 2025.
106. « АО «ВЗПП-С» » ['JSC "VZPP-S"'], <https://www.vzpp-s.ru/>, accessed 12 October 2025.

Figure 6: The Pantsir Supply Chain



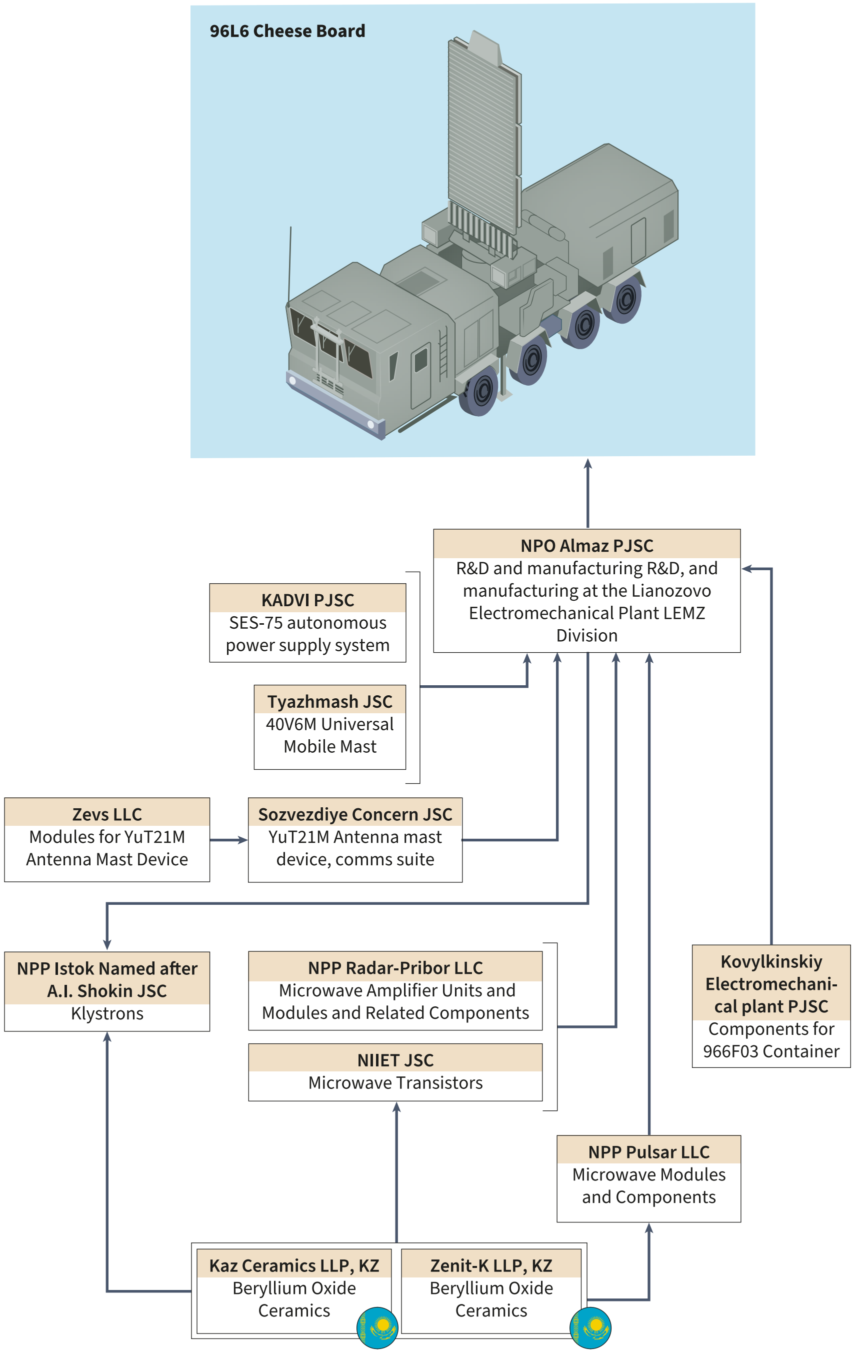
Source: The authors and Alex Whitworth; financial data based on records for 2024, seen by the authors.

Figure 7: The 92N6 Gravestone Supply Chain



Source: The authors and Alex Whitworth; amounts based on financial records for 2024/25 seen by the authors.

Figure 8: The 96L6 Supply Chain



Source: The authors and Alex Whitworth; amounts based on financial records for 2024/5 seen by the authors.

Optron not only supplies Saturn with components to produce homing heads and NIIIP-NZIK with components for radars but also appears in the supply chains for 1L119 Nebo-SVU and 55Zh6M Nebo-M radars. The NEBO-M multi-functional radar is produced by JSC FNPTs NNIIRT and NZ 70-Letiya Pobedy. The 1L119 Nebo-SVU is manufactured in

Ulyanovsk at the Ulyanovsk Mechanical Plant. The 48Ya6-k1 Podlet, meanwhile, is produced by JSC VNIIRT,[107] based in Moscow.

The fusion and coordination of the S-400 complex is carried out on the 55K6E C2 Vehicle, while the integration of the system with the wider IADS is carried out in the Polyana-D4M1. The 55K6E is designed and assembled by NPO Almaz. Subsystems include the Ramek Computing Module, supplied by Ramek-VS JSC[108] of St Petersburg, and Elbrus Processors, supplied by JSC MTsST in Moscow. Further microelectronics are supplied by the JSC Kremniy El Group.[109] The Polyana-D4M1 is produced by JSC Radiozavod,[110] with its main production site in Penza.

Unsurprisingly, there is significant overlap with NPO Almaz's suppliers of subsystems, since the system must be integrated. Thus, the communications suites are produced by JSC Kontsern Sozvezdiye. The system also draws on computing modules such as the Baget, produced by JSC Design Bureau Korund-M in Moscow.[111] Just as the consumer electronics of the missile enterprise of MMZ Avangard used a wholesaler – JSC Spetselektronkomplekt – to source non-Russian parts, the C2 enterprise of the S-400 complex draws heavily on JSC Elektroavtomatika to acquire components from Taiwan, South Korea and the wider West through China.[112]

107. « АО «Вниирт» » ['JSC "VNIIRT"'], 18 July 2017, <https://www.rusprofile.ru/id/3417308>, accessed 12 October 2025.
108. « РАМЭК » ['Ramec'], <https://www.ramec.ru/>, accessed 12 October 2025.
109. « АО Группа Кремний Эл » ['JSC Kremniy Group El'], <https://www.group-kremny.ru/>, accessed 12 October 2025.
110. « АО Пенза-Радиозавод » ['JSC Penza-Radiozavod'], <https://www.penza-radiozavod.ru/, accessed 12 October 2025.
111. « АО Конструкторское бюро «Корунд-М» » ['JSC Design Bureau "Korund-M"'], <https://www.korund-m.ru/>, accessed 12 October 2025.
112. According to 2025 trade data reviewed by the authors.

Vulnerability of Russia's Air Defence Production

Although the first and second tiers of Russian air defence production (at first glance) appear to be sovereign and founded on a robust research and industrial base, the industry also faces significant dependencies on foreign supply of raw materials, components and machine tools. Each of these dependencies are also exposed to sanctions, have economic weaknesses, or are vulnerable to direct attack. The authors have carried out a comprehensive vulnerability assessment, and this chapter highlights some – though by no means all - prominent examples that can be capitalised on.

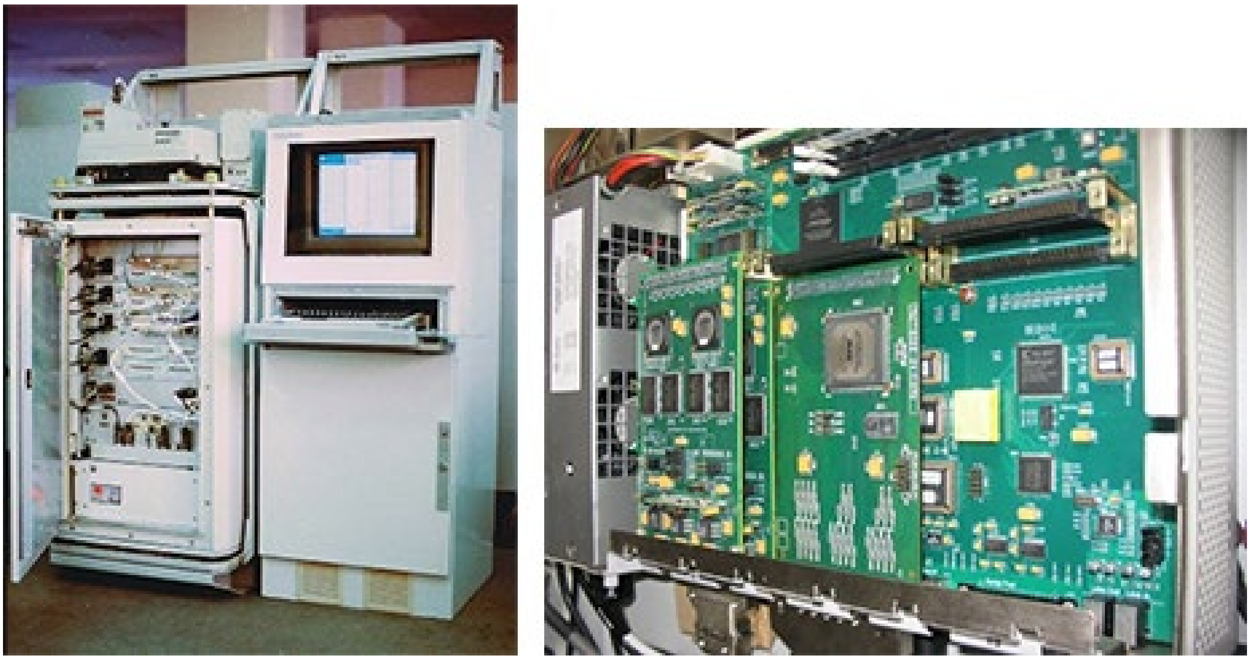
Exposure to Supply Chain Disruption

Russian air defences use a wide range of foreign-sourced microelectronics that Russia has struggled to produce domestically, and this exposes Russia to systemic risks of supply chain disruption for critical subcomponents. Russia's S-400 systems, from the 55K6 C2 Centre, to the 92N6 Gravestone Radar Complex, use Russia's Elbrus-90micro computing system,[113] which handles data processing and target tracking (Figure 9).[114] Since 2022, both the developer and the manufacturer of the system have experienced, and continue to face, obstacles related to its production.

The system was designed by the Moscow Centre of SPARC Technologies (MCST) around the SPARC architecture in 1998,[115] and uses domestically developed MCST-R

113. Carlo Kopp, 'Almaz-Antey 40R6 / S-400 Triumf Technical Report', *Air Power Australia*, May 2009, <https://www.ausairpower.net/APA-S-400-Triumf.html>, accessed 12 October 2025; I Ashurbeyli et al., « Глава Первая. Технологии противовоздушной обороны » ['Chapter 1. Air-Defence Technologies'], in V Minayeva et al. (eds), *Диалектика технологий воздушно-космической обороны* [*The Dialectics of Aerospace Defence Technologies*] (Moscow: CJSC Izdatelskiy Dom Stolichnaya Entsiklopediya, 2011), p. 40.
114. Dmitry Sudakov, 'Russia's S-400 Air Defence Systems for NATO Armies', *Pravda.ru*, 25 September 2017, archived via the Wayback Machine 27 October 2018, <https://web.archive.org/web/20181027225122/http://www.pravdareport.com/world/asia/turkey/25-09-2017/138745-s_400_air_defence-0/>.
115. Ashurbeyli et al., « Глава Первая. Технологии противовоздушной обороны », 'Chapter 1. Air-Defence Technologies', p. 63.

Figure 9: Elbrus-90micro Computing System



Source: FSUE EMZ Zvezda, « Вычислительный комплекс «Эльбрус» » ['"Elbrus" Computing Complex'], archived via the Wayback Machine, 27 March 2022, <https://web.archive.org/web/20220327033206/http:/zvezdasp.ru/products/vychislitelnyy-kompleks-elbrus>, accessed 12 October 2025.

microprocessors. According to MCST in 2013, these microprocessors are said to be manufactured at Taiwan's TSMC until domestic production capacity is established.[116]

Since then, however, there have been no open sources confirming that MCST has successfully moved production to Russia. The latest generation microprocessor of the MCST-R series, MCST-R2000, which was developed in 2018 under a Russian Ministry of Defence contract,[117] required 28 nanometer (nm) process technology. The most advanced microprocessors that Russia can produce are 90 nm at Zelenograd's Mikron, making the presumed manufacturer of these microprocessors TSMC. The domestic production of its predecessor, MCST-1000,[118] seems technically possible, as it requires

116. Alexander Kim et al., « ГЛАВА 1. Общая характеристика семейства «Эльбрус» » ['Chapter 1. General Characteristics of the "Elbrus" Family'], in *Микропроцессоры и вычислитеные комплексы семейства «Эльбрус»* [*"Elbrus" Family Microprocessors and Computing Systems*] (St Petersburg: Piter, 2013), p. 18, <https://www.mcst.ru/doc/book_121130.pdf>, accessed 12 October 2025.
117. Serial production was reportedly to be launched in 2019. See « Показан новый российский 8-ядерный 28-нм процессор МЦСТ R-2000 » ['New Russian 8-Core 28nm MCST R-2000 Processor Demonstrated'], *Техносфера,* 17 April 2018, archived via the Wayback Machine, 22 February 2019, <https://web.archive.org/web/20190222082614/https://tehnoomsk.ru/node/3148>, accessed 11 November 2025; Denis Voyeikov, « Создатели «Эльбрусов» выпускают процессор альтернативной архитектуры впервые за семь лет» » ['Elbrus Developers Release Alternative Architecture Processor for the First Time in Seven Years'], *CNews,* 27 April 2018, <https://www.cnews.ru/news/top/2018-04-27_razrabotchiki_elbrusov_vpervye_za_sem_let>, accessed 12 October 2025.
118. In serial production as of 2012. See Kim et al., «ГЛАВА 1. Общая характеристика семейства «Эльбрус» » ['Chapter 1. General Characteristics of the "Elbrus" Family'], p. 19.

90 nm fabrication. However, available financial records for MCST and Mikron from 2024 and 2025 reveal that the two companies have no business relationship.[119]

Following the full-scale invasion of Ukraine in 2022, TSMC reportedly terminated its agreement with the Russian developer due to the sanctions risk. MCST then announced that it was to move production to JSC Mikron in Zelenograd. In October 2024, the head of the Russian Academy of Sciences, Gennady Krasnikov, stated that Mikron had already started manufacturing another Elbrus microprocessor using the same process as for the fabrication of MCST-R1000.[120]

However, there have been several indications casting doubt on how successful MCST has been in establishing domestic production following sanctions. As noted above, MCST appears to have no buyer–supplier relationship with Mikron, and despite Krasnikov's claim, media articles from the same month have argued that there was no indication that such production had started at Mikron.[121] Furthermore, in September 2024, the Russian Ministry of Trade and Industry transferred management of the company under NPC Elvis, which sources of the *Vedomosti* newspaper claim was due to MCST failing to fulfil a state defence order.[122] A source close to *Kommersant* stated that, as a result of this challenge, MCST was facing bankruptcy by law and that fellow microprocessor developer NPC Elvis was tasked with ensuring the former's 100% fulfilment of the state defence order. To comply with its defence contracts, according to

119. Furthermore, multiple Russian media outlets since 2022 have implied that, at the time, Mikron had not started manufacturing Elbrus microprocessors using 90 nm process technology. Alexander Kim, the head of MCST's close business partner INEUM, stated that Mikron had only manufactured Elbrus microprocessors at pilot scale. See « Российский микропроцессор Эльбрус 8C » ['Russian Elbrus 8C Microprocessor'], *Хабр*, 23 January 2022, <https://habr.com/ru/articles/647277/U>, accessed 12 October 2025; *Дзен*, « Почему выпущенные по техпроцессу 90 нм в России миркопроцессоры Эльбрус имеют частоту ниже, чем такие же Итаниумы » ['Why Do the Elbrus Microprocessors Produced Using the 90 nm Process in Russia Have a Lower Frequency than the Same Itaniums'], 16 June 2022, <https://dzen.ru/a/YqnKUlTln3-rPknT>, accessed 11 November 2025; *Ростех,* « Александр Ким: Наши процессоры защищены от атак на уровне кремния » ['Aleksandr Kim: Our Processors are Protected Against Attacks on the Silicon Level'], 21 July 2025, <https://rostec.ru/media/news/aleksandr-kim-nashi-protsessory-zashchishcheny-ot-atak-na-urovne-kremniya/#start>, accessed 12 October 2025.
120. Anna Urmantseva, « Новая жесткая РАН. Академия не приняла отчеты об исследованиях на 2,5 млрд рублей » ['A New, Tough RAS. The Academy Rejected Research Reports Worth 2.5 Billion Rubles'], *Gazeta.ru*, 30 September 2024, <https://www.gazeta.ru/science/2024/09/30/19814251.shtml> accessed 12 October 2025.
121. *Монокль*, « «Эльбрус» в тумане неизвестности » ['"Elbrus" in the Fog of Uncertainty'], 14 October 2024, <https://monocle.ru/monocle/2024/42/elbrus-v-tumane-neizvestnosti/>, accessed 12 October 2025.
122. MCST was reportedly subject to a ₽3 million arbitration proceeding filed by the Russian Ministry of Defence in May 2023 for a contract delay, either due to terms of delivery of products or R&D work. See Sofia Pletneva, « Разработчика процессоров «Эльбрус» передали во внешнее управление » ['Processor Developer "Elbrus" Transferred to External Management'], *Forbes.ru*, 30 September 2024, <https://www.forbes.ru/tekhnologii/522243-razrabotcika-processorov-el-brus-peredali-vo-vnesnee-upravlenie>, accessed 12 October 2025.

Kommersant's source, MCST had to redesign its microprocessors, but the state was not willing to fund the project.[123]

Currently, MCST may still be engaging in small-scale production of microprocessors for Elbrus-90micro, either at Mikron or through complex supply chains of technical intermediaries in different countries.[124] MCST's financial records indicate that currently, the largest supplier is NPC Elvis – which, according to a *Kommersant* source, has 'somehow' continued to manufacture advanced microprocessors, despite sanctions.[125] In 2025, MCST co-founder Boris Babayan and his son announced that by 2027 they plan to develop separately from MCST a new Elbrus-B Microprocessor for high-power computing and had entered a $2-billion contract with Indian partners.[126] Russian intermediaries have also approached prominent Taiwanese businessmen, including Foxconn's Terry Gou, with proposals to establish a production facility for Elbrus in India. It is not clear if these advances were met with a favourable response.[127]

The most recent sources point to FSUE Electromechanical Plant Zvezda (hereafter EMZ Zvezda) as the main serial manufacturer of Elbrus-90micro. Financial records link the entity to nearly all major manufacturers in the S-400 ecosystem – NPO Almaz, Mariyskiy Machine-Building Plant, Obukhovskiy Zavod, NZ 70-Letiya Pobedy and Almaz-Antey itself.[128] Historically, EMZ Zvezda has been a key developer of computing complexes for Russian air defence systems. It was a co-developer and main manufacturer of the VK 5E26, created in 1969 for the S-300, and of its successor TsVK 40U6 for the S-300P. It subsequently undertook the production of supercomputers from the Elbrus family.[129]

123. *MashNews,* « АРПЭ просит проверить передачу разработчика процессора «Эльбрус» МЦСТ прямому конкуренту – НПЦ » ['ARPE Requests to Check the Transfer of Processor Developer "Elbrus" to a Direct Competitor – NPC Elvis'], 9 October 2024, <https://mashnews.ru/arpe-prosit-proverit-peredachu-razrabotchika-proczessora-elbrus-mczst-pryamomu-konkurentu-npcz-elvis.html>, accessed 12 October 2025.
124. A strategy allegedly used by some Russian microelectronics manufacturers, according to the head of the Russian Association of Electronics Manufacturers. See Aleksandr Ivanter, « Из колеи ARM в созвездие «Эльбруса» » ['From the ARM Track to the "Elbrus" Constellation'], *Монокль*, 8 July 2024, <https://monocle.ru/monocle/2024/28/iz-kolei-arm-v-sozvezdiye-elbrusa/>, accessed 12 October 2025.
125. Timofey Kornev, « К «Эльбрусу» подошли с вопросом » ['Questions are Posed about "Elbrus"'], *Коммерсантъ*, 9 October 2024, archived via Archive.today, 16 October 2024, <https://archive.fo/b51Wi#selection-1845.0-1891.559>, accessed 12 October 2025.
126. Christina Holupova, « Сооснователь МЦСТ пообещал через два года выпустить процессор на новой архитектуре, превосходящий иностранные аналоги «в 30-200 раз» » [MCST Cofounder Promised to Release a Processor in Two Years Based on New Architecture that will Outperform Foreign Analogues "by 30-200 Times"], *CNews*, 12 May 2025, <https://www.cnews.ru/news/top/2025-05-12_osnovatel_mtsst_i_vyhodets>, accessed 24 November 2025.
127. Correspondence seen by the authors.
128. According to 2024 financial data reviewed by the authors.
129. « ФГУП Электромеханический завод «Звезда» » ['FSUE Electromechanical Plant "Zvezda"'], « История завода » ['History of the Plant'], archived via the Wayback Machine, 14 March 2022, <https://web.archive.org/web/20220314075611/http://zvezdasp.ru/about-company/>, accessed 12 October 2025.

According to a brochure from its archived website, as of 2017, the entity was also manufacturing the Elbrus-90micro computing system and related modules.[130]

Despite a revival period from 2006, when the entity became part of a federal programme for the development of the Russian military–industrial complex,[131] EMZ Zvezda reportedly has struggled financially in the past six years and ended up initiating bankruptcy proceedings in March 2025. Its operations were suspended several times prior to that – first as a response to the pandemic, and later as a support measure in an attempt to reorganise the plant and make it more profitable.[132] Nevertheless, financial records indicate that the company remained relatively active in that period: it had 27 transactions worth $423,837, just for the second half of 2022, with the main manufacturer of the Gravestone radar's antenna, the former Radio Equipment Plant (ZRTO).

By the end of 2024, the plant had less than $50,000 in sales for the whole year to ZRTO's successor, Obukhovskiy Zavod, and by April 2025, the plant's entire inventory was appraised and prepared for auction.[133] As of October 2025, the outcome of the bankruptcy proceedings is still undetermined. However, a *MashNews* correspondent has argued that an actual liquidation of the plant is unlikely, given its strategic status, and that EMZ Zvezda may end up being absorbed by Rostec or Rosatom.[134]

The conclusion is that Russia's microelectronics industry is underperforming, still dependent on foreign suppliers for more complex chips, and that disruption to its operations would have a serious impact on the production of some of the most critical components of its air defence systems. Even where Russia does produce its own microelectronics, it is often dependent on imports of critical materials and products, including from the US. Russian language sources clearly show that printed circuit board (PCB) laminates, made by world-leading US company Rogers Corporation, are preferred by Russia's radar engineers for their low-loss, phase-stable, radar-grade radio frequency and microwave performance.

---

130. « ФГУП Электромеханический завод «Звезда» » ['FGUP Electromechanical Plant "Zvezda"'], « Производство корпусны изделий. Технический каталог 2017 » ['Cabinet Manufacturing. Technical Catalogue 2017'], archived via the Wayback Machine, 23 April 2023, <https://web.archive.org/web/20230423062511/http://zvezdasp.ru/upload/files/tech_catalog_2017.pdf>, accessed 12 October 2025.
131. « ЭМЗ «Звезда» наращивает мощности» » ['EMZ "Zvezda" Increases Capacity'], *Агентство новостей Подмосковья*, <http://www.mosoblpress.ru/mass_media/3/130/item117462/>, accessed 12 October 2025.
132. Evgeniy Belitskiy, « В Подмосковье обанкротился принадлежащий Минпромторгу РФ стратегический завод » ['A Strategic Plant Owned by the Ministry of Industry and Trade of the Russian Federation Went Bankrupt in the Moscow Suburbs'], *MashNews*, 21 April 2025, <https://mashnews.ru/v-podmoskove-obankrotilsya-prinadlezhashhij-minpromtorgu-rf-strategicheskij-zavod.html>, accessed 12 October 2025.
133. « ФГУП ЭМЗ «Звезда» » ['FSUE EMZ "Zvezda"'], *Федресурс*, <https://fedresurs.ru/companies/bb0d8cce-df8c-4dab-b45b-afacb08a5604/publications>, accessed 12 October 2025.
134. Belitskiy, « В Подмосковье обанкротился принадлежащий Минпромторгу РФ стратегический завод » ['A Strategic Plant Owned by the Ministry of Industry and Trade of the Russian Federation Went Bankrupt in the Moscow Suburbs'].

One of the public proofs of the use of Rogers products is a 2023 article from Almaz-Antey's Bulletin (« Вестник Концерна ВКО Алмаз-Антей » – March 2023) on the thermal management of the transmit / receive module (TRM) of AESA radars. The Russians are actively expanding the use of AESA radars as they develop their S-500 system. According to Ukrainian sources,[135] the 96L6E Yenisei radar in the S-500 is an AESA. Oleg Kochetkov, the lead engineer within PAO Radiofizika (Almaz-Antey's radar design unit), noted in an article that the Rogers models used in Russian AESA radars include RO4350B, RO4003C (Figure 10), RO5880 and RO3003. According to data from the manufacturer, Rogers RO3000 and RO4000 series are known for their performance. The resins used expand at a minimum level with temperature rise, thus keeping layer registration precise even when TRMs heat and cool repeatedly. This quality preserves the alignment of the antenna feed networks and microstrip lines, which are critical for phased-array radar modules that need to maintain an identical element phase.

The trade-off, as Kochetkov's article states, is low thermal conductivity. Rogers PCBs are excellent in loss minimisation but give a poor heat flow. Thermal management of the TRM is described as critical because when heat is not removed or transferred equally, local hot spots form and parts of the module become tens of degrees hotter than others, reaching up to 125–130°C. This harms the radar's performance in several ways: some semiconductor parameters vary with temperature, component lifetime reduces and beam direction can shift, reducing accuracy.

A second source – again from a Radiofizika publication[136] – details the proceedings of the 21st All-Russian Youth Scientific–Technical Conference. The paper, signed by two Radiofizika engineers, describes laboratory tests showing how easily gases pass through different PCB dielectric materials, used for high-frequency and microwave circuits in radars. The materials tested were:

- Rogers RO3003 (Chinese analog FSD300GR).
- Rogers RO3010 (Chinese analog FSD1020GR).
- Rogers RO4003 (Chinese analog FSD883T).
- Rogers RO4350 (Chinese analog FSD888T).
- Duroid RT5880 (Chinese analog FSD220G).
- DuPont Pyralux, AD8540R (US).

135. Dylan Malyasov, 'Ukrainian Forces Take Out S-500 Air Defense Radar', *Defence Blog,* 8 August 2025, <https://defence-blog.com/ukrainian-forces-take-out-s-500-air-defense-radar/>, accessed 12 October 2025.
136. Vladislav Zakharkin et al., « Исследование газопроницаемости диэлектрических материалов » ['Study of Gas Permeability of Dielectric Materials'], in *Радиолокация и связь — перспективные технологии. XXI Всероссийская молодежная научно-техническая конференция* [*Radar and Communications – Promising Technologies. XXIst All-Russian Youth Scientific-Technical Conference*] (Moscow: LLC Izdatelstvo Mir Nauki, 2024), p. 59.

Figure 10: Rogers RO4003C, Advertised on a Chinese Website in Russian, Specifically for Radar Application

Source: *Highleap Electronic*, « RO4003C Высокочастотный материал печатных плат для надежных ВЧ и СВЧ применений » [‘RO4003C High-Frequency Printed Circuit Board Material for Rugged RF and Microwave Applications’], <https://hilelectronic.com/ru/ro4003/>, accessed 12 October 2025.

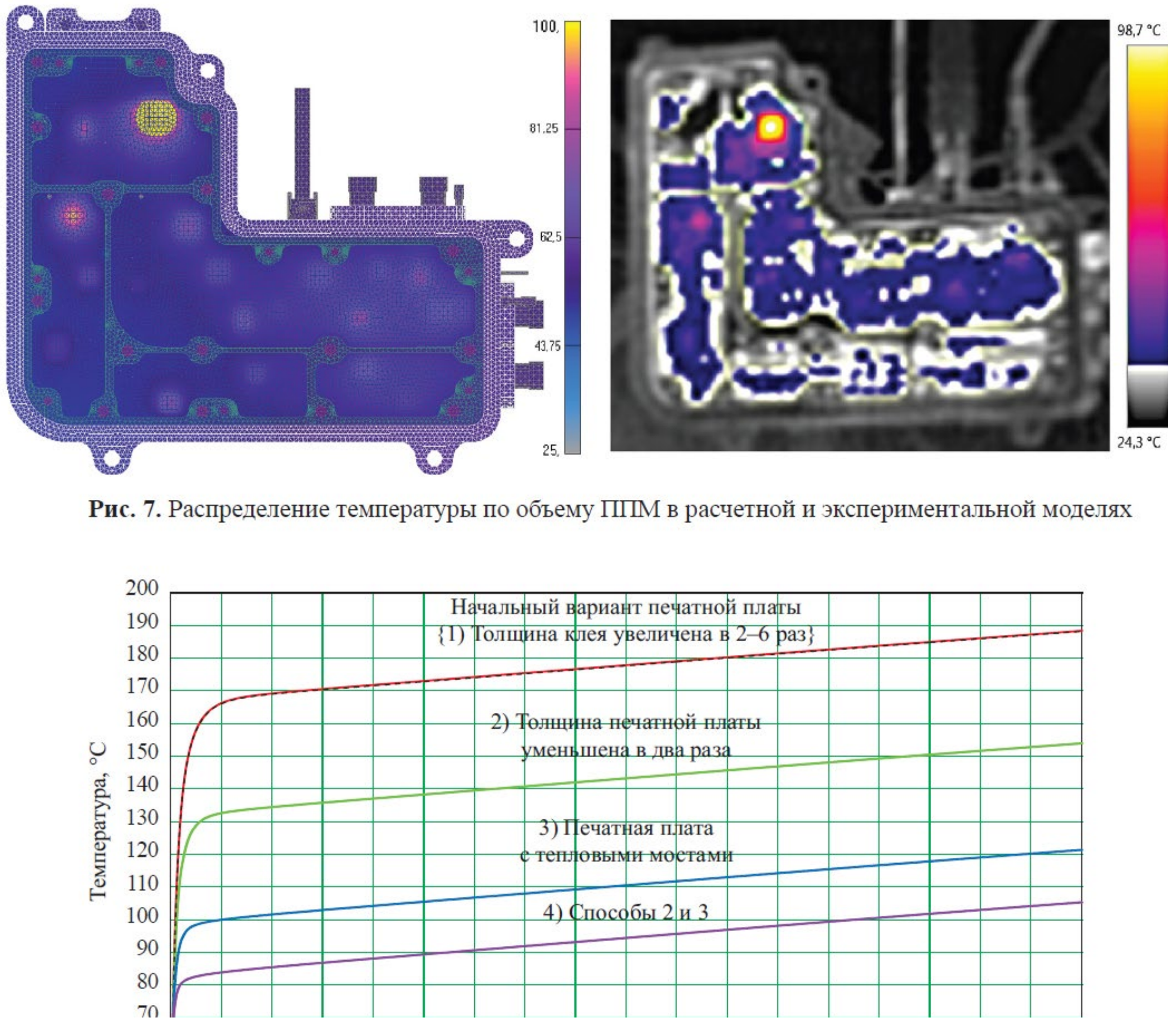
Since 1 January 2024, Russian companies have imported $1.1 million of Rogers PCBs, mostly via China but also via Turkey, India and Lithuania, according to trade records. The biggest importer in 2024, LLC Electrade-M OOO, sold directly to Russia’s biggest military plants. In 2024 alone, trade data indicates that this company has sold goods to some of the major Russian military equipment manufacturers, including radar plants, for $577,088. The list includes NPO Almaz, Obukhovskiy Zavod, Sozvezdiye, Krasnoye Znamya and Kremniy El.

As of October 2025, LLC Electrade-M is only sanctioned by Ukraine. Since the end of 2023, LLC Electrade-M has become an exclusive distributor to Russia for FSD analogue products, allegedly made by XiaMen AFS Electronics & Materials Co. Ltd (China).[137]

Disrupting Russia’s supply of these products could set back the performance of some of their most advanced radar, and thus, air and missile defence systems more generally.

137. XiaMen AFS Electronics & Materials Co.,Ltd., to LLC Electrade-M, ‘Letter Granting Exclusive Distribution Rights’, 28 November 2023, <https://eltm.ru/attach/news/v_401_16.pdf>, accessed 12 October 2025.

Figure 11: Test Results from Different Experiments on How to Lower Heat (Left Axis) in the TRM by Stacking PCBs and Using Thermal Bridges



Source: O Kochetkov et al., « Способы влияния на температурное распределение по объему приемо-передающего модуля » ['Methods for Influencing Temperature Distribution across the Volume of a Transmitter-Receiver Module'], *Bulletin of the Almaz-Antey Air Defence Concern* (No. 3, 2023), p. 85.

Opportunities to Sanction

Beyond disruption, there is also significant dependence on foreign supplies of raw materials; imports of these materials could be denied through economic sanctions. Among these raw materials, beryllium oxide ceramics are commonly used in high-power radiofrequency and microwave electronics for their superior ability to prevent overheating.[138] Insulating products made with this material include heat sink insulator substrates for transistors and diodes, waveguide windows for microwave devices, and high-power microwave absorbers,[139] used in anechoic chambers. These components are all extensively used in the manufacturing of radar systems and any actor seeking to disrupt Russia's air defences could consider targeting these through sanctions.

Russia has no operating plants for the production of beryllium oxide ceramics,[140] and has instead historically relied on a factory based in Ust-Kamenogorsk, eastern Kazakhstan, [141] now known as Kaz Ceramics.[142] The plant was built in the early 1980s as an initiative of the USSR's Ministry of Electronic Industry, and uses beryllium oxide powder as a raw material manufactured by the Ulba Metallurgical Plant to custom specifications. After 1998, the plant was privatised and changed its name, and possibly ownership, at least four times – with the most recent name change dating from 2022.[143] As of that date, the factory had an output of 150 kg of beryllium oxide ceramic products per year.[144]

At the time of writing, Russia has remained Kaz Ceramics' most important customer. In December 2014, a company named Zenit-K[145] was established at the same address as the ceramics factory (Figure 12). The company launched a Russian-language website using the corporate logo of the Kazakh factory and regularly participated in Russian public procurement, winning tenders from the Research Institute of Electronic Equipment (NIIET) and NPP Almaz, both microwave electronics manufacturers.[146] According to commercial trade data, since 2024, both Kaz Ceramics and Zenit-K have regularly exported their products (marked with HS code 85471 for ceramic insulating fittings) to major manufacturers of radar components, including to key Almaz-Antey

138. Chin Trento, 'What Are the Uses of Beryllium Oxide Ceramics?', Stanford Advanced Materials, 24 July 2025, <https://www.samaterials.com/content/what-are-the-uses-of-beryllium-oxide-ceramics.html>, accessed 12 October 2025.
139. « Керамический завод ТОО «Зенит-К» » ['Ceramics Factory TOO "Zenit-K"'], « Каталог » ['Catalogue'], archived via the Wayback Machine, 27 September 2021, <https://web.archive.org/web/20210927080158/http://zenith-k.ru/ru/catalog>, accessed 12 October 2025.
140. Aleksandr Pavlov, « Синтез и исследование свойств бериллиевой керамики, модифицированной наночастицами диоксида титана » ['Synthesis and Study of the Properties of Beryllium Ceramics Modified with Titanium Dioxide Nanoparticles'], PhD dissertation, Siberian Federal University, 2023.
141. G Akishin et al., « Производство BeO-керамики в СССР и его возрождение в современной России » ['Production of BeO-Ceramics in the USSR and Its Revival in Modern Russia'], *Novye Ogneupory* (No. 5, 2019), pp. 12732.
142. « ТОО «KAZ CERAMICS» », <https://kazceramics.kz/>, accessed 11 November 2025.
143. Previously, the entity also had the names LLC Proizvodstvennaya Firma Best, LLC KazMetizProm, LLC Altreyd and JSC Keramika. See « ТОО Производственная фирма «BEST»: техника безопасности. Тест тренировочный с ответами (Казахстан, 2022 год) » ['LLC Manufacturing Company "BEST": Safety. Practice Test with Answers (Kazakhstan, 2022)'], *Sinref.ru*, <https://www.sinref.ru/000_uchebniki/04600_raznie_13/944_ohrana_truda_zavodi_Kazahstana_2022_otvet_ianvar/371.htm>, accessed 12 October 2025.
144. State Institution, 'Office of the Akim of the City of Ust-Kamenogorsk', « Протокол общественных слушаний' » ['Minutes of the Public Hearings'], 12 December 2022, <https://ecoportal.kz/Public/PubHearings/LoadFile/77974>, accessed 12 October 2025.
145. Zenit-K's business identification number (BIN) is 141240006383.
146. *Tenderguru.ru*, « Заключенные контракты поставщика ТОО «Зенит-К» » ['Contracts Concluded with the Supplier LLC "Zenit-K"'], archived via Archive.today, 8 October 2025, <https://archive.fo/7qWxs>, accessed 12 October 2025.

Concern suppliers NPP Pulsar ($5.7 million), NIIET ($4.3 million) and NPP Istok ($4.1 million), and even to the manufacturer of the 91N6 Big Bird itself, NIIIP-NZiK ($459,241). Kazakh official trade statistics indicate that exports grew rapidly after the start of the full-scale invasion of Ukraine, from $1.2 million in 2022 to $17.8 million in 2024.

Figure 12: Zenit-K and Kaz Ceramics Use an Identical Corporate Logo for their Websites

Source: Ceramic Plant LLP Zenit-K, <https://web.archive.org/web/20210927073847/http://zenith-k.ru/ru>; Kaz Ceramics LLP, <https://kazceramics.kz/>, accessed 12 October 2025.

The Kaz ceramics factory is probably proceeding with the shipments and adjusting its operations, due to its awareness of the risk of sanctions. The website of Zenit-K, which referenced sanctioned companies NIIET, VZPP-S and Integral (Belarus) as customers, closed in January 2023. In 2025, Zenit-K and Kaz Ceramics started to increasingly ship their products to LLC Zenit,[147] a Novosibirsk-based low-profile affiliate of the group, which was detected to have launched sales to major importer NPP Istok in the same year.

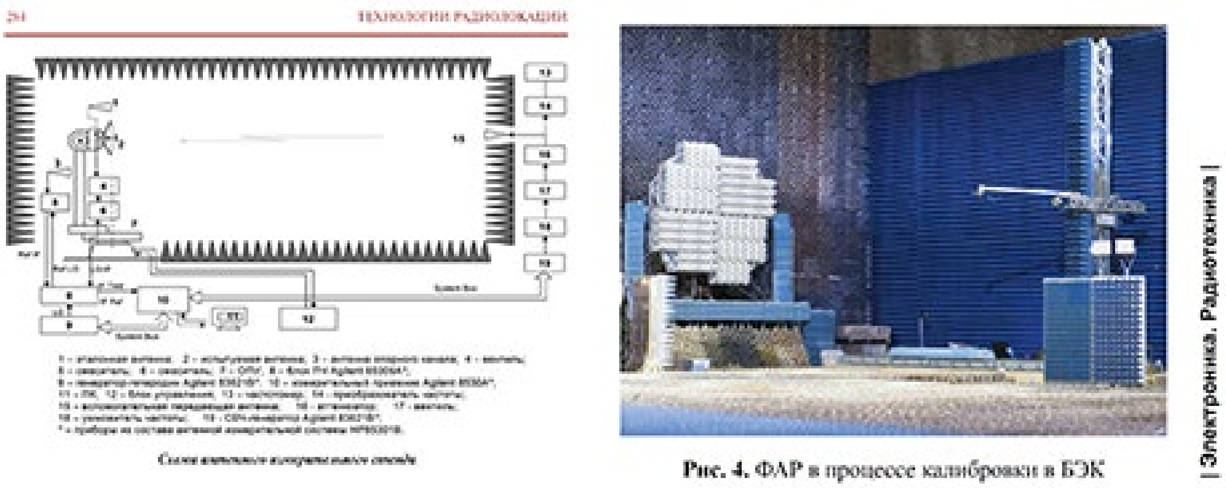
Meanwhile, Kaz Ceramics has regularly imported equipment critical for its production operations from Ukraine and the EU, in addition to China, since at least 2023. It has received diamond-cutting tools worth $20,676 from PJSC Poltavsky Diamond Instruments (Ukraine), pressing tools worth a total of $21,620 from Intervit Co., Ltd (Ukraine), as well as industrial electric furnaces SNOL from UAB Snoltherm (Lithuania) worth a total of $92,473.[148]

The disruption of trade flows through the application and enforcement of sanctions operations would have a significant impact on radar production for the S-400. This is one example, but there are a range of critical materials for the production of klystrons and other radar components that Russia largely imports. These entities remain unsanctioned by Russia's adversaries.

The Russians also rely on Western technologies to calibrate and measure the performance of their own radars. These are important for the initial acceptance of radars into service, but also for the continuous process of improving radar performance against threats.

147. In Russian, the group is called « ООО « Зенит» », with a Taxpayer Identification Number (INN) of 7708317135.
148. According to 2024 Russian trade data reviewed by the authors.

Figure 13: Diagram of Antenna Measuring Stand Used at PJSC Radiofizika



Source: A Tobolev, « Глава 8. Радиотехнические измерения. Измерение параметров антенн » [‘Chapter 8. Radiotechnical Measurements. Measuring Antenna Parameters’], in B Levitan et al., *Технологии радиолокации. К 55-летию ПАО “Радиофизика* [*Radar Technologies. On the 55th Anniversary of PJSC Radiofizika*] (Moscow: Veche, 2015), p. 284; E Korotetskiy, « Калибровка фазированных антенных решеток на открытых полигонах » [‘Calibration of Phased Array Antennas at Open Ranges’], *Bulletin of the Almaz-Antey Air Defence Concern* (No. 4, 2022), p. 33.

There are four Agilent (the previous name of Keysight) elements in the scheme (Figure 13, left), which depicts an anechoic testing chamber. The elements are all part of a vector network analyser (VNA) measurement system for microwave and antenna testing at the anechoic chamber of PAO Radiofizika in Moscow (Figure 13, right), claimed to be the biggest in Russia and Europe. The schematic was published in 2015 in a special edition on the 55th anniversary of PAO Radiofizika. Each module’s function is described below:

- Agilent 8530A is a measurement receiver for measuring amplitude / phase.
- Agilent 85309A is an IF (intermediate frequency) receiver, which converts and filters signals to IF.
- Agilent 83621B is a microwave generator, producing liable radio frequency / microwave signals for testing.
- Agilent 85301B is a system controller for coordinating, synchronising and aligning all modules.

PAO Radiofizika is not only involved in laboratory testing but also in the final stage before handing over new radars to the VKS in field or open-site tests. In a 2022 article, a team of three senior PAO Radiofizika engineers[149] described the key measurement errors that affect calibration results and also ‘an approach to the technique and

149. E Korotetskiy, « Калибровка фазированных антенных решеток на открытых полигонах » [‘Calibration of Phased Array Antennas at Open Ranges’], *Bulletin of the Almaz-Antey Air Defence Concern* (No. 4, 2022), p. 33.

procedure of phased array calibration at open test sites'. Two of the authors are heads of Radiofizika's main departments – Phased Array Engineering, and Antenna and Microwave Engineering. Unlike the 2015 publication, this paper does not mention the specific equipment being used, but changes in their testing as a result of disruption during the full-scale invasion of Ukraine are unlikely.

Instruments for the production and testing of radio equipment made by US manufacturer Keysight Technologies are widely used by Russian manufacturers of electronics, including key enterprises in the S-400 supply chain, such as Obukhovskiy Zavod, Mikron and Optron. According to trade records seen by the authors, in 2023 and 2024, Russian companies continued to import products made by Keysight and National Instruments mostly through China and Hong Kong, but also via Thailand, the UAE and Turkey, among others.

Russian companies received a total of $42,469,768 of equipment with Keysight branding in 2024.[150] The most imported instruments include signal generators, oscillographs and spectrum analysers. Disruption of the supply of testing equipment through the sanctioning and enforcement against suppliers would have an impact on the ongoing improvement of Russia's air defence systems.

Vulnerability to Attack

Beyond the question of economic interventions, Ukraine is also acquiring a growing array of kinetic and non-kinetic means for attacking Russian industries.

Russian developers and manufacturers of radioelectronic components and equipment used in radars continue to be critically reliant on foreign-made software tools, particularly for the modelling and simulation of components. In September 2025, NPO Almaz's LEMZ division, which manufacture 96L6 Cheese Board radars, sought design engineers to develop PCBs and microwave components using Altium Designer.[151] Obukhovskiy Zavod, the manufacturer of the 92N6 radar, advertised for lead engineers with experience in products such as Ansys HFSS and Keysight ADS[152] to model microwave components on Simulink, AWR Microwave Office and Multism, among others.[153]

150. According to 2024 financial data reviewed by the authors.
151. *HeadHunter*, « Инженер-конструктор по печатным платам и микроплосковой СВЧ-технике » ['Design Engineer for Printed Circuit Boards and Micro-Flat Microwave Technology'], 18 September 2025, archived via Archive.today, 13 October 2025, <https://archive.ph/LTgZm#selection-993.13-993.24>.
152. *DreamJob*, « [Вакансия в архиве] Ведущий инженер разработчик СВЧ » ['(Archived Vacancy') Lead Microwave Development Engineer'], archived via Archive.today, 28 September 2025, <https://archive.ph/hJQr3>, accessed 11 November 2025.
153. *HeadHunter*, « Ведущий инженер (СВЧ) » ['Lead Engineer (Microwave)'], 19 October 2025, archived via the Wayback Machine, 11 November 2025, <https://web.archive.org/web/20251111145619/https://spb.hh.ru/vacancy/120857156?from=employer&hhtmFrom=employer>.

Meanwhile, Mikron, Russia's most advanced plant for semiconductor devices, is currently looking for engineers experienced in using Cadence Virtuoso and Menthor Graphics.[154] In addition, training on foreign-made software products, such as AWR Microwave Office and Altium Designer, continue to be included in the curriculum for microwave device modelling at multiple Russian universities as of 2024 and 2025.[155]

The dependence on foreign-made software by Russian military–industrial enterprises has long been recognised as a cyber vulnerability by the Russian state, which has been funding projects for the development of domestic analogues. A list originally published by the Russian Ministry of Trade and Industry in June 2024 indicates that it was overseeing key Russian enterprises in the sector, particularly the VKO Almaz-Antey Concern, NPP Istok and Mikron, in their efforts to transition to Russian tools.[156]

According to the list, as of June 2024, suitable replacements for designing radio-electronic components and equipment had still not been developed; further, possible Russian alternatives to Altium Designer, used by VKO Almaz-Antey for radioelectronic equipment, and to AWR Microwave Office, used by NPP Istok for microwave devices, were not specified. In October 2024, the Industrial Competence Centre for the replacement of foreign industry digital products and solutions announced that Russia lacked domestic substitutes for 65 product categories, 52 of which were modelling and simulation tools for electronic components and equipment.[157]

154. *HeadHunter*, « Ведущий проектировщик фотошаблонов » ['Lead Photomask Designer'], 6 October 2025, archived via Archive.today, 11 November 2025, <https://archive.ph/jYggW>.
155. Saint Petersburg Electrotechnical University LETI, named after V I Ulyanov (Lenin). See St Petersburg, « Рабочая программа дисциплины «Междисциплинарный проект «Проектирование микроволнового транзисторного усилителя мощности» для подготовки магистров по направлению 11.04.04 «Электроника и наноэлектроника» по программе «Микроволновая и телекоммуникационная электроника» » ['Work Programme for the Discipline "Interdisciplinary Project "Design of a Microwave Transistor Power Amplifier" for the Training of Master's Students in the Direction 11.04.04 "Electronics and Nanoelectronics" Under the Program "Microwave and Telecommunication Electronics"'], 2025, <https://etu.ru/sveden/files/eih/RP24-711MeghdisciplinarnyiProekt_proektirovanieMikrovolnovogoTranzistornogoUsilitelyaMoschnosti_.pdf>, accessed 12 October 2025; Nizhny Novgorod Radio Engineering College, « Основная профессиональная образовательная программа «Профессионалитет». Специальности 11.02.17 Разработка электронных устройств и систем » ['Basic Professional Educational Programme "Professionalism". Specialisation: Development of Electronic Devices and Systems'], 2025; Moscow Aviation Institute, « Системы автоматизированного проектирования изделий СВЧ-техники. Аннотация к программе повышения квалификации » ['Computer-Aided Design Systems for Microwave Technology Products. Annotation to the Advanced Training Programme'], <https://mai.ru/education/dpo/fpk/cads_mep/>, accessed 12 October 2025.
156. Ministry of Industry and Trade of the Russian Federation (Minpromtorg), «Приказ об организации работы по утверждению приоритетных направлений замещения зарубежных отраслевых решений российскими аналогами» ['Order on the Organisation of Work to Approve Priority Areas for Replacing Foreign Industry Solutions with Russian Analogues'], РТ-Глобальные Ресурсы , 25 June 2024.
157. Igor Korolev, « После бегства иностранцев в российском ПО для микроэлектроники осталось 65 «белых пятен» » ['After the Flight of Foreigners, 65 "Blank Spots" Remained in Russian Microelectronics Software'], *Cnews*, 17 October 2024, <https://www.cnews.ru/news/top/2024-10-17_posle_uhoda_inostrantsev>, accessed 12 October 2025.

Russian technology solution providers have made progress in the development of alternatives to some of the most critical software tools, but they appear to still lack functionalities that would allow for full replacement, with R&D on more sophisticated design tools not expected to be completed before 2027 (Figure 14). For example, over the past decade, Rosatom subsidiary the All-Russian Scientific Research Institute of Experimental Physics (RFYaTs-VNIIEF) has been working on developing LOGOS, a software package for engineering analysis and supercomputer modelling.[158] LOGOS is intended to replace multiple simulation software packages developed by US company Ansys,[159] which are widely used by subsidiaries of the Almaz-Antey Concern, as shown in numerous publications in the Almaz-Antey Concern Bulletin. Yet, based on current job vacancies, at the time of writing there is scarcely any evidence that LOGOS has been adopted by any key enterprises. In addition, several Russian researchers in pertinent fields, including employees at a current division of the Obukhovskiy Zavod, have recently argued that the software still lags behind foreign counterparts.[160]

The conclusion is that there is a large attack surface within Russian design bureaus that could be exploited to either disrupt the design and modelling of Russian radar, or even to introduce compromises into the design.

Russia's air defence enterprise is also vulnerable to physical attack, largely because of its concentration of functions around some key concerns. To take Pantsir complexes as an example, there are two primary KBP assembly sites: KBP's main facility and Shcheglovsky Val (Figure 15). The cannons for Pantsir are produced by TulaTochMash and TsKBA, which also play a key role in the production of radars for the system. The primary assembly facilities, all located in Tula (Figure 15), are around 350 km from Ukraine and heavily defended. Ukraine's attack drones lack sufficient payload or

158. V E Kostyukov, « Предложения по развитию российских суперкомпьютерных и информационных технологий. Проекты ФГУП «РФЯЦ-ВНИИЭФ» (Госкорпорация «Росатом»)» » ['Suggestions for Development of Russian Supercomputers and Information Technologies. An FGUP "RFYATS-VNIIEF" Project (State Corporation "Rosatom")'], Government of the Russian Federation, February 2016, <http://static.government.ru/media/files/p5s9xN7FOBTZFoMahAzjAGjSh0aiXBAJ.pdf, accessed 12 October 2025.

159. *Российский фонд развития информационных технологий*, « Внедрение российского ПО кратно повысило точность моделирования ракетных двигателей » ['The Introduction of Russian Software has Multiplied the Accuracy of Modeling Rocket Engines'], 6 April 2025, <https://rfrit.ru/news/vnedrenie-rossiiskogo-po-kratno-povysilo-tochnost-modelirovaniia-raketnykh-dvigatele/>, accessed 12 October 2025; R Shagaliev, « Имитационное моделирование: Отетчественные суперкомпьютерные технологии ФГУП «РФЯЦ-ВНИИЭФ» » ['Simulation Modeling: Domestic Supercomputer Technologies of the Russian Federal Nuclear Center-VNIIEF'], June 2015, <https://www.connect-wit.ru/wp-content/uploads/2015/06/2-9.2_Grebennikov.pdf>, accessed 12 October 2025.

160. A Vasilyev, « Выбор оптимального программного обеспечения для численного моделирования работы энергопоглощающих элементов перспективных систем амортизации специальных объектов в контексте импортозамещения средств инженерного анализа » ['Selecting the Optimal Software for Numerical Modeling of Energy-Absorbing Elements of Advanced Depreciation Systems for Special Facilities in the Context of Import Substitution of Engineering Analysis Tools'], *Bulletin of the Almaz-Antey Air Defence Concern* (No. 3, 2022), pp. 5–20; *PortNews*, « ПО «Логос» в некоторых отношениях уступает зарубежным аналогам и требует доработки – Крыловский ГНЦ » ['"Logos" is Inferior to Foreign Analogues in Some Respects and Needs to be Improved – Krylov State Scientific Centre'], 12 May 2023, <https://portnews.ru/news/347610/>, accessed 12 October 2025.

kinetic energy to damage many industrial targets and have so far failed to damage key facilities around Tula. However, as Ukraine's stockpile of indigenous cruise missiles expands, the ability to reach and damage the relevant targets improves.

Figure 14: R&D Projects for Domestic Design Tools, Shown at the Microelectronics Forum, September 2025

Source: Forum Microelectronics, « Отечественные САПР: дорожные карты и господдержка обсуждены на форуме «Микроэлектроника 2025 » ['Domestic CAD Systems: Roadmaps and Government Support Discussed at the "Microelectronics 2025 Forum"'], RuTube, at 0.55, <https://rutube.ru/video/b3aca58876c2aa841570d136b78b4be9/>, accessed 12 October 2025. The chart indicates that the earliest date that work for the development of more sophisticated tools, such as world-class computer-aided design software for microwave devices, could be expected to start is 2027.

While the clustering of these sites enables the concentration of air defence, it also means that once the defences are saturated, all sites become vulnerable. Ukraine could, therefore, mount an operation to saturate the defences on an approach to Tula before delivering a significant blow to Pantsir production with cruise missiles – ironically resulting in limiting Russia's ability to defend other targets over the course of 2026.

These are but a fraction of the points of vulnerability identified in Russia's integrated air defence production. A systematic effort to exploit these vulnerabilities could have a disproportionate impact on assisting Ukraine to strike the economic backbone of the Russian war effort and reduce the barriers to NATO airpower, consequently deterring future Russian aggression by denial.

Figure 15: The Concentration of Pantsir Production in Tula

Source: Produced using Felt mapping tools, <https://felt.com/>, accessed 23 November 2025. All sites are within an 8 km diameter area.

Conclusion

This paper has demonstrated how Russian air defences are multilayered and highly capable against current Ukrainian and European capabilities. They therefore pose a challenge to European security by reducing the capacity of European militaries to bring airpower to bear in conflict. By degrading the efficiency of Ukraine's long-range strike campaign, they also prevent Ukraine from undermining the revenue generation that is enabling Russia's full-scale invasion. The paper also outlines the contours and critical industrial centres of the production process for the design and production of Russia's air defences.

The research for this paper demonstrates that Russia has significant dependence on foreign software to design its weapons and measure equipment to certify their performance. Russia also has a dependence on foreign components and raw materials for production. Moreover, many of its key facilities are concentrated and potentially vulnerable to attack. The vulnerabilities discussed in this paper represent a fraction of those identified by the authors and as such are indicative rather than comprehensive. Of most concern is that Russia is still managing to acquire critical machine tooling, subcomponents and raw materials from NATO members, let alone from third countries.

The authors would emphasise that Ukraine and its international partners have a wide range of opportunities to disrupt Russian air defence production. In the short term, this may contribute to forestalling the expansion of Russia's production of interceptors, thereby improving the effectiveness of Ukraine's long-range strike campaign. In the long term, it would contribute to maintaining the balance of conventional deterrence in Europe. Disrupting production is feasible. The ultimate question is the will of Ukraine's international partners to apply targeted sanctions and carry out diligent enforcement to deliver the requisite effects.

It should also be highlighted to those actors considering the purchase of Russian air defence systems that the exposure of Russian industry to disruption may make Russia an unreliable supplier of reloads in a crisis. Moreover, noting the level of information in this paper on systems and their production, and the necessarily more detailed knowledge in NATO governments, it must be asked to what extent Russian air defences are technically compromised, irrespective of how well they perform in testing. Customers should ask whether they can provide a reliable shield against emerging NATO strike systems.

Authors

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

Nikolay Staykov is a Lead Analyst at Panoptikon.

Maya Kalcheva is an Analyst at Panoptikon.

Olena Yurchenko is the Director for Analysis, Investigations and Research at the Economic Security Council of Ukraine (ESCU).

Bohdan Kovalenko is a Senior Analyst at ESCU.

Olena Zhul is a Senior Analyst at ESCU.

Oleksii Borovikov is a Senior Analyst at ESCU.

Anastasiia Opria is an Analyst at ESCU.

Roman Rabieiev is an Analyst at ESCU.

Nadiia Reminets is an Analyst at ESCU.

Alex Whitworth is an illustrator and graphic designer.

RUSI

194 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 194 years.

18 31